Cuadernos penales
José María Lidón

Núm. 4

Delito e informática: algunos aspectos

Juan José González Rus / Norberto J. de la Mata Barranco / Esther Morón Lerma / Ricardo M. Mata y Martín / Jaime Moreno Verdejo / Fermín Morales Prats / Manuel Viota Maestre / José Manuel Ortiz Márquez / Ladislao Roig Bustos / Luis Carreras del Rincón / Antonio Narváez Rodríguez / Carolina Sanchís Crespo / Carmen Adán del Río

Universidad de Deusto

Cuadernos penales
José María Lidón

Cuadernos penales José María Lidón

Núm. 4

Delito e informática: algunos aspectos

Juan José González Rus
Norberto J. de la Mata Barranco
Esther Morón Lerma
Ricardo M. Mata y Martín
Jaime Moreno Verdejo
Fermín Morales Prats
Manuel Viota Maestre
José Manuel Ortiz Márquez
Ladislao Roig Bustos
Luis Carreras del Rincón
Antonio Narváez Rodríguez
Carolina Sanchís Crespo
Carmen Adán del Río

Bilbao
Universidad de Deusto
2007

© Publicaciones de la Universidad de Deusto
Apartado 1 - 48080 Bilbao
e-mail: publicaciones@deusto.es

ISBN: 978-84-9830-753-5

Índice

Presentación
Carmen Adán del Río, Norberto J. de la Mata Barranco 9

Precisiones conceptuales y político-criminales sobre la intervención penal en Internet
Juan José González Rus 13

Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general
Norberto J. de la Mata Barranco 41

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos
Esther Morón Lerma 85

Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo)
Ricardo M. Mata y Martín 129

Algunas cuestiones acerca de la estafa informática y uso de tarjetas (Incidencia del Anteproyecto de 2006 de reforma del Código penal)
Jaime Moreno Verdejo 173

Los delitos informáticos: dudas e incertidumbres en el Proyecto de Reforma del Código Penal
Fermín Morales Prats 227

Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)
Manuel Viota Maestre 237

Responsabilidad penal de los proveedores de enlaces
José Manuel Ortiz Márquez 259

La cuestión informática en el ámbito procesal (y también penal). Aproximaciones a partir del caso Bitel.
Ladislao Roig Bustos 277

La cuestión informática en el ámbito procesal. Algunos aspectos
Luis Carreras del Rincón 287

Tutela de la privacidad e interceptación pública de las comunicaciones
Antonio Narváez Rodríguez 297

El levantamiento de la carga de la prueba en Internet: ¿ficción o realidad?
Carolina Sanchís Crespo *375*

Anexo: Vocabulario informático y siglas de interés
Carmen Adán del Río 391

Presentación

Carmen Adán del Río
Fiscal del Tribunal Superior de Justicia del País Vasco

Norberto J. de la Mata Barranco
Profesor Titular de Derecho Penal de la UPV

Los *Cuadernos Penales José María Lidón* se presentaban en su número uno como un homenaje sentido a su persona y con un cierto anhelo de un Derecho que impulse la construcción de una sociedad cada vez más humana. El contenido del curso que se refleja en este número sigue respondiendo a ese deseo tanto en el recuerdo y en el homenaje como en la búsqueda de un Derecho que responda a las necesidades de la sociedad en general y del ciudadano en particular.

Hace ya tiempo que los medios informáticos se han integrado con naturalidad en nuestra vida diaria. Conceptos como ciberespacio y universo digital no nos resultan ya lejanos o de ciencia ficción. Son parte de nuestra realidad. Pero convivir con ellos no equivale a entenderlos, a salvo de intuir o percibir que el futuro depara sin duda una evolución en este ámbito de proporciones inesperadas.

Un fenómeno similar se produce en el ámbito del Derecho que se refiere a esta nueva realidad. Las innovaciones que el Código Penal vigente introdujo en la materia ya no dan respuesta a un creciente número de supuestos; insuficiencia que el propio legislador reconoce en los preparativos del nuevo Código Penal, dando carta de naturaleza, por ejemplo, a la figura del *hacker* y justificando la decisión de penalizar la actuación de los piratas informáticos y las intromisiones ilegales en sistemas informáticos en la necesidad de «[…] actualizar y modernizar la respuesta penal ante determinados delitos que se producen en sectores nuevos, producto de los últimos avances tecnológicos […]».

Las *Jornadas* que se celebraron en Bilbao los días 22 y 23 de marzo de 2007 que se nos encargó coordinar y cuyas ponencias se recogen en este volumen, fueron concebidas con la idea de abarcar los diferentes ámbitos de influencia de la informática en el Derecho Penal, no sólo en su aspecto sustantivo, sino también en el del procedimiento. Cada una de las intervenciones refleja un esfuerzo por acercar la realidad al

texto legal, en ocasiones con un cierto reconocimiento de que utilizar los conceptos y los tipos penales que ya conocemos para los nuevos supuestos, conlleva la sensación de no pisar suelo firme. Y junto a la intuición general de estar ante un fenómeno creciente que nos puede desbordar, destaca, de forma curiosa pero unánime, que la sensación de poder, alcance y facilidad de acceso a datos sorprendentes que ofrece la informática, se complementa con la sensación de un ciudadano inerme y débil frente a ella.

El aspecto sustantivo se abordó desde el doble concepto de delitos informáticos. Tanto el más adecuado de delitos contra los sistemas informáticos como el más amplio de delitos cometidos a través o por medio de la informática. Este concepto amplio es el elegido por la Fiscalía General del Estado, que, en la línea iniciada por la Instrucción 11/2005 de dar un tratamiento unitario y de mayor eficacia a determinadas materias, ha designado en mayo de este año un Fiscal de Sala, como Delegado del Fiscal General, en materia informática, cuya función es asumir la coordinación de los delitos cometidos específicamente «a través de medios informáticos y singularmente por medio de Internet», a fin de asegurar un tratamiento unitario y uniformidad de los criterios de actuación, ejerciendo la dirección de quienes en la Carrera Fiscal lleven estas materias.

Interesa destacarlo como muestra de que en la práctica penal consta ya la importancia del fenómeno, aunque es pronto para saber hasta qué punto Internet y los medios informáticos pueden influir de futuro en la sistemática del Código Penal.

Esta llamada a un tratamiento unitario y a la uniformidad de criterios de actuación no resultará fácil, dada la diversidad de bienes jurídicos a proteger frente a los ataques por medios informáticos e Internet. La pregunta de si el catálogo de bienes jurídicos y los tipos penales actuales son suficientes (con la sola necesidad de ir recogiendo nuevas formas de ataque) para responder a la realidad actual o de si, por el contrario, hemos de definir un nuevo bien jurídico relacionado con estos medios no es de fácil respuesta.

En todo caso, es evidente que se avecinan cambios legislativos. El debate ya se ha abierto con relación a la propiedad intelectual en Internet, aunque sea con una sensación manifestada públicamente en diferentes medios de comunicación de cierto pesimismo, en la medida en que, aún logrando una delimitación y un reconocimiento no difuso, «[…] quizá no haya autoridad capaz de imponer esa ley». El fenómeno de la contratación electrónica, en el que confluyen las reglas generales de contratación y al tiempo las específicas derivadas de la utilización de medios electrónicos, afecta por ahora al ámbito civil, pero es claro

que como mínimo por la vía de los negocios jurídicos criminalizados, aparecerá en lo penal. Perfeccionar y redefinir algunos de los tipos penales se demanda incluso por quienes son partidarios de mantener la sistemática actual del Código Penal.

Por otro lado, en el apartado del procedimiento, al margen de las modificaciones de la Ley de Enjuiciamiento Criminal, nos encontramos en un momento temporal aún de espera, pero ante el hecho indudable de que el nuevo procedimiento está en una fase de desarrollo avanzado. Por mucho que este procedimiento penal, mal llamado virtual, parezca algo lejano e irreal, lo cierto es que la estructura básica se encuentra ya creada, prometiendo agilidad y facilidad de comunicación a las partes, obviando los trámites de fotocopia o traslado de originales, haciendo posible por fin, si se quiere llegar a ello, un adecuado cómputo de los plazos para todos, etc., logros todos ellos que, al final, reforzaran derechos y garantías.

En el mismo sentido, la investigación y la prueba ya han sido influidas por los nuevos medios. Un ejemplo claro es el de la valoración de la prueba testifical o pericial, que se relacionaba tradicionalmente con la inmediación, exigencia que hoy se cubre, en los juicios orales, por medios electrónicos, evitando dilaciones y complicaciones innecesarias.

Con relación a estos dos últimos apartados, hemos de estar igualmente, al resultado de las reuniones periódicas que en la actualidad mantienen los ministros de Justicia de la Unión europea, sobre la llamada «e-justicia», que partiendo de la enorme disparidad de sistemas jurídicos entre los Estados miembros, reconoce como fin último, aplicar las ventajas de las nuevas tecnologías y la sociedad de la información, a la interconexión de la justicia en Europa. Reuniones, de las que ya constan experiencias satisfactorias como la de los registros informatizados, a disposición de las respectivas administraciones, sobre antecedentes de ciudadanos que circulan por Europa, pero cuyos resultados de mayor calado son los que hoy están en fase de preparación y estudio en las reuniones de Bremen y Dresde.

De todo ello, es fácilmente predecible que el futuro nos depara en materia informática cambios que afectarán a los aspectos sustantivo y procesal del Derecho Penal. Cambios que esperamos faciliten la aplicación del Derecho, incorporando aportaciones de la doctrina y la jurisprudencia, pero sin olvidar que el Código Penal debe reflejar aquello que una sociedad en un momento temporal concreto acepta como digno de protección.

Precisiones conceptuales y político-criminales sobre la intervención penal en Internet

Juan José González Rus
Catedrático de Derecho penal. Universidad de Córdoba

I. La intervención penal en Internet

Hoy carece de sentido plantearse si la intervención estatal y, en particular, la intervención penal en Internet está justificada o no. Tan obvia es la respuesta, que no se hace preciso comentario particular alguno.

La cuestión que hoy debe ser tratada es, pues, directamente la de cómo debe intervenir el Derecho Penal en relación con las aplicaciones y procedimientos informáticos y las redes de transmisión de datos e Internet. Ello, en un triple sentido: (1) sobre qué premisas valorativas debe apoyarse la intervención, lo que conduce a la determinación de los bienes jurídicos que deben ser protegidos; (2) qué tipo de ataques deben ser considerados penalmente relevantes, y (3) qué instrumentos de técnica legislativa resultan preferibles para articular la tutela penal.

De esas tres cuestiones, la primera es, sin duda, la de mayor importancia. Sólo cuando se defina con la suficiente precisión qué debe ser protegido en relación con los intereses que se desenvuelven en Internet y en las redes de transmisión de datos podrá efectuarse de manera certera la determinación de los riesgos que resultan admisibles y, consecuentemente, de las conductas que deben ser eventualmente mandadas o prohibidas. Como en tantos otros ámbitos del Derecho Penal actual, la identificación y delimitación de los bienes jurídicos que deben ser eventualmente protegidos resulta, pues, la cuestión central.

En relación con la intervención penal en Internet y en las redes de transmisión de datos, se mantienen actualmente dos criterios. Uno, partidario de incorporar a la tutela penal los «nuevos» bienes jurídicos que habrían nacido como consecuencia de la generalización y consolidación de los medios y procedimientos informáticos y que tendrían la suficiente importancia para merecer la intervención penal; ello, naturalmente, sobre la base implícita de que las previsiones penales actualmente disponibles resultan insuficientes para afrontar los problemas que punición que

presentan Internet y las redes de transmisión de datos. Otro sector, en cambio, partidario de agotar las posibilidades de protección que ofrece el derecho vigente, sobre la base de los bienes jurídicos «tradicionales»; sin perjuicio, naturalmente, de introducir, en la medida en que resulten precisas, las modificaciones concretas necesarias.

La posición más caracterizada del primer sector doctrinal es la de quienes mantienen la conveniencia de destacar como sector autónomo del ordenamiento y de la Dogmática Penal el que se denomina «Derecho Penal de la informática» o «Derecho Penal informático». En este sentido, por ejemplo, PICOTTI (págs. 22 y ss.), entiende que a pesar de que las normas penales que se ocupan ahora de la criminalidad informática constituyen un conjunto heterogéneo, con una clara visión sectorial y fragmentaria, es necesario un tratamiento conceptual que tenga en cuenta los puntos comunes, las semejanzas entre unas y otras normas, para poner un cierto orden en la materia. Sobre esas bases se construiría lo que denomina directamente el «Derecho Penal de la informática». El criterio en torno al que se construiría el mismo es, en primer lugar, el bien jurídico protegido, y, como elemento auxiliar, la clasificación sistemática de las figuras; así como la propia evolución legislativa y el análisis de las razones que determinaron su incorporación al Código Penal.

La segunda posición es la mayoritaria en el derecho comparado y es la que —puedo anticiparlo ya— considero preferible, por las razones que expongo a continuación.

II. **Intervención penal apoyada en bienes jurídicos «nuevos» de naturaleza informática**

De acuerdo con el criterio de un significativo (y creciente) sector doctrinal, la intervención penal en Internet no puede hacerse desde la base que ofrecen los bienes jurídicos que actualmente reciben protección penal. Las particularidades del medio, la extraordinaria difusión alcanzada por Internet y las redes de transmisión de datos, el elevadísimo número de usuarios y de relaciones que se desarrollan a través de las mismas, hace obligado, a su juicio, prestar protección a «nuevos» bienes jurídicos, que resultarían la plasmación de los intereses personales y sociales que se desenvuelven actualmente en Internet.

El desarrollo tecnológico, estima PICOTTI, ha hecho surgir nuevos intereses, que se han mostrado merecedores de específica y autónoma tutela jurídica, incluso penal. Se trata de bienes jurídicos «nuevos» en la medida en que no encuentran una precisa correspondencia con otros preexistentes, aunque tengan una cierta analogía con ellos. De acuerdo

con el criterio más compartido, tales bienes serían: la seguridad informática, la intangibilidad o indemnidad de los datos informáticos y la libertad informática. Se trataría de bienes jurídicos que se postulan como susceptibles y necesitados de protección penal, con significación propia y autónomos respecto de los bienes jurídicos personales con los que aparecen relacionados.

Junto a ellos, la materia propia del Derecho Penal de la informática comprendería también los bienes jurídicos «tradicionales», que, al aparecer insertos en el medio informático o relacionados con procedimientos de esa naturaleza, adquieren una dimensión nueva que los hace diferentes del sentido originario, que mantienen en el ámbito del, por decir así, Derecho Penal «general».

La cuestión que primero debemos abordar es, pues: ¿hay tales?; ¿hay, efectivamente, bienes jurídicos «distintos» de los «tradicionales» y cuyo sustrato fáctico y significación valorativa aparece sustancialmente vinculada a Internet y a los medios, elementos o procedimientos informáticos o telemáticos?

1. *Seguridad informática*

La «seguridad informática» se concibe como un bien jurídico colectivo que viene a dar protección anticipada a otros de naturaleza personal como la intimidad, el honor, el patrimonio, la libertad de información, el secreto y la inviolabilidad de las comunicaciones; aunque no siempre queda claro cuáles son efectivamente los derechos relacionadas con ella.

Su lesión se produciría en cuanto se atenta al uso y funcionamiento correcto de redes y sistemas informáticos con conductas como, por ejemplo, el acceso indebido a un ordenador, incluso si no es para realizar una actividad ilícita ulterior. La posibilidad de prohibir tales comportamientos se fundamenta en que generan riesgos para los bienes jurídicos personales a cuya protección mediata sirve la seguridad informática. Se trataría de un bien jurídico colectivo e indisponible, en la medida en que las agresiones a la seguridad informática crean riesgos frente a todos los usuarios y no respecto de un sujeto concreto.

La necesidad de crear un tal bien jurídico se apoya, por una parte, en que el recurso a la exclusiva protección de bienes personalísimos desconoce la relevancia social que ha adquirido Internet como forma de comunicación interpersonal, con identidad y autonomía propia, de manera que la tutela específica y diferenciada cumpliría una función simbólica positiva, estimulando la conciencia social sobre la necesidad de proteger

su seguridad y la gravedad del uso y funcionamiento indebidos de las redes. Por otra, en que la intervención penal a través de las figuras dirigidas a la protección de los bienes jurídicos individuales requiere probar la motivación y la intención subjetiva del autor respecto del bien jurídico lesionado de manera efectiva, lo que dificulta la protección, dado que en la mayoría de los casos el ataque a la red o al sistema informático no se dirige contra esos bienes jurídicos. Por eso, estaría justificada la configuración de la seguridad informática como bien jurídico colectivo autónomo y la anticipación de la tutela al momento del peligro.

En sentido parecido se ha pronunciado expresamente PICOTTI (págs. 70 y ss.) en la doctrina italiana. A su juicio, el bien jurídico «integridad y seguridad informática» adquiere relevancia práctica y autonomía conceptual como consecuencia de la creciente amplitud de las relaciones que se desenvuelven a través de la informática. La garantía de la pronta y correcta utilización de los datos, sistemas y productos informáticos deviene, así, un interés necesitado y merecedor de protección eficaz, ante el peligro de alteraciones, destrucciones, dispersiones o impedimentos a su utilización. Y ello, con independencia de que se lesionen «también» otros bienes jurídicos más tradicionales, que están en el fondo del comportamiento, como, por ejemplo, el patrimonio, la fe pública, el orden público, el derecho de exclusiva, etc. «La pronta y correcta posibilidad de usar los nuevos medios informáticos merece, así, convertirse en objeto de tutela penal, por el intrínseco valor de su plena disponibilidad, integridad, disfrutabilidad, en el ámbito de las relaciones económicas y sociales» (pág. 71). Se trata de un concepto que procura un nivel anticipado y preventivo de protección, respecto al de la efectiva lesión de la integridad y posibilidad de utilización de los datos, sistemas y productos informáticos, o, si se prefiere, de su concreto daño, comprendiendo todos los dispositivos, medidas, procedimientos instrumentales de protección, etc., que se desarrollan a nivel técnico y organizativo.

En el Código Penal italiano este bien jurídico protegido sería el objeto jurídico del artículo 392, que efectúa una ampliación del concepto de «violencia sobre las cosas», hasta comprender, no sólo las alteraciones, modificaciones o cancelaciones parciales de un programa informático, sino también la simple obstaculización o perturbación del funcionamiento de un sistema informático o telemático. Asimismo, también protege la integridad y seguridad informática el artículo 615-*quinquies* CP italiano, que castiga la difusión de programas dirigidos a dañar o interrumpir un sistema informático, en la medida en que anticipa la protección penal a un momento anterior al de la directa causación del daño. Ello permite castigar, por ejemplo, la difusión de virus informáticos desde el mismo momento de su difusión, con independencia de que llegue a producirse

efectivamente el daño al sistema (págs. 75). Lo mismo ocurriría en el artículo 615-*ter*, p. 2.º, que agrava la pena del delito de acceso abusivo a un sistema informático ajeno, la destrucción del sistema o de los datos, informaciones o programas o la interrupción total o parcial de su funcionamiento (pág. 76).

2. *Integridad y disponibilidad de los datos*

Consideraciones semejantes a las que quedan hechas en relación con la seguridad informática se han planteado también para auspiciar la necesidad de reconocer y prestar tutela penal a la integridad y disponibilidad de los datos, concebida como bien jurídico «nuevo» y específicamente «informático».

La integridad y disponibilidad de los datos es un bien jurídico que se considera protegido específicamente en algunas de las figuras del delito relacionadas con la informática que se recogen en algunos países como Alemania o Austria. Se entiende por tal la incolumidad de los datos, su libre disposición y su mantenimiento en los términos en que los ha configurado su titular.

En el derecho español, algunos autores han considerado que este es el interés protegido en el artículo 264.2, cuyo bien jurídico protegido no sería la propiedad, ni se inscribiría en la órbita del delito de daños, sino que se dirigiría a la tutela de los datos en sí mismos, cuya incolumidad, libre disposición y mantenimiento en los términos en que los ha configurado su titular constituiría el objeto de la protección penal (así, Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, Andrés Domínguez, Morón Lerma y Corcoy Bidasolo).

Concebido así el delito del art. 264.2, adquirían sentido ciertas consecuencias interpretativas que resultan poco explicables desde la óptica estricta del delito de daños. Por ejemplo, la distinta pena que corresponde a los daños en elementos no informáticos y a los daños en elementos informáticos, en la medida en que la destrucción de éstos, contemplada en el artículo 264.2, está castigada con más pena que las de los primeros, incluible en el tipo básico del artículo 263. En efecto, concebido el delito en términos de lesión del bien jurídico integridad o incolumidad de los datos, ninguna dificultad hay, en principio, para entender que la protección que debe darse a los datos informáticos habría de ser superior a la que reciben los elementos físicos, por lo que deben sancionarse con mayor gravedad los atentados a la integridad o a la libre disposición de los mismos que los delitos de daños, que sólo protegen la propiedad.

Tampoco sería obstáculo para una interpretación de este tipo el que la conducta típica del art. 264.2 aparezca construida en torno a la destrucción, alteración, inutilización o daño, por cualquier otro modo o procedimiento, de los datos y documentos electrónicos, puesto que ésta es también la forma en que puede lesionarse la integridad o libre disponibilidad de los mismos. Circunstancia que permitiría explicar, igualmente, la ubicación sistemática de la figura dentro de los delitos de daños.

La primera consecuencia que se derivaría de un entendimiento de este tipo es que la cuantía económica del elemento dañado no resultaría relevante para la configuración del delito ni para la determinación de su gravedad; aspecto, por cierto, omitido también en la letra del artículo 264.2, lo que podría verse como un indicio más en favor de esta tesis. La segunda consecuencia es que cuando la conducta afecte de consuno a elementos lógicos y físicos debería apreciarse un concurso ideal de delitos entre este artículo 264.2 y el de daños que corresponda en atención a la naturaleza o valor del elemento físico afectado (v. críticamente *in extenso*, González Rus, 2002 y 2004).

3. *Libertad informática y «riservatezza informatica»*

La «libertad informática» se plantea también como bien jurídico autónomo y diferenciado, de naturaleza estrictamente informática y digno y necesitado de protección penal específica. El contenido central del mismo vendría dado por el derecho del individuo a decidir qué información personal se podrá difundir sobre él y su familia y el destino de la misma. Se trata de un derecho que se presenta como complementario del propio y tradicional de la intimidad y tendría que ver fundamentalmente con los peligros que para esta supone el desarrollo de la informática. Ya no se trataría, pues, simplemente del derecho a excluir a los demás de un determinado ámbito que el titular considera reservado, y que se protege frente a intromisiones indeseadas, sino de un poder positivo de control sobre la información personal que los demás tienen de cada uno y sobre el uso que hacen de la misma. Ese es el sentido de la llamada libertad informática, *habeas data* o derecho de autodeterminación informativa.

En una línea semejante se encuentra la *riservatezza informatica*, postulada por Picotti como «nuevo» bien jurídico merecedor y necesitado de específica tutela penal relacionado con los procedimientos informáticos (*riservatezza informatica*; págs. 78 y ss.). Tal bien se concibe como interés al disfrute y control exclusivo de los productos y de las utilidades de las nuevas tecnologías, «verdadero y propio derecho de excluir a los terceros no legitimados» y que no estaría suficientemente garantizado

ni por los tradicionales medios de tutela de la propiedad y de la posesión de las cosas materiales, ni por la protección jurídico penal prestada al secreto, a la intimidad personal y domiciliaria y a los bienes inmateriales.

La privacidad informática, entendida así, sería el objeto de tutela del artículo 615-*ter* CP italiano, en el que se castiga el acceso abusivo a un sistema informático o telemático, colocado en el derecho italiano junto a la violación de domicilio (artículo 614). Otro tanto sucedería en el artículo 615-*quarter* (CP italiano), que castiga la mera tenencia y difusión abusiva de códigos de acceso a sistemas informáticos o telemáticos, así como proporcionar indicaciones o instrucciones con ese objeto. Se trata de un delito de consumación anticipada, que se realiza sin necesidad alguna de ofensa a la intimidad ajena ni a la seguridad de los sistemas, castigando conductas meramente preparatorias. En la misma línea de ataque se encontraría también el artículo 617-*quater* y el art. 617 *quinquies*, que castigan la interceptación de comunicaciones relativas a un sistema informático o telemático o de comunicación entre sistemas, y que ofrece la particularidad de que se refiere a comunicaciones entre sistemas, lo que los diferencia de la confidencialidad de las comunicaciones o conversaciones telefónicas y telegráficas entre personas, que es el objeto protegido en las figuras paralelas.

4. *Bienes jurídicos informáticos «por transformación» de su sentido originario*

Otra corriente de opinión doctrinal estima que los bienes jurídicos de las —digamos así—, figuras de delito «tradicionales» y los que son propios de los comportamientos y delitos informáticos no son los mismos. La idea central de esta posición es que los bienes jurídicos «tradicionales», cuando tienen que ver con elementos informáticos sufren una transformación que les da un contenido diferente del originario. En este sentido se ha pronunciado en la doctrina italiana PICOTTI, con consideraciones que recogemos a continuación con cierto detalle por constituir un resumen suficientemente representativo de la posición en examen.

Esa «transformación» sustancial de los bienes jurídicos se produciría:

(I) en los «tradicionales», cuando se les protege contra nuevas modalidades de agresión relacionadas con procedimientos informáticos;
(II) en los bienes jurídicos «análogos» surgidos de nuevos objetos materiales de la conducta.

(I) A juicio de PICOTTI (págs. 55 y ss.), cuando en el comportamiento se ven involucrados objetos, procedimientos o conductas de naturaleza

informática, aparecen connotaciones nuevas que hacen —incluso en los bienes jurídicos más consolidados y tradicionales, como, por ejemplo, el patrimonio—, que lo que realmente se vea afectado no sea «exactamente» lo mismo que se lesiona o pone en peligro en los delitos contra el patrimonio «no informáticos».

Así ocurriría, por ejemplo, en la estafa informática, cuyo bien jurídico no sería sólo o exactamente el patrimonio, sino que el hecho de que en las defraudaciones producidas por medios informáticos no pueda producirse el error característico de la misma, determina que el objeto de tutela del nuevo delito se traslade hacia «la garantía de —junto al patrimonio— una correcta y fiel activación y ejecución de los procedimientos programados, contra el riesgo de intervenciones, no sólo manipuladoras en sentido estricto, sino también abusivas ("sin derecho", *ex* artículo 640-*ter* CP italiano), sufriendo, por tanto, una evidente transformación» (pág. 55). En vez de inscribirse claramente en la tutela del patrimonio, la estafa informática se encontraría más próxima a un paradigma de tutela del patrimonio caracterizado por la infidelidad del agente.

Otro tanto sucede en el caso del uso fraudulento de tarjetas de crédito, en donde el objeto de tutela sería distinto del meramente patrimonial privado. Lo que se protegería sería el interés público en «evitar que el sistema informático sea utilizado con el fin de blanqueo y el de salvaguardar la fe pública; lo que justificaría, incluso, la posibilidad de concurso material o formal entre los dos delitos. Ello otorgaría a estos supuestos una dimensión colectiva o pública» (págs. 56-57).

Una manifestación de esta dimensión colectiva que tienen los ataques relacionados con medios o procedimientos informáticos la pondría de manifiesto, también, el hecho de que determinados delitos informáticos hayan sido situados directamente en el ámbito de bienes jurídicos tradicionales de naturaleza colectiva. Así, el atentado a instalaciones de elaboración de datos de utilidad pública se ha colocado en el Código italiano en él ámbito de los delitos contra el orden público (artículo 420 CP italiano), poniendo de manifiesto que la seguridad o el orden público es lo que predomina en esos atentados de naturaleza informática (pág. 58).

(II) Lo mismo sucede en relación con los bienes jurídicos «tradicionales» que tienen ahora por sustrato material nuevos objetos materiales. Por ejemplo, en el caso de documentos informáticos, la fe pública no podría ser entendida de la misma forma que en relación con documentos tradicionales: como consecuencia, la indudable peculiaridad del objeto sobre el que recae la falsedad informática, necesariamente afectaría al bien jurídico protegido, que ya no puede ser la tradicional «fe pública

documental». Y ello porque «el aseguramiento de la colectividad y de los participantes en el tráfico informático o telemático —que merece y es necesario que sea específicamente tutelado también por el Derecho Penal— concierne a instrumentos y técnicas de manifestación y comunicación del pensamiento distintas a las que representan los documentos materiales o "actos", tradicionalmente entendidos» (pág. 63). Lo que vendría a protegerse sería la fe pública en los «datos», más que en los «documentos», y esa sería la peculiaridad última que haría distintos a unos bienes jurídicos y a otros (pág. 64).

Consideraciones semejantes pueden hacerse, a juicio de PICOTTI, en torno al derecho de autor, en relación con el que la difusión de medios y procedimientos informáticos abre posibilidades de ataque y formas de explotación inéditas (págs. 65-67), y sobre la protección de la intimidad y la circulación de los datos personales, en donde se protegerían también objetos jurídicos, próximos, si se quiere, pero sustancialmente distintos de los tradicionales (págs. 67-69).

5. *Consideraciones críticas*

A) SOBRE EL CONCEPTO Y NECESIDAD DE PROTECCIÓN DE LA SEGURIDAD INFORMÁTICA COMO «NUEVO» BIEN JURÍDICO INFORMÁTICO

Por mi parte, no veo que en el derecho español sea necesaria la protección de un bien jurídico como la «seguridad informática», tal y como ha quedado definida; ni veo actualmente en el Código Penal español ninguna figura delictiva dedicada a proteger un bien jurídico así.

Tal como aparece concebida y formulada, la seguridad informática no tiene aún, a mi juicio, un contenido sustancial lo suficientemente elaborado y preciso como para permitir una construcción certera de la tutela penal. Prueba de ello es que unas veces se la relaciona con el honor, el patrimonio y la intimidad, y otras, además, con la libertad de información, el secreto de las comunicaciones, la libertad de expresión, etcétera, lo que dice bastante de la ambigüedad del concepto. Sin que se vea bien la razón, por otra parte, de que no guarde también relación con la salud pública, la indemnidad sexual, el interés fiscal del Estado, etcétera, en la medida en que Internet sirve también para la realización de conductas ilícitas relacionadas con tales bienes jurídicos.

Y si no está bien definido el objeto de ataque, se hace difícil identificar las conductas agresivas que comportan un riesgo para el mismo y que deberían, por tanto, prohibirse (¿el acceso no autorizado?; ¿la destrucción?; ¿la perturbación del uso?; ¿con cualquier finalidad?,

etc.). Sobre todo, si se tiene en cuenta que alguna de las conductas que eventualmente habrían de prohibirse en el tipo penal que se estableciera para la protección de la seguridad informática, pueden estar integrando ya modalidades delictivas relacionadas con la protección de bienes jurídicos «tradicionales» de naturaleza personal. La incorporación al ámbito de la protección penal de un bien así, necesitaría, por tanto, revisar los términos de la protección que actualmente se presta en el Código Penal a bienes jurídicos personales, en relación con comportamientos que se producen en Internet o con medios o procedimientos informáticos

Lo que confirma que siempre que se plantea la eventual protección de un bien jurídico nuevo, la pregunta decisiva es otra; a saber: ¿es realmente necesaria la creación de un bien jurídico colectivo como la seguridad informática para lograr la tutela efectiva de los bienes jurídicos personales que pueden verse lesionados o puestos en peligro con las conductas que tratan de evitarse con el reconocimiento del mismo?; ¿la tutela de la seguridad informática ofrecería realmente ventajas sustanciales respecto de la que ahora puede lograrse sin el reconocimiento de un bien jurídico así?

Uno de los ejemplos que se ha puesto para apoyar la conveniencia de proteger la seguridad informática es lograr una punición eficaz de los virus informáticos (PICOTTI, entre otros). Sin embargo, la posibilidad de castigar la simple distribución de los mismos a través de Internet no pasa, a mi juicio, por el necesario e ineludible reconocimiento de la seguridad informática como bien jurídico desde el que contemplar la punición de esos comportamientos.

De hecho, tal anticipación de la tutela es perfectamente posible incluso si el comportamiento se plantea desde la perspectiva de la protección del patrimonio o, incluso, en relación con algunas variantes de los mismos, desde la protección de la intimidad (programas espías —*spyware, sniffers*—, por ejemplo). Baste recordar, a estos efectos, por ejemplo, que el artículo 270.3 castiga ya en el derecho español la mera fabricación, importación, puesta en circulación o tenencia de medios específicamente destinados a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualesquiera otras obras protegidas (GÓMEZ MARTÍN, 2002). Y ello, tomando como referente de la protección simplemente los derechos de propiedad intelectual del autor.

Otro tanto puede decirse, por ejemplo, del artículo 248.3, que ha ampliado la calificación de estafa a la fabricación, introducción, posesión o facilitación de programas de ordenador específicamente destinados a

la comisión de las mismas. Sin pretender hacer ahora una calificación definitiva de supuestos cuya eventual inclusión en el artículo 248.3 requiere muchos matices, lo cierto es que el precepto puede permitir ya la inclusión de variantes de los virus de finalidad defraudatoria, como los lectores de teclado que permiten obtener claves de usuario, contraseñas o números de tarjetas de crédito (*keylloggers*); de las rutinas manipuladoras de direcciones, que, con semejante finalidad, redirigen al usuario a una página falsa, de apariencia igual a aquélla en la que pretendía acceder (*pharming*); de los programas telefónicos fraudulentos, que redirigen las comunicaciones a números de pago (*dialers*) y supuestos similares.

Otro tanto podría decirse en el derecho español en relación con el intrusismo informático (*hacking*), en donde, desde la perspectiva de la protección de la intimidad, no ha habido inconveniente alguno para que pueda considerarse ya constitutivo de delito por el artículo 197.1 el simple «apoderamiento» (entendido, a estos efectos, en sentido de captación intelectual) de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, realizado con el propósito de descubrir los secretos o vulnerar la intimidad de otro, aunque no llegue a lograrse materialmente el acceso al secreto o la información reservada que los mismos contienen (V. González Rus, 2004). Resultado que, se insiste en ello, puede alcanzarse desde la perspectiva de la protección de la intimidad, sin necesidad de recurrir a la creación de un bien jurídico informático específico.

Lo decisivo para la punición de comportamientos de este tipo no es solo, pues, el bien jurídico que se tome como referencia, cuanto la cuestión de determinar el momento a partir del cual y cómo debe producirse la intervención penal. En todo caso, el logro de una tutela eficaz ante los peligros que suponen comportamientos realizados en Internet no pasa necesariamente por el reconocimiento de un bien jurídico «nuevo» como la seguridad informática, sino que puede lograrse también adelantando el momento de la protección de otros como la intimidad o el patrimonio; lo que a mi juicio resulta, como expondré a continuación, más ventajoso desde el punto de vista político-criminal.

B) Sobre el concepto y necesidad de protección de la integridad y disponibilidad de los datos como «nuevo» bien jurídico informático

Semejantes consideraciones pueden hacerse en torno a la necesidad de reconocer a la integridad y disponibilidad de los datos informáticos como un «nuevo» bien jurídico. Ni, a mi juicio, puede interpretarse el artículo 264.2 como una figura delictiva dedicada a la protección de ese

bien jurídico, sino que se trata de una modalidad específica de daños (v. González Rus, 2002 y 2004; así también Mata y Martín, Matellanes Rodríguez Valdecabres Ortiz).

Como ya tuve ocasión de exponer al ocuparme específicamente de esta cuestión, creo que no es posible considerar al artículo 264.2 como un delito contra la integridad o la libre disponibilidad de los datos, porque ello provoca conclusiones interpretativas poco satisfactorias.

Fundamentalmente, porque entendiendo que la protección penal se asienta en la existencia y valor del dato en cuanto tal, que se declara «indemne» al margen de su significación económica y de su contenido, se desbordarían los límites de una intervención penal razonable en este ámbito, puesto que obligaría a entender que el art. 264.2 considera constitutiva de delito la destrucción de cualquier fichero informático, cualquiera que sea su contenido o cualquiera que sea su valor. Delito, por cierto, que está castigado con la pena de uno a tres años de prisión y multa de doce a veinticuatro meses, lo que puede hacer que surjan problemas desde el punto de vista de la proporcionalidad.

Conforme a una fundamentación de este tipo, además, tampoco sería posible limitar el ámbito típico del artículo 264.2 exigiendo la cuantía superior a 400 € que se reclama para los daños, pues ello supondría introducir un elemento, el del valor económico, absolutamente impertinente en una figura delictiva cuyo fundamento habría de ser, precisamente, proteger los datos, con independencia de su significación económica. Como contrapartida, la irrelevancia típica de la cuantía económica provocaría para los supuestos contemplados en el art. 264.2 la impunidad de los comportamientos imprudentes, prevista con carácter general, sin embargo, para los daños, en el artículo 267, cuando la cuantía de los mismos sea superior a 80.000 €.

Por añadidura, un entendimiento de este tipo tendría que justificar qué particularidad tienen los datos o los documentos electrónicos respecto de otros soportes susceptibles de protección penal y que sea capaz de justificar que deba protegerse su integridad o libre disponibilidad, al margen de su valor económico o de su contenido. Desde luego, desde la óptica de la propiedad, que es en donde está situado el artículo 264.2, un tipo delictivo que prescinda por completo del valor económico de los datos no tiene sentido alguno. Patrimonialmente hablando, los factores que cobran relevancia en orden a una eventual intervención penal son, o el valor económico del objeto material del delito, o el perjuicio que puede provocarse al propietario con la realización de la conducta típica, y ni una ni otra dimensión tendrían cabida en un delito que tuviera como única finalidad proteger la integridad de los datos en sí, al margen de su contenido o significación económica. Por tanto, un tipo que prescinde

de ambos elementos tiene que residenciar el valor protegible de los datos en alguna otra circunstancia.

La superior importancia de los datos y elementos lógicos sobre los físicos podría pensarse que se encuentra en que constituyen una especie de «creación intelectual», lo que les conferiría mayor valor que el que tienen las cosas puramente físicas. De ser así, ello obligaría a reclamar en los datos y documentos electrónicos susceptibles de protección penal un cierto contenido, que para nada sugiere, en cambio, la letra del 264.2. En todo caso, prueba de que tampoco ésta es una dimensión que haya tomado en cuenta el artículo 264.2 es, de una parte, que si los datos que dan contenido al fichero electrónico estuvieran impresos en un papel, su destrucción no daría lugar a modalidad agravada alguna, aun incorporando el objeto destruido idéntico contenido creativo; de otra, que no puede olvidarse que el fichero de datos puede ser el resultado de una operación de procesamiento llevado a cabo directamente por el ordenador al ejecutar una aplicación, lo que los convertiría en algo que tiene que ver con el resultado de un proceso mecánico o electrónico y no con creación intelectual alguna.

Otra razón eventualmente utilizable para justificar la creación de un tipo dirigido a proteger la integridad de los datos podría ser la mayor vulnerabilidad de los mismos ante determinadas conductas dañosas realizadas a través de redes de transmisión de datos y en particular de Internet. La especial peligrosidad de estos procedimientos, ante los que los sistemas informáticos y los datos ofrecerían una gran fragilidad, podría ser, pues, otra de las razones político-criminales eventualmente esgrimibles a la hora de justificar la necesidad de una figura delictiva de este tenor.

Una visión así, empero, no se corresponde tampoco con el sentido del art. 264.2. En primer lugar, porque en él se comprenden también supuestos en los que el ataque se produce también por procedimientos no informáticos y no aparece circunscrito, por tanto, a los daños que se causan como consecuencia de accesos ilícitos a sistemas provenientes de Internet o de redes de transmisión de datos. El propio artículo resalta esa vocación generalista de la conducta al insistir por partida doble en que se castigan los daños que se produzcan «por cualquier medio» o «de cualquier otro modo», poniendo de relieve su voluntad de no restringir en modo alguno la tipicidad de las posibles conductas dañosas a los ataques estrictamente informáticos y menos a los que provengan exclusivamente o se produzcan a través o desde Internet o redes de transmisión de datos.

Como consecuencia, no creo, como ya anticipaba, que el artículo 264.2 pueda ser interpretado como un delito dirigido a la protección de los datos. De hecho, de buscar paralelismos, incluso podría conside-

rarse una figura más próxima a la postulada «seguridad informática», que a la propia integridad de los datos. En el derecho español no hay, por tanto, a mi juicio, ninguna figura de delito que tenga por contenido sustancial la integridad o incolumidad de los datos.

De todas formas, como antes, la cuestión sigue siendo otra: ¿es verdaderamente necesario individuar un bien jurídico de naturaleza informática como éste para lograr la tutela pretendida? A mi juicio, como ya he puesto de manifiesto en relación con la seguridad informática —y a salvo lo que se diga más adelante sobre la situación en el derecho español—, ello no es necesariamente así.

C) Sobre la libertad informática

Distinto es, en cambio, el caso de la llamada libertad informática, cuyo contenido y significación aparecen directamente ligados a los datos de carácter personal y, muy particularmente, a la explotación de los mismos mediante bases de datos y procesamiento electrónico.

En el derecho español, la referencia sustancial básica de este hoy reconocido ya como derecho fundamental se encuentra en el art. 18.4 del texto constitucional, en donde se hace expresa alusión a que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos» (v. Morales Prats, Ruiz Marco). Lo que, con el relieve adquirido por los datos de carácter personal, ha obligado a una evolución del ámbito de protección de lo relacionado con la intimidad, que ha pasado de la tutela del clásico derecho «a estar solo», hasta incluir el derecho a controlar la información que los demás tienen sobre los datos relativos a nuestra persona y a nuestra vida personal y familiar y el uso que hacen de ella.

De un sentido estrictamente «negativo», que centra la protección en el «derecho a ser dejado en paz», y que viene a reconocer el derecho de la persona a decidir a quién dará a conocer y a quién no datos que afectan a su vida personal y familiar, a quién introduce en el ámbito de lo que le resulta más íntimo y esencial y a quién no, y que se materializa en la protección frente a intromisiones ajenas en ese espacio tan esencial para el desarrollo de su personalidad, se ha pasado a una situación —es evidente que obligada en buena medida por el desarrollo de las nuevas tecnologías—, en la que se reconoce y tutela, además el derecho del ciudadano a conocer y controlar la información que los demás poseen sobre él.

Éste es el sentido último del artículo 18.4 CE, del que se deriva un poder de acción para exigir que determinados datos personales no sean

conocidos, lo que supone reconocer un derecho a la autodeterminación informativa, entendido como libertad de decidir qué datos personales pueden ser obtenidos y tratados. La llamada libertad informática significa, pues, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente (*habeas data*); en particular, entre otros aspectos, la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (v. Muñoz Machado, Álvarez-Cienfuegos Suárez, por todos).

Esta evolución del concepto de intimidad ha sido perfectamente apreciable en la jurisprudencia del Tribunal Constitucional. En un primer momento, la intimidad se configura como el derecho del titular a exigir la no injerencia de terceros en la esfera privada, concibiéndola, pues, como un derecho de corte garantista o de defensa. En un segundo momento, que algunos cifran fundamentalmente en la STC 134/1999, 15 de julio, la intimidad pasa a ser concebida como un bien jurídico que se relaciona con la libertad de acción del sujeto, con las facultades positivas de actuación para controlar la información relativa a su persona y su familia en el ámbito público: «El derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros, sean estos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información, prohibiendo su difusión no consentida» (SSTC 134/1999, 15 de julio y 144/1999, 22 de julio).

Con mayor rotundidad aún la libertad informática se reconoce como derecho fundamental en la STC 292/2000, 30 de noviembre, en donde directamente se proclama que «el derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado» (FJ 6). «El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal» (FJ 6). La peculiaridad que lo diferencia de otros derechos fundamentales es que «el derecho a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos… que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo

es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de sus datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales» (FJ 6).

El derecho fundamental a la protección de datos «faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede ese tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y usos» (FJ 7).

La protección penal de este derecho se hace en el articulo 197.2 del Código Penal, que no limita la protección de los datos reservados de carácter personal a los que estén registrados en ficheros informáticos, electrónicos o telemáticos, sino que, por el contrario, extiende la tutela de los mismos a cualesquiera otros que se hallen registrados en cualquier tipo de archivo o registro público o privado, incluso si su procedimiento de confección y explotación es manual. En este sentido, esta dimensión de la intimidad se describe más correctamente con las expresiones «derecho a la protección de datos personales», *habeas data* o «derecho a la autodeterminación informativa», que con la referencia a la «libertad informática», en la medida en que ésta sugiere una vinculación (necesaria y limitativa) con los medios de explotación y configuración informáticos, electrónicos o telemáticos, que no es exacta, dado que esos soportes y esos procedimientos de confección y explotación constituyen sólo una parte (esencial, sin duda) de lo que resulta penalmente protegido.

Este es, por tanto, el único bien genuinamente informático que ha consolidado como derecho fundamental la generalización de los medios y procedimientos informáticos y telemáticos y que encuentra tutela en el Código Penal.

III. **Posición personal**

1. *Aplicación a Internet y a las redes de transmisión de datos de los criterios político-criminales que rigen en el espacio social general*

En la definición de los términos de la intervención penal en relación con los comportamientos que se producen en Internet y en redes de transmisión de datos —en definitiva, en la determinación de qué bienes jurídicos deben ser protegidos y ante qué tipo de ataques—, el criterio político-criminal básico que ha de seguirse es el de respetar en la mayor medida en que ello sea posible el criterio de la «identidad de valoraciones» e «identidad de desvaloraciones».

O, dicho en términos formales: que lo que es penalmente impune fuera de Internet debe serlo también en Internet, y, a la inversa, que lo que se considera penalmente sancionable fuera de Internet debe serlo también en Internet. Internet no es sino un espacio, un instrumento de comunicación interpersonal y social más y, por tanto, deben regir en él los mismos o semejantes criterios de valoración y de actuación que están vigentes en el espacio social general en el que se inscribe. Entre el mundo «virtual» y el mundo «real», por decir así, no puede haber fracturas valorativas, sino continuidad, coherencia. En definitiva: que la valoración de los objetos jurídicos de protección y la de los comportamientos lesivos de los mismos debe hacerse en sede de informática e Internet en términos semejantes a la valoración que tales intereses y conductas reciben cuando la protección se produce fuera de Internet.

Por mi parte, no veo que la naturaleza del medio en el que se produce un hecho tenga que suponer necesariamente una transformación tan sustancial de las necesidades y posibilidades de tutela como para reclamar como única vía de protección eficaz la aparición de nuevos bienes jurídicos y de previsiones penales específicas. La aparición de nuevos medios, procedimientos o escenarios de desarrollo personal y social, pueden alterar sustancialmente las formas de agresión a los derechos e intereses individuales y sociales, pudiendo hacer surgir formas de ataque hasta ese momento inéditas que pueden comportar, efectivamente, significativas revisiones del concepto de un bien jurídico, capaces de provocar la incorporación de nuevos contenidos que vengan a complementar su sentido originario. Así ha ocurrido, por ejemplo, como se ha visto, con la libertad informática y la intimidad.

Sin embargo, tal posibilidad no puede convertirse sin más en el criterio político-criminal general que presida la intervención penal en relación con Internet y las redes de transmisión de datos, presumiendo en todo caso la necesidad de reconocer bienes jurídicos «nuevos», sea por vía de

aparición *ex novo*, sea por «transformación» de los ya tutelados; con la correlativa secuela de necesitar una protección específica, diferenciada de la que reciben los bienes jurídicos semejantes, cuando el ataque se produce fuera de Internet o al margen de los medios o procedimientos informáticos.

El contenido y significación de un bien jurídico no cambia de forma tan automática como se pretende, por el simple hecho de que varíe la forma de ataque o el objeto material en el que eventualmente se sustancia el mismo. El contenido del bien jurídico vida, por ejemplo, no cambia simplemente porque aparezcan nuevas formas de agresión al mismo. Es evidente que las nuevas técnicas de investigación y manipulación genética, por ejemplo, pueden hacer surgir formas de ataque hasta hace poco inéditas, que hagan conveniente la previsión de figuras delictivas nuevas; pero ello no significa entender que lo que se está protegiendo en ese caso sea un bien jurídico distinto de la propia vida. Trasladado al tema que nos ocupa, ello supone mantener que las nuevas formas de ataque que propician los medios y procedimientos informáticos y las telecomunicaciones pueden determinar, efectivamente, la conveniencia de adelantar el momento de la intervención penal o incluso dar lugar a figuras pluriofensivas, pero no tienen por qué significar de forma inevitable, como con tanto énfasis sostiene Picotti, la aparición de un nuevo y distinto bien jurídico.

Tampoco la aparición de nuevos objetos materiales obliga a entender que se produce esa inevitable y radical «transformación» del bien jurídico. La multiplicación de soportes o de sustratos fácticos en los que puede materializarse un bien jurídico no determina necesariamente un cambio en el sentido y significación de aquél. Que junto al documento tradicional, en papel, aparezca el documento informático, no es óbice para que cambie el sentido como bienes jurídicos de la fe pública o de la seguridad del tráfico jurídico. Que las nuevas tecnologías abran nuevas formas de explotación y de agresión a la propiedad intelectual no tiene por qué significar necesariamente una mutación de ese bien jurídico; más aún, la definición legal de la propiedad intelectual deja su contenido abierto a la incorporación de las nuevas posibilidades de explotación que puedan ofrecerse en el futuro; pero, en todo caso, la naturaleza de la propiedad intelectual sigue siendo la del reconocimiento de un derecho de exclusiva sobre una creación, al margen de que varíe la forma de manifestación de esa creación. Ni el soporte ni la forma de ataque, pues, definen necesariamente el bien jurídico ni tienen por qué suponer inevitablemente una transformación esencial de su sentido. Pueden producirla, sin duda, y ya hemos visto que eso ocurre, pero esa modificación deberá ser probada y no simplemente presumida o aceptada como consecuencia ineludible impuesta por la novedad del medio.

La consecuencia que acaba teniendo este tipo de posiciones, que reclaman una intervención diferenciada y específica para atender las demandas punitivas derivadas de Internet, es una ampliación del campo de la intervención penal más allá de lo que se establece para esos mismos intereses y bienes jurídicos frente a los ataques que se causan fuera de Internet. De tal forma, que lo que acaba por producirse es un desequilibrio en la protección de bienes jurídicos semejantes, en función de que el ataque se produzca en Internet o fuera de él. Una protección asimétrica, pues, en función del entorno en el que se produce la agresión. En estos casos, lo que ocurre en realidad es que Internet y las nuevas tecnologías se convierten en la razón —o en el pretexto— para una ampliación del campo de la intervención penal, más allá de lo que aconsejarían los principios de subsidiariedad, carácter fragmentario y proporcionalidad.

El castigo, por ejemplo, de la simple perturbación del uso de un sistema informático, supone de hecho una ampliación sustancial de los términos de castigo de las infracciones de uso en el derecho español, que siempre han sido tratadas con criterios restrictivos en el Derecho Penal patrimonial. La necesidad de revisar ese criterio político-criminal, que personalmente me sigue pareciendo asumible como postulado general, debería pasar por la justificación detallada y convincente de que el medio informático o Internet introducen circunstancias de la suficiente importancia como para reconsiderarlo en relación con los ilícitos informáticos.

A mi juicio, lo que debe decidirse en tesituras como ésta, en las que debe resolverse sobre la necesidad de individuar uno o varios bienes jurídicos «nuevos», y sobre la oportunidad de crear uno o varios delitos también «específicos» relacionados con los mismos, es si ello resulta verdaderamente necesario. En otras palabras: en este caso se trata de decidir —sin entusiasmos apriorísticos provocados por el interés y la novedad de una materia, por ejemplo— si la protección que reciben los bienes jurídicos personales y/o generales y colectivos eventualmente afectados por los comportamientos que se producen en Internet y/o en relación con medios o procedimientos informáticos, es suficiente o no.

Como consecuencia, la pregunta central en esta cuestión es si la informática e Internet suponen factores de peligro adicional para los derechos e intereses individuales y sociales que no estén cubiertos (y que no puedan ser cubiertos) con la aplicación (y, eventualmente, con la complementación y ampliación) de las figuras delictivas actualmente disponibles dirigidas a la protección de bienes jurídicos personales, colectivos y generales. Sólo a partir de ahí podrá determinarse si es necesaria para la tutela de los bienes e intereses implicados en las redes de transmisión de datos e Internet la creación de «nuevos» bienes jurídicos específicos, de naturaleza informática.

2. *Delimitación de las necesidades de tutela derivadas de los medios informáticos, en particular de Internet*

La determinación de si actualmente están suficientemente cubiertas las necesidades de tutela de los bienes jurídicos dignos de protección penal ante las amenazas provenientes de Internet y de las redes de transmisión de datos, pasa necesariamente por la identificación concreta de los peligros «nuevos» que suponen los procedimientos informáticos y telemáticos. A mi juicio, los «nuevos» riesgos que supone Internet son básicamente tres:

1) En primer lugar, el comportamiento realizado en Internet puede suponer una lesión más «intensa» y/o «extensa» del bien jurídico. Los genéricamente llamados «delitos informáticos» pueden suponer, en efecto, incrementar y multiplicar los efectos lesivos del bien jurídico que producen los delitos «tradicionales». Por citar sólo dos ejemplos, un escrito injurioso difundido a través de un único correo electrónico o insertándolo en una página web puede llegar a ser conocido por miles, incluso millones de personas; un virus informático puede llegar a infectar millones de ordenadores, afectando a millones de usuarios, posibilidad que es poco factible cuando el delito se comete por procedimientos no informáticos.
2) Internet ha supuesto también la aparición de nuevos soportes y elementos, que, en cuanto relacionados con las nuevas tecnologías, con los procedimientos informáticos o la transmisión de datos, hace poco ni siquiera existían y, por tanto, no podían gozar de protección. Así ocurre, por ejemplo, con los correos electrónicos, los documentos electrónicos, los programas de ordenador, las bases electrónicas de datos, etc., que pueden ser, sin embargo, soporte de bienes jurídicos fundamentales y eventual objeto de ataque.
3) Internet ha hecho aparecer también nuevas formas de atentar contra intereses individuales y sociales, adaptadas al medio informático. Así, por ejemplo, las transferencias electrónicas de fondos, el uso de tarjetas, el intrusismo informático, el acceso no autorizado a bancos de datos, etc.

Pues bien, la cuestión es: para contemplar esas nuevas necesidades de protección ¿es obligado recurrir a la creación de bienes jurídicos nuevos o, por el contrario, sería suficiente con reforzar y complementar la tutela que actualmente prestan los tipos penales disponibles? ¿Qué es político-criminalmente más conveniente?

A) Superior dimensión lesiva de los delitos informáticos

En lo que hace a la primera característica apuntada, ni siquiera esa eventual superior dimensión lesiva de los ilícitos informáticos constituye una novedad atribuible ni en exclusiva ni por primera vez a Internet, pues se trata de efectos conocidos y resueltos ya por el Derecho Penal en ámbitos «tradicionales», ajenos al informático. Un efecto semejante producen, por seguir con uno de los ejemplos propuestos, los atentados al honor que se cometan a través de televisión, periódicos de amplia tirada, radios, revistas y medios de comunicación en general, que pueden producir un efecto lesivo semejante. Y lo mismo podría decirse, en relación con los daños y los virus informáticos, cuya principal particularidad de ser capaces de afectar a un muy elevado número de sujetos, tampoco resulta nueva en el Derecho Penal, que tiene resueltos ya problemas así, por ejemplo, en el ámbito de los consumidores.

La realización de la conducta delictiva en Internet, por tanto, puede efectivamente suponer un mayor desvalor de acción o de resultado, o la ampliación y multiplicación del peligro o de la lesión propia del delito, hasta alcanzar a un número muy elevado de sujetos y unas dimensiones de gran envergadura. Pero desde el punto de vista de técnica penal, sin embargo, ello no constituye novedad alguna suficiente como para justificar la aparición de bienes jurídicos «nuevos» y la creación de específicas figuras de delito.

En el Derecho Penal moderno, para afrontar situaciones como ésa basta con crear tipos agravados que tomen en cuenta esa superior capacidad lesiva, incrementando la pena en la proporción que resulte adecuada. Por ejemplo, que el hecho revista especial gravedad, atendido el valor de la defraudación, la entidad del perjuicio o el número de perjudicados, etc.; eventualidad prevista, como no es necesario recordar ahora, en un buen número de figuras delictivas. Semejante recurso podría servir —más exactamente: debería servir— igualmente aquí para contemplar esta «novedad» de Internet.

B) Creación de nuevos objetos materiales del delito

Tampoco la aparición de nuevos objetos materiales del delito creados por la informática e Internet es capaz de justificar la aparición de bienes jurídicos «nuevos».

La aparición del correo electrónico, de los documentos electrónicos, de los programas de ordenador, de las transmisiones de datos, etc., adquieren relevancia social, y por tanto penal, en la medida en que constituyen el soporte en el que se materializan, contienen o expresan de-

rechos e intereses individuales y sociales; en definitiva, bienes jurídicos. La naturaleza de estos bienes jurídicos, a cuyo servicio se ponen, y no necesariamente el medio o la forma en la que se produce la agresión, es, pues, la que debe decidir los términos de la protección penal. La tutela que venía prestándose a los bienes jurídicos que se manifiestan ahora en esos nuevos soportes o procedimientos, debe extenderse también a éstos, lo que puede lograrse por el simple expediente de incluirlos dentro de la descripción de los eventuales objetos materiales de las correspondientes figuras delictivas. Como, por lo demás, así ha hecho el legislador español en las figuras delictivas en las que ello ha sido necesario.

A título de mero ejemplo, baste recordar aquí la inclusión de las referencias a los mensajes de correo electrónico, en el artículo 197.1; la previsión concreta del ataque a los datos de carácter personal o familiar registrados en ficheros o soportes informáticos, electrónicos o telemáticos, del art. 197.2; la mención de los datos, programas o documentos electrónicos y las referencias a redes, soportes o sistemas informáticos, del art. 264.2; las previsiones relativas a los programas de ordenador, del artículo 270.3 o la mención de los documentos electrónicos, soportes informáticos, en el artículo 278, relativo al descubrimiento de secretos de empresa. Evidencia, por tanto, de que pueden cubrirse las necesidades de tutela conectadas a los medios informáticos y a Internet sin necesidad de la individualización de bienes jurídicos nuevos.

En relación a los objetos materiales de naturaleza informática, debe resaltarse la importancia extraordinaria que adquiere en ellos la información, como aspecto central a considerar en la tutela que se disponga. Ese valor inmaterial constituido por la información, pasa a menudo a integrarse como elemento esencial definidor de la propia tutela penal en determinadas figuras delictivas, determinando, por ejemplo, que el valor de la cosa relevante a efectos de daños corresponda al de la información contenida en el mismo, por encima del que tiene el soporte físico en el que se contiene. En ocasiones, incluso, el soporte físico puede tener un valor inapreciable en cuanto tal y alcanzar, sin embargo, por su contenido, un alto valor económico, que será a la postre el que decida la entidad de la responsabilidad penal.

Tampoco esta particularidad, empero, constituye una novedad de la informática. Baste recordar ahora, por sólo citar un caso, que eso mismo ocurre en los objetos con valor histórico o artístico, pinturas, esculturas, etc. en los que el valor de la cosa no lo determina tanto la componente material en sí, sino el valor que le otorga la dimensión de bien cultural. Lo mismo que sucede en los títulos al portador, títulos valores, etc., en donde lo relevante para la protección penal no es el valor del objeto en sí, sino el del derecho o cualidad inmaterial que incorpora o repre-

senta. También esta peculiaridad, por tanto, está resuelta por el Derecho Penal y debe ser abordada en Internet con los mismos parámetros que rigen fuera de la red.

Otra característica de los delitos informáticos es que frecuentemente será más costoso restablecer el sistema al estado en que se encontraba antes del ataque informático, que lo que suponga la pérdida de los ficheros, datos o elementos que constituyeron el objeto específico del ataque. Lo que aconseja recomendar como directriz político-criminal que en relación a los comportamientos informáticos se tome en cuenta para determinar la responsabilidad criminal, no tanto (o al menos no sólo) el valor económico del objeto material del delito, cuanto los perjuicios que pueden derivarse para el sujeto de la comisión del delito.

Piénsese, por ejemplo, en un virus informático que destruye numerosos ficheros cuyo valor material es, o puede ser, de escasa entidad; no obstante, los perjuicios que puede provocar la desaparición de los mismos o la restauración de las copias de seguridad que pudieran existir, puede significar unos perjuicios que serán a menudo muy elevados. Como fórmula intermedia podría adoptarse la que ya sigue el legislador en delitos contra el patrimonio, como por ejemplo el hurto o los mismos daños, en donde la responsabilidad criminal básica se determina en atención a la cuantía del objeto material (más de 400 euros, artículo 234 o 263), mientras que la pena se agrava en consideración a la especial gravedad de los perjuicios producidos (artículo 235.3 y 264.1.5.º, respectivamente).

C) Aparición de nuevas formas comisivas

Finalmente, otro tanto ocurre en relación con las nuevas formas de comisión delictiva surgidas como consecuencia de las posibilidades de acción que ofrecen las nuevas tecnologías informáticas y de transmisión de datos. Una vez más, se trata aquí de «nuevas» formas de expresión de atentados a bienes jurídicos ya conocidos, fundamentalmente el patrimonio y la intimidad. Las particularidades de las formas de comisión electrónica hacen necesaria, sin embargo, la previsión de tipos derivados específicos, dentro del marco genérico de la protección prestada al bien jurídico lesionado y al servicio de los propósitos político-criminales que inspiren la protección de éste.

Así ha ocurrido, por ejemplo, en la «estafa informática» del artículo 248.2, que viniera a salvar la laguna de punición que planteaba la imposibilidad de configurar en las transferencias electrónicas de fondos el engaño característico del delito de estafa. El bien jurídico protegido, sin embargo, sigue siendo el patrimonio, y la naturaleza del comporta-

miento —aún con matices— el de las defraudaciones, sin que la peculiaridad evidente del procedimiento informático que constituye el medio comisivo haya obligado a una tutela diferenciada, basada en técnicas y valoraciones distintas a las que se siguen en las demás modalidades de estafa. A la postre, lo que importa es la entidad el perjuicio causado al titular del patrimonio; hasta el punto de que el legislador español ha considerado que la utilización de medios y procedimientos informáticos no comporta un suplementario desvalor de acción capaz de configurar un tipo cualificado de estafa semejante a los que se recogen en el artículo 250.

Como consecuencia, también las necesidades de punición que pueden plantear las formas comisivas inéditas, susceptibles de producirse en Internet y en redes de transmisión de datos, pueden ser resueltas con y desde las figuras de delito «tradicionales» actualmente disponibles; sin perjuicio, naturalmente, de que en ocasiones resulte preciso complementar los actuales tipos con previsiones nuevas.

IV. **Conclusión: la vía de la utilización y complementación de las figuras delictivas actualmente disponibles, como opción político-criminal más conveniente**

A la vista de lo expuesto, puede concluirse afirmando que las «demandas punitivas» de Internet pueden solventarse, respectivamente: bien mediante la creación de tipos agravados o circunstancias cualificadoras que tomen en cuenta el incremento del desvalor de acción o de resultado de figuras de delito ya existentes; bien ampliando la protección penal a los nuevos elementos o soportes que pueden resultar eventuales objetos materiales de delitos ya también previstos y castigados; bien, considerando punibles particulares formas de conducta lesivas de bienes jurídicos, asimismo ya contemplados y tutelados penalmente.

La solución político-criminal y técnica más conveniente para dar respuesta penal a las necesidades de tutela surgidas del desarrollo de la informática, Internet y las redes de transmisión de datos, resulta pues, a mi juicio, la de complementar, en los términos que cada caso recomiende, las figuras de delito ya disponibles. De esta forma, en vez de incorporar bienes jurídicos informáticos «nuevos» y crear delitos específicos dirigidos a la protección de los mismos, resulta preferible abordar la punición de los llamados «delitos informáticos» desde las modalidades delictivas ya existentes; sin perjuicio de que, cuando resulte necesario, se complementen los tipos existentes con previsiones fundadas en los aspectos particulares que caracterizan a los medios o procedimientos in-

formáticos. Sólo cuando haya una verdadera «laguna» de punición (en el sentido de que ninguno de los bienes jurídicos ya protegidos penalmente es capaz de cubrir adecuadamente la demanda de protección surgida en relación con el uso de medios, procedimientos informáticos o redes), estará justificada la incorporación de un bien jurídico «nuevo», como ha ocurrido, por ejemplo, con el derecho a la protección de datos personales.

Esta vía de la complementación de la figuras delictivas existentes fue adoptada finalmente por el Código Penal español de 1995 y es la mayoritaria en el derecho comparado. Salvo el caso de Portugal, que incluyó todas las disposiciones de naturaleza informática en una ley especial, y el francés, que alojó todos los delitos de esta naturaleza en un título propio del Código de 1994[1], éste ha sido el modelo seguido también en Alemania[2], Italia, Austria —a partir de la ley de 1987—, y Suiza —desde la reforma de 1993—, que optaron por incluir las figuras delictivas relacionadas con la informática junto a las figuras de delito tradicionales con las que guardaban mayor relación.

Esta forma de proceder, además, ofrece importantes ventajas a la hora de interpretar y aplicar las figuras penales o los elementos del tipo de naturaleza informática que puedan incorporarse, en la medida en que se insertan en una figura de delito cuyo sentido y particularidades está previamente delimitado por doctrina y jurisprudencia. De esta forma, se asegura la homogeneidad de los criterios valorativos que se apliquen en Internet y fuera de Internet, se facilita la interpretación y aplicación de los delitos (permitiendo aprovechar la experiencia y las aportaciones de doctrina, tribunales y operadores jurídicos), y se potencia su vinculación con el bien jurídico protegido en las mismas. Lo que sirve, además, para reforzar la legitimidad de las previsiones penales de naturaleza informática y de las penas establecidas para los comportamientos delictivos de esta naturaleza.

Debo advertir también —para que se comprendan mejor mis reservas a la creación de bienes jurídicos «nuevos»—, que personalmente no sigo con entusiasmo alguno la pasión desatada a favor de la creación

---

[1] Arts. 323.1 a 323.7: atentados a los sistemas de tratamiento automatizado de datos, dejando fuera únicamente la falsedad informática, que se incluyen dentro de las falsedades documentales, artículo 441.1.

[2] Así, a partir de la reforma de 1986: § 202a, sobre el espionaje de datos, junto al § 202, en donde se incluye la violación de domicilio y de la intimidad en las comunicaciones; en el § 263a, el fraude informático, junto a la estafa común, en el § 263; la falsedad informática del § 269, junto a las falsedades documentales del § 267; y el daño a datos y el sabotaje informático del § 303a y 303b, junto a los daños del § 303; todos ellos del Código Penal alemán.

de delitos de peligro dirigidos a proteger bienes jurídicos colectivos de nueva creación, que surgen con una fecundidad admirable, y que nos introducen en una dinámica que se corresponde mal con los tan celebrados y poco respetados principios de carácter fragmentario y *ultima ratio* del Derecho Penal. Sobre todo, cuando su creación no es indispensable para que queden adecuadamente salvaguardados los bienes jurídicos personales relacionados con ellos, pues su tutela está eficazmente asegurada sin la incorporación de tales bienes jurídicos y delitos específicos de naturaleza estrictamente informática.

Personalmente, como criterio político-criminal prefiero el de que los delitos de peligro se creen cuando no haya otra alternativa de punición eficaz, lo que, como acaba de verse, no ocurre en estos casos. Además, a mi juicio, el margen que se ofrece para la eventual creación de nuevos delitos de peligro es distinta cuando se trata de prestar protección mediata a bienes jurídicos personalísimos, que cuando ellos tiene que ver con bienes jurídicos patrimoniales o socioeconómicos, ámbito en el que no debería extenderse mucho más el campo de la protección que actualmente se presta.

A mi juicio, es preferible anticipar el momento de la protección de un bien jurídico individual bien caracterizado y de contenido y límites bien definidos, que crear un delito de peligro para un bien jurídico colectivo; y más si éste es «nuevo» y de perfiles difusos y sin concretar suficientemente. Peligro por peligro, me inclino por el primero. Por eso, puestos a elegir entre dos males, prefiero previsiones como la de los artículos 270.3 o 248.3 del Código Penal español, que adelantan la protección del bien jurídico al momento del peligro derivado de la realización de meros actos preparatorios, que la construcción de un delito de peligro para un bien jurídico colectivo como la seguridad informática, del artículo 615-*quarter* del Código Penal italiano, basado en la simple tenencia abusiva de códigos de acceso a sistemas informáticos o telemáticos, o en proporcionar indicaciones o instrucciones con ese objeto.

Bibliografía

AAVV, *Profili penali dell´informatica*, Milano, 1994.

AAVV, *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002.

Álvarez-Cienfuegos Suárez, «La libertad informática, un nuevo derecho fundamental en nuestra Constitución», en *La Ley*, n.º 5230, 2001.

Andrés Domínguez, *El delito de daños: consideraciones jurídico-políticas y dogmáticas*, Burgos, 1999.

Corcoy Bidasolo, «Protección penal del sabotaje informático. Especial consideración de los delitos de daños», en *La Ley,* 1990.

Fernández López, «La nueva regulación de la protección de datos personales en España a partir de la Ley Orgánica 15/1999, de 13 de diciembre», en *Ius & Law*, n.º 1 y 2, 2001.

Giannantonio, *Manuale di diritto dell´informatica*, 1994.

Gómez Martín, «La protección penal de los derechos de autor sobre los programas informáticos: un ejemplo de la naturaleza patrimonialista de los delitos contra la propiedad intelectual en el CP de 1995», en *Poder Judicial*, número 66.

Gómez Martín, «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3.º CP). A la vez, un estudio sobre los delitos de emprendimiento o preparación en el CP de 1995», en *Revista Electrónica de Ciencia Penal y Criminología*, 04-16, 2002.

González Rus, «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *RFDUCM*, Monográfico n.º 12, 1982.

González Rus, «Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos», en *Revista Electrónica de Derecho Penal y Criminología*, 01-14, 1999.

González Rus, «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (Artículo 264.2 del Código Penal)», en *La Ciencia del Derecho Penal ante el nuevo siglo. Libro Homenaje al Profesor Doctor Don José Cerezo Mir*, Madrid, 2002.

González Rus, 2004, «El *cracking*, los *virus*, la denegación de servicio y otras formas de sabotaje informático», en *Delincuencia Informática*, Plan de Formación Continuada, Centro de Estudios Jurídicos de la Administración de Justicia, Madrid, 2004.

Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código Penal», en *Ámbito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, Madrid, 1996.

Herrán Ortiz, *La violación de la intimidad en la protección de datos personales*, Madrid, 1999.

Marchena Gómez, «El sabotaje informático: entre los delitos de daños y desórdenes públicos», en *Actualidad Informática Aranzadi*, número 40, julio de 2001.

Mata y Martín, *Delincuencia informática y Derecho Penal*, Madrid 2001.

Morales Prats, «Internet: riesgo para la intimidad en Internet y Derecho penal», en AA.VV., *Internet y Derecho Penal,* Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002.

Morón Lerma, *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Pamplona, 1999.

Muñoz Machado, *La Regulación de la Red. Poder y Derecho en Internet*, Madrid, 2000.

Orts Berenguer / Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001.

PICOTTI, «Sistematica dei reati informatici, tecniche di formulacione legislativa e beni giuridici tutelati», en *Il diritto penale della´informatica nell´epoca di Internet*, a cura di Lorenzo PICOTTI, Padova, 2004.

RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, «Derecho Penal e Internet», en CREMADES/FERNÁNDEZ-ORDÓÑEZ/ILLESCAS, *Régimen Jurídico de Internet*, Ed. La Ley, Madrid s/f.

ROMEO CASABONA, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», en *Poder Judicial*, n.º 31, 1993.

ROMEO CASABONA, «La protección penal de la intimidad y de los datos personales en sistemas informáticos y en redes telemática (Internet)», en *Estudios Jurídicos. Ministerio Fiscal*. *La Delincuencia Informática,* Centro de Estudios de la Administración de Justicia, Madrid, III-2001.

ROMEO CASABONA, «La protección penal de la intimidad y de los datos personales: Los mensajes de correo electrónico y otras comunicaciones de carácter personal a través de Internet y problemas sobre la ley penal aplicable», en *Estudios Jurídicos. Ministerio Fiscal*. *La Delincuencia Informática,* Centro de Estudios de la Administración de Justicia, Madrid, II-2003.

RUÍZ CARRILLO, *Los datos de carácter personal*, Barcelona, 1999.

RUÍZ MARCO, *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*, Madrid, 2001.

ZÚÑIGA RODRÍGUEZ, MÉNDEZ RODRÍGUEZ, DIEGO DÍAZ-SANTOS (Coords.), *Derecho Penal, sociedad y nuevas tecnologías*, Madrid, 2001.

Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general

Norberto J. de la Mata Barranco
Titular de Derecho Penal. Universidad del País Vasco

I. Conductas que afectan al correcto desarrollo de los contextos digitales y delincuencia vinculada a las tecnologías de la información y la comunicación (delitos informáticos y cibernéticos)[1]

Es incuestionable que el desarrollo de las nuevas tecnologías de la información y de la comunicación y la imparable consolidación de los contextos digitales en nuestra sociedad actual han planteado, además de indudables ventajas que no cabe cuestionar, riesgos concretos para la correcta garantía de determinados intereses, que corresponde salvaguardar, en primer lugar, y es importante destacarlo ya de entrada, a quien se sirve o participa de ellos.

Lo es, asimismo, que el Derecho Penal, siempre como último eslabón de la cadena de tutelas jurídicas posibles, tiene capacidad —o se admite que la tiene— para dar cobertura —preventiva y sancionadora— a los intereses más importantes para una convivencia en que se ha de tratar de maximizar la libertad de todos quienes participan de ella evitando en la medida de lo posible la realización de las conductas que más gravemente puedan afectarlos.

Pero aunque ciertamente la digitalización del mundo empresarial, laboral, educativo e incluso doméstico ha favorecido la aparición de una serie de conductas que amenazan los intereses de quienes se mueven en estos contextos, profusamente destacadas en los medios de comunicación con una terminología de origen anglosajón que parece restringida a grupos de iniciados, se confunde en ocasiones lo que es la vulneración de determinados sistemas, la realización de conductas que afectan a

[1] Esta contribución forma parte del Trabajo realizado dentro del Cluster de Privacidad y Seguridad en desarrollo del Proyecto Etortek IE05-140 del Gobierno Vasco AmIGUNE.

los mismos, su utilización ilícita, etc., de carácter muchas veces inocuo —otras, no—, con lo que debe ser el campo de intervención no ya civil o administrativo, sino incluso penal, generándose a menudo cierto clima de alarma social —sólo a veces justificado— sobre la trascendencia de esas conductas, que tiende a favorecer el recurso a éste.

Estas conductas de riesgo y amenaza que acompañan el desarrollo de los contextos digitales —al margen de sensaciones de inseguridad, en ocasiones inexistente o exagerada, que pueden dificultar su aceptación, en el ámbito público o privado— y que, junto a razones económicas, pueden hacer desistir de su implantación, sólo cuando realmente vulneren intereses a los que presta o debe prestar atención el Derecho Penal pueden competer a éste.

Se alude en este ámbito, reiteradamente, a:

—la precipitación en el acceso a los sistemas digitales que, de modo imprudente favorece la causación de daños en los sistemas, un funcionamiento indebido de los mismos o incluso el acceso ilícito a ellos,

—la pérdida de privacidad por la acumulación de datos tanto en poder del gestor de los distintos sistemas como de aquellos a quienes se transmite la información que se posee y la confusión a veces entre lo público y lo privado cuando el sistema interconexiona distintos ámbitos de actuación individual,

—y, por supuesto, los propios déficits del sistema que impiden garantizar tanto su salvaguarda como la de los datos que contiene el mismo, favoreciendo su vulneración tanto externa como interna, ya sea en cuanto a la propia privacidad del contenido del sistema, ya en cuanto a la tutela de los derechos de gestión digital derivados o garantizados por el sistema, su propio funcionamiento en sí mismo considerado o el correcto desarrollo de los distintos entornos que permite el mismo para los fines que le son propios.

Son múltiples las posibilidades de ataques a bienes jurídicos tradicionales como la intimidad, el patrimonio o la propiedad intelectual e industrial a través de la informática y, con ella, de la cibernética; en particular, tras la emergencia y generalización de Internet. Pocas dimensiones de nuestra vida dejan de verse afectadas por los procesos digitales de tratamiento de datos, que incluso van a permitir la comisión, más fácil, de los delitos más clásicos (en la doctrina penal se alude al caso inglés de quien entra en los sistemas informáticos de un hospital para modificar el programa que organiza la distribución de la medicación de los enfermos, que sin duda daría lugar a un delito de asesinato en grado de tentativa), lo que afecta tanto a nuestro ámbito privado como profesional.

Y la referencia en la actualidad, incluso en el lenguaje común, a las expresiones «ataques *DOS*», «ataques a *botnets*», «ataques a *browser*», «ataques a *web sites*», difusión de «códigos maliciosos», «troyanos» o «virus» o a los términos, dentro del concepto genérico de *crimeware*, de *carding, cracking*, *cyberpunking*, *cybersquatting*, *hacking*, *pharming*, *phising*, *phreaking*, *sniffing*, *spamming, spyware* o *viring*, entre otros muchos, es, como digo, ya absolutamente habitual.

Ahora bien, una cosa es que las conductas a que hacen referencia todos estos términos puedan representar una quiebra para intereses del usuario o del gestor de los contextos digitales —en unas ocasiones absolutamente intrascendentes desde un punto de vista jurídico cuando se traducen en meras incomodidades, imposibilidad de uso inmediato del sistema, lentitud en el acceso o transmisión de datos, etc.; en otras, trascendentes, por ejemplo, por el perjuicio económico que genera la imposibilidad de utilización del sistema conforme a su potencialidad—, que habrán de tratar de combatirse desde lo que significa la securización de los contextos digitales, principalmente tecnológica (antivirus, cifrados, controles de acceso, controles de copia, cortafuegos, etiquetas de localización de productos, firmas digitales, protocolos de seguridad, sistemas de alerta basados en sensores, sistemas de detección de intrusos, sistemas de evitación de suplantación de identidad, sistemas de identificación incluso biométrica, técnicas de trazabilidad), informativa y formativa desde la perspectiva preventiva positiva y otra que estemos ante conductas que merezcan y necesiten atención por parte del Derecho Penal.

Téngase en cuenta, por otra parte, que a pesar de la trascendencia que se da a varias de ellas —a menudo, simplemente, por la a primera vista enigmática terminología que se utiliza— en realidad muchos de los conceptos que se utilizan en los contextos digitales son similares a los de la realidad más tradicional (archivos y datos reservados, cortafuegos, firmas falsas, llaves de acceso, usurpación de personalidad, etc.), que el mundo digital no difiere en lo sustancial del mundo real, ni en sus actores ni en sus interrelaciones ni en los entornos en los que se mueven y surgen unos y otras, sino que, al contrario, aquél lo que pretende es reproducir éste, claro está, de forma virtual y que, en consecuencia la respuesta a las mismas, penal o de otra índole, debe discurrir paralela a la que se ofrece prescindiendo del ámbito en que se producen; al menos, de entrada y sin perjuicio de que cuestiones como la dimensión del daño que permite la cibernética, por ejemplo, pueda obligar a determinadas matizaciones.

De hecho, en Derecho Penal el concepto de Derecho Penal informático, como acostumbra a señalarse, no hace referencia a una rama del

Derecho Penal como el Derecho Penal sexual, el Derecho Penal ambiental o el Derecho Penal de la Administración Pública nucleada en torno al interés objeto de tutela; es difícil concebir un delito informático como tal si por él hubiéramos de entender el delito contra la informática. Lo que puede existir es un Derecho Penal informático o relacionado con la informática como concepto que, con necesarias matizaciones, hace referencia a conductas típicas vinculadas, por el medio comisivo, el objeto del ataque, etc., al ámbito de la informática o de la cibernética, al ámbito del mundo digital. Pero obsérvese que hablamos de conductas típicas, al menos al margen de consideraciones político-criminales sobre posibles lagunas de penalidad que sea necesario cubrir.

Al Derecho Penal en definitiva lo que le interesa es, en primer lugar, si por muy compleja que sea toda esa terminología, por muy difícil que sea la comprensión de lo que realmente implica la conducta que se presenta como susceptible de lesionar el correcto desarrollo de los contextos digitales, la misma es o no susceptible de subsumirse en alguno de los tipos que, vigentes, se encuadran en la tutela de alguno de los intereses que se reconocen como merecedores y necesitados de intervención penal o debiera serlo porque afecta a estos del mismo modo y con similar intensidad a como lo hacen otras perfectamente subsumibles en ellos.

Por muy novedoso que sea el concepto de *cracker*, si en definitiva de lo que hablamos es de un delito de daños, habremos de acudir a los artículo 263 y siguientes para calificar esa conducta; obviamente podrá haber peculiaridades en el modo de ataque, en el objeto, que podrán dificultar la subsunción y exigir, en su caso, la modificación del texto legal que permita su sanción, si así se estima oportuno, como se pretende, por ejemplo, con el nuevo art. 264 del Proyecto de Código Penal de 2006. Por muy novedoso que sea el concepto de *phising*, estamos o en el ámbito de la estafa del art. 248, ya en su párrafo primero, ya en su párrafo segundo, aunque sea en un estado de imperfecta ejecución, ya, quizás, en el de los delitos contra la intimidad de los arts. 197 y siguientes, y la discusión sobre su tratamiento habrá de reconducirse a la interpretación de estos delitos y a la decisión sobre qué intereses se afectan y cuál es el mejor acomodo típico para lo que implica la conducta de suplantación de identidad o engaño.

Podrá ocurrir que sea difícil la subsunción de determinados supuestos en alguno de los delitos más o menos clásicos que contempla el Código Penal con los que sin duda se relacionan; ello, como digo, podrá favorecer la modificación del precepto, si así se entiende necesario, que permita la misma. Podrá ocurrir también que determinadas conductas no encajen de ninguna manera en precepto penal alguno, como puede ocurrir —no es ésta la opinión unánime— con el caso de los *hacker*s

inocuos o blancos o con el de obtención de prestaciones indebidas sin causación de perjuicio alguno; el debate aquí será el de si es necesaria la tipificación de estas conductas —postura que, siguiendo el modelo de otras legislaciones se adopta en el Proyecto de Código Penal de 2006 actualmente en el Congreso en un caso pero no en otro—, una vez se detecte, si es que existe, el bien jurídico-penal afectado con ella.

Esto es, el Derecho Penal, en su configuración actual, lo que comprende —prescindiendo de su categorización como delitos informáticos— es la descripción típica de una gran variedad de comportamientos que pueden materializar los riesgos y amenazas característicos del mundo digital, idóneos para hacer disfuncional el sistema, y que, por tanto, puede responder a ellos, tanto desde una vertiente preventiva como represiva. Y también es evidente que en algunos casos la respuesta no es posible, tanto por la propia voluntad legal de que así sea, al entenderse que no estamos ante conductas relevantes para merecer la intervención penal, como por la existencia de lagunas que quizás habría que colmar. Pero la cuestión nuclear no es la de la detección de conductas que atenten contra la voluntad del usuario o del gestor de los contextos digitales, sino la de si esas conductas son o deben ser objeto de atención por el Derecho Penal porque afectan a intereses ya tutelados o que debieran serlo —esto último, con todas las cautelas necesarias—, porque responden a conductas delictivas ya existentes —si se quiere, con nuevas formas de aparición— o porque siendo absolutamente novedosas, sin posibilidad de encaje en ninguna de las ya tipificadas, deben ser atendidas por su idoneidad lesiva para esos intereses ya tutelados o que debieran serlo.

Desde esta perspectiva, cuando hablamos de las conductas que afectan a los sistemas informáticos, telemáticos o cibernéticos —de delitos, si se quiere, que tienen que ver con las nuevas tecnologías de la información y la comunicación— que abarcan realidades muy diversas, y en el intento por precisar los diferentes prismas desde los que puede hablarse de esta clase de delitos, han sido numerosas las clasificaciones que se han efectuado de ellos, que, fundamentalmente, se dirigen a distinguir, en relación a agresiones tanto de carácter interno como externo, esto es, tanto desde dentro como desde fuera del ámbito de utilización autorizada del sistema, ya se dirijan las mismas contra intereses del gestor del sistema ya contra intereses ajenos, ya en su comisión por el propio usuario, ya contra él, los siguientes grupos de infracciones:

1.º) El que abarca lo que es la delincuencia que tiene por objeto el ataque a los sistemas informáticos en sí mismos considerados, con repercusión o no en el desarrollo de la actividad que permiten los mismos.

2.º) El que se refiere a la delincuencia que tiene por objeto los datos con los que se trabaja informáticamente, ya tengan carácter personal, ya carácter empresarial, desarrollada mediante la utilización de contextos digitales, que es al que en sentido más estricto se reserva por algún autor la caracterización de Derecho Penal informático por tratarse de agresiones contra y a través de sistemas informáticos. Como a menudo se señala, en realidad el resto de grupos no abarcan sino delitos tradicionales cometidos contra nuevos objetos materiales o a través de nuevas modalidades de conducta nucleados unos y otras en torno al hecho informático o cibernético.

3.º) El que engloba todas las conductas que se sirven de los sistemas informáticos para facilitar la actuación delictiva, ya sea de un tercero contra el titular o el beneficiario del sistema, ya sea de éste contra un tercero, que favorecen nuevas formas de ataque a bienes tradicionales o al menos facilitan la extensión de la lesividad, la peligrosidad o la proliferación de los ataques a tales bienes.

4.º) Finalmente, el que comprende lo que es la delincuencia que pretende únicamente atentar contra los derechos derivados de los procesos de innovación informática o de gestión de determinados derechos digitales.

Tratando de reflejar cómo responde el Código Penal español a la cuestión de la delincuencia informática —a pesar de que apenas existen alusiones expresas a conceptos directamente vinculados a la misma (que se resaltarán en cursiva en los artículo que se transcribirán a continuación)—, en lo que sólo pretende ser una primera aproximación a ello, general e introductoria, no cabe sino hacer referencia a los delitos que, en diversas ubicaciones del Código, pueden acoger las conductas que cabe incluir en alguno de los cuatro grupos de delitos descritos anteriormente, pues no existe en nuestro texto legal —cuyo acertado criterio de sistematización de los diferentes delitos es, básicamente, el del bien jurídico afectado por cada uno de ellos—, ni un Capítulo dedicado a los delitos informáticos, ni un concepto de delito informático, ni un listado de conductas vinculado a este tipo de criminalidad.

Muchos de los problemas que va a plantear el tratamiento penal de las conductas que puedan incluirse en cualquiera de los delitos a que a continuación se hará referencia —las conductas que queden fuera requerirán una discusión político-criminal sobre la relevancia de su nocividad—, que por supuesto no se pretenden analizar dogmáticamente,

sino únicamente describir en sus contenidos básicos en lo que en este específico contexto informático interesa destacar —y aún en él, insisto, sólo de modo esquemático—, pueden resolverse conforme a los criterios generales que delimitan lo que es un delito y la interpretación de los elementos que, en concreto, definen cada hecho típico. Otros han necesitado y van a necesitar todavía quizás determinadas precisiones legales que aludan directamente a la cuestión informática.

Al margen de la discusión sobre el contenido de cada uno de los elementos típicos y sobre si es posible o no subsumir la conducta objeto de atención en el dictado del precepto que pretende aplicarse, o de la que afecta a las cuestiones que plantea un tipo de actividad cada vez más identificada con fenómenos de delincuencia organizada, interesa también llamar la atención sobre dos de los problemas de aplicación general comunes a los diferentes grupos de delitos referidos a los que mayor atención se ha prestado en los Foros Internacionales.

Por una parte, el del ámbito espacial y temporal de comisión de los hechos, que dificulta conocer la ley aplicable, la jurisdicción competente para su enjuiciamiento, su posible prescripción y la propia persecución de algunos de estos delitos —de carácter transnacional en muchas ocasiones—, especialmente por el absoluto distanciamiento geográfico que puede existir entre autor y objeto o víctima de la conducta (aunque no necesariamente sucederá así en los casos de ataques de *insiders*) y la frecuente aparición de determinados eslabones anteriores, intermedios o posteriores (terminales y servidores que se utilizan para la ocultación del origen de la intrusión o el destino de los efectos de la misma) en el *iter criminis* delictivo.

Por otra parte, y en relación con el anterior, el de la individualización de la responsabilidad penal, por hechos propios o ajenos, en relación, por ejemplo, con la cuestión de los operadores de redes y servicios de comunicaciones telemáticas y de los proveedores de servicios de transmisión o acceso a redes de comunicaciones electrónicas o de servicios de hospedaje de páginas, motores de búsqueda, directorios de direcciones, etc. y su posible exención de responsabilidad por la constatación de acreditarse una neutralidad tecnológica con respecto a los contenidos o señales transmitidas o almacenadas y/o una colaboración para impedir el acceso a posibles contenidos ilícitos.

A ellos se ha tratado de dar diferentes respuestas dogmáticas y jurisprudenciales (por ejemplo, atendiendo la teoría de la ubicuidad en cuanto al lugar de comisión de los hechos) —también legales desde un punto de vista supraestatal—, sin que, sin embargo, en el caso español y junto a compromisos de cooperación pueda contarse con algo más que las normas generales sobre competencia jurisdiccional (arts. 23 y

concordantes de la Ley Orgánica del Poder Judicial) y sobre personas penalmente responsables (arts. 27 y siguientes del Código Penal).

Sí interesa destacar la importancia que tanto en esta sede como en cuanto a la definición de conductas susceptibles de sanción penal tiene la normativa internacional (especialmente, el Convenio sobre cibercriminalidad del Consejo de Europa de Budapest de 23 de noviembre de 2001, con su Protocolo de 28 de enero de 2003 de Estrasburgo sobre incriminación de actos de naturaleza racista y xenófoba y que traten de manera grosera de negar o justificar el genocidio o los crímenes contra la humanidad) y, en nuestro ámbito más próximo, la de la Unión europea (en particular, la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información).

También, por supuesto, junto a la de la propia normativa penal y procesal-penal —donde se debe trabajar especialmente en la cuestión de la obtención (con especial atención al tema de los registros y al concepto de lo privado y lo público), mantenimiento y valoración de la prueba, en la de la cooperación policial y judicial y quizás en la de la especialización de las Fiscalías—, la de carácter administrativo y privado, que será la que permita complementar e interpretar el contenido de muchas de las conductas delictivas a las que trata de hacerse frente (así, por ejemplo, y entre otras muchas, la Ley Orgánica de Protección de Datos de Carácter Personal o la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico).

Pero, hay que insistir en ello, téngase en cuenta en todo caso que al Derecho Penal no le ha interesado, al menos hasta ahora, lo que es la intromisión en el sistema en sí, si ésta se entiende que presenta un carácter inocuo y no es relevante en relación a la vulneración de algún interés que sí se considere debe ser objeto de tutela por el Derecho Penal y que, por ello, las conductas que acostumbra a referir cualquier análisis de las actividades ilícitas en el ámbito de los contextos digitales sólo importan en cuanto puedan reflejar dicha vulneración.

Claro que estamos ante un tipo de delincuencia —por lo que implica la absoluta digitalización de nuestra vida diaria y especialmente por el desarrollo de Internet— que permite una mayor extensión e intensidad de los efectos del delito, tanto desde una perspectiva local como personal, una mayor prolongación temporal de los mismos, quizás mayor facilidad de comisión y de ocultación de la identidad del autor y una dificultad de respuesta —normalmente tardía— por carencias competenciales, económicas, tecnológicas e incluso de capacitación para ello, pero éstas son consideraciones que han de tenerse en cuenta a partir del análisis de lo que en realidad significan —típicamente hablando— las conductas objeto de atención.

II. **Delitos cometidos contra sistemas informáticos**

1. *Delitos de daños (atentados contra la integridad de los sistemas y de los datos)*

A) Texto

> Art. 263: «El que causare daños en propiedad ajena no comprendidos en otros títulos de este Código, será castigado con la pena de multa de seis a 24 meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de 400 euros.»
>
> Art. 264: «[…] 2. [Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses] el que por cualquier medio destruya, altere, inutilice o de cualquier otro modo *dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos*.»
>
> Art. 267 pfo. 2.º: «Los daños causados por imprudencia grave en cuantía superior a 80.000 euros, serán castigados con la pena de multa de tres a nueve meses, atendiendo la importancia de los mismos […].»
>
> Art. 560: «1. Los que causaren daños que interrumpan, obstaculicen o destruyan *líneas o instalaciones de telecomunicaciones* o la correspondencia postal, serán castigados con la pena de prisión de uno a cinco años. […]».
>
> Art. 625: «Serán castigados con la pena de localización permanente de dos a 12 días o multa de 10 a 20 días los que intencionadamente causaran daños cuyo importe no exceda de 400 euros.»

B) Contenido

Estamos ante delitos comunes perseguibles de oficio excepto en el caso de los daños imprudentes del art. 267.

Concebidos los daños como destrucción, deterioro, alteración, inutilización o menoscabo de una cosa, estos delitos —y al margen de la especificidad de la figura de desórdenes públicos del art. 560.1 consustancial a tales infracciones— permiten sancionar tanto los daños que afecten a los sistemas informáticos en cuanto a los elementos materiales que incorporan (*hardware*) —art. 263— como los que afecten a los datos, programas o documentos contenidos en dichos sistemas, redes o simples soportes informáticos, que la doctrina viene denominando como elementos lógicos (*software*) —art. 264.2—, cuando tengan carácter doloso y superen los 400 euros, debiendo remitir la conducta a

los arts. 267 o 625, respectivamente, en el caso de daños imprudentes o de cuantía inferior.

Esta tipología permite abarcar —en lo que la delincuencia informática tiene de específico, al margen de la mera destrucción de los equipos informáticos equiparable a la de cualquier otro tipo de bien inventariable o del material informático que pueda considerarse de carácter fungible— las conductas de sabotaje informático desarrolladas mediante instalaciones de bombas lógicas, gusanos, programas maliciosos, troyanos, o virus (cualquier supuesto dentro de la tipología que abarca el concepto de *cracking* o «vandalismo informático»); conductas que afectan a la integridad de la información o a la estructura de los elementos lógicos del sistema, así como a su correcto funcionamiento, ya sea mediante el borrado irreversible de información almacenada, ya, por ejemplo, mediante la alteración o corrupción de la programación favoreciendo la causación de errores aleatorios en el funcionamiento del sistema.

Llama la atención la mayor penalidad de la afección al *software* frente a la del *hardware* cuando la conducta es dolosa y el importe del daño supera los 400 euros. Pero a este respecto hay que señalar que, siguiendo el mandato del Convenio sobre cibercriminalidad y la descripción que del delito de «atentado contra la integridad de los datos» se realiza en su art. 4, donde se exige sancionar como infracción penal la conducta de «dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos», y el correspondiente art. 4 de la Decisión Marco de 2005, el Proyecto de Código Penal de 2006 desplaza el contenido del art. 264.1 al texto del art. 263 en un nuevo apartado segundo que mantiene la pena agravada y convierte el art. 264.2 vigente en un nuevo art. 264 que sanciona, pero ahora ya con prisión de seis meses a dos años —inferior a la del tipo agravado aunque todavía superior a la del básico— a quien «sin autorización y de manera grave borre, dañe, deteriore, altere, suprima o haga inaccesibles datos o programas informáticos ajenos». Téngase en cuenta que, a pesar de la aparente mayor amplitud de las conductas descritas, las mismas ya se venían interpretando podían formar parte de los conceptos de daño, alteración o inutilización del actual art. 264.2, con lo que la nueva previsión, quizás frente a la intención inicial, lo que conlleva es simplemente un menor rigor punitivo, tanto por la exigencia de que el daño causado sea «grave» —que dificulta, además, interpretar si en los casos de ausencia de tal gravedad, superando el daño los 400 euros, podrá acudirse al art. 625, si el concepto de gravedad debe equipararse al daño de más de 400 euros, la opción más lógica, o si tal exigencia destipifica *de facto*, respecto a ese tipo de daños en *software*, los

supuestos hasta hoy considerados como falta—, como por la referida reducción de la pena.

Al margen de esta reforma, la legislación exige en todo caso para la aplicación de la sanción prevista la causación de un daño cuantificable en importe superior a 400 euros en el caso de las conductas dolosas, de 80.000 euros en el caso de las imprudentes y de una entidad concreta, la que sea, en el caso de las faltas dolosas. Y lo que en relación con ello es importante, que ese daño se produzca, en el caso de los sistemas lógicos, en el concreto objeto material de que se trate en sí mismo considerado —en su valoración económica o funcional, dependiendo del concepto de patrimonio que se adopte—, sin que sea suficiente la causación de perjuicios indirectos que, en su caso, podrán integrar el importe sujeto a responsabilidad civil.

Así, por supuesto, no integra la conducta típica la mera amenaza o peligro de daño, ni siquiera cuando ya se ha producido una vulneración del sistema (*hacker* blanco), salvo, claro está, que estemos en un supuesto de tentativa en que el acto de destrucción no se produce pero por causas ajenas al desistimiento voluntario del intruso, supuesto en el que el acceso ilícito habrá de entenderse como medio para la consecución de un sabotaje informático que no llega a producirse.

En este sentido, las características conductas de creación o difusión de virus, de mecanismos de lanzamiento múltiple de mensajes basura (*spamming*) o las más modernas de creación de ordenadores *zombies* al servicio de potenciales actividades delictivas mediante la introducción de troyanos en las *botnet*s o redes de ordenadores difícilmente pueden tener respuesta penal en sí mismas consideradas, con la legislación actualmente vigente, lo que ya sí ocurre en otros ordenamientos, y se prevé igualmente por el Convenio de Budapest, que en su art. 5 obliga a sancionar los «atentados contra la integridad del sistema», entendiendo como tales «la obstaculización grave del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos». Son los conceptos de introducción y transmisión de datos los que permiten describir perfectamente aquel tipo de conductas que, sin embargo, quedan fuera del texto penal español. A este respecto hay que señalar, sin embargo, que también el Proyecto de 2006 contempla un nuevo art. 264.2, previsto para sancionar a quien «sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema de información ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos»; no hablamos ya aquí, en todo caso, de mero intrusismo ni de causación de deficiencias en el funcionamiento del sistema —mayor lentitud, por

ejemplo—, sino de auténtico impedimento: obstaculización o interrupción del servicio que presta el mismo.

En la actualidad, como se ha señalado, si bien es cierto que no hace falta ni la destrucción total o parcial del soporte material ni la del sistema lógico, uno u otro tiene que al menos ver deteriorado su valor de uso en las cuantías reseñadas. Los perjuicios económicos que puedan derivarse de una deficiente producción de bienes de la empresa o de una incorrecta prestación de sus servicios no tienen cabida a efectos de valorar la existencia del delito y sí únicamente como responsabilidad civil.

Por ello justamente en otras legislaciones los delitos de daños informáticos se centran ya en la actualidad más simplemente en la cuestión de impedir la posibilidad de que se altere el funcionamiento de los sistemas de tratamiento de datos que en el hecho de la afección en sí a la estructura lógica del sistema; más en la cuestión de la causación de perjuicios económicos en su sentido más amplio generados mediante el sabotaje informático que en los daños informáticos en sentido estricto, que pueden ser ínfimos, por la facilidad de reparar el sistema o el escaso coste del material y tiempo requerido para ello una vez detectado el problema —y, por tanto, no dar siquiera lugar a la posibilidad de considerar delictiva la conducta y sí únicamente, en todo caso, falta del art. 625— o incluso inexistentes a pesar de la imposibilidad de uso temporal del sistema (así, por ejemplo, en el caso señalado de bombardeo de mensajes o en los de accesos masivos al sistema sincronizados, denegación de servicio con rechazo de mensajes de respuesta, lanzamiento de gusanos que se multiplican ocupando espacio libre o mínima alteración de un *link*, todos ellos de difícil encaje incluso en la falta de daños del art. 625).

2. *Delitos de hurto y apropiación indebida (apropiación de soportes digitales y utilización fraudulenta de equipos o sistemas de identidad digital)*

A) Texto

> Art. 234: «El que, con ánimo de lucro, tomare las cosas muebles ajenas sin la voluntad de su dueño será castigado, como reo de hurto, con la pena de prisión de seis a 18 meses si la cuantía de lo sustraído excede de 400 euros.
>
> Con la misma pena se castigará al que en el plazo de un año realice cuatro veces la acción descrita en el artículo 623.1 de este Código, siempre que el montante acumulado de las infracciones sea superior al mínimo de la referida figura del delito.»

Art. 235: «El hurto será castigado con la pena de prisión de uno a tres años:
3. […] Cuando revista especial gravedad, atendiendo al valor de los efectos sustraídos, o se produjeren perjuicios de especial consideración.»

Art. 252: «Serán castigados con las penas del artículo 249 o 250, en su caso, los que en perjuicio de otro se apropiaren o distrajeren dinero, efectos, valores o cualquier otra cosa mueble o activo patrimonial […] cuando la cuantía de lo apropiado exceda de cuatrocientos euros […].»

Art. 623: «Serán castigados con localización permanente de cuatro a 12 días o multa de uno a dos meses:
1. Los que cometan hurto, si el valor de lo hurtado no excediera de 400 euros.
2. Los que cometan […] apropiación indebida […] en cuantía no superior a 400 euros.»

B) Contenido

El delito o la falta de hurto consisten simplemente en el apoderamiento de cosa mueble ajena. En el contexto de la securización digital pueden entrar en juego, y de ahí la necesidad al menos de su consideración, al margen por supuesto de apoderamientos de material informático, de la clase que sea, que no revisten particularidad alguna, en los supuestos de incorporación al ámbito de dominio patrimonial de un sujeto de objetos ajenos que permitan el acceso a lugares, recintos, informaciones, documentaciones, etc., sin autorización. La sustracción de tarjetas magnéticas con incorporación de información digitalizada será el supuesto habitual.

En caso de que el objeto —la tarjeta— ya la tenga en su poder el sujeto en cuestión, tras haberla recibido lícitamente, su apropiación definitiva habiendo finalizado ya el período de autorización para su utilización —por ejemplo, por haber cesado en el puesto de trabajo—, dará lugar al delito o la falta de apropiación indebida. La misma infracción habrá que aplicar cuando se trate de un objeto perdido o de dueño desconocido.

En relación a ambas tipologías delictivas, únicamente han de recordarse tres cuestiones.

La primera, que sólo cabe una u otra infracción respecto de objetos corporales, no respecto de informaciones, fluidos o energías. Sólo cabe apoderamiento —hurto— o apropiación —apropiación indebida—, además, de cosas susceptibles de desplazamiento físico; y que sean, claro está, ajenas. No cabe, y aunque sea obvio el señalarlo, hurto de iden-

tidad digital, hurto de información digitalizada o apropiación indebida de conocimientos de acceso a sistemas de securización digital. Las conductas que se encuadran en el Convenio de Budapest dentro del art. 6 dedicado al «Abuso de equipos e instrumentos técnicos» en relación con la obtención «de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático» (art. 6.1.a.2.), quedan fuera de estos preceptos; serían, en su caso, actos preparatorios del delito que se vaya a cometer a partir de dicha obtención; otra cosa es la obtención «de un dispositivo, incluido un programa informático» (art. 6.1.a.1.) con soporte material.

La segunda, que la distinción entre delito y falta viene marcada por el valor corporal del objeto sustraído o apropiado; con independencia del beneficio o del perjuicio patrimonial que puedan obtenerse o causarse; y con independencia de que la utilización posterior de ese objeto que da acceso a un lugar o a una información conduzca a una actuación de carácter delictivo, en cuyo caso habrá de aplicarse además la pena que corresponda a la nueva infracción cometida en caso de que ésta exista efectivamente, sea cual sea, en el ámbito patrimonial o de tutela de la intimidad, por ejemplo.

La tercera, que el uso temporal de sistemas informáticos o soportes digitales es, en sí mismo considerado, irrelevante penalmente desde el punto de vista de los delitos de apoderamiento, sin que puedan entenderse ubicables en este contexto los supuestos de acceso ilícito o de abuso de equipos o instrumentos informáticos a que alude el Convenio de Budapest.

3. *Delitos de robo (apropiación de soportes digitales y utilización fraudulenta de equipos o sistemas de identidad digital)*

A) Texto

> Art. 237: «Son reos del delito de robo los que, con ánimo de lucro, se apoderaren de las cosas muebles ajenas empleando fuerza en las cosas para acceder al lugar donde éstas se encuentran o violencia o intimidación en las personas.»
>
> Art. 238: «Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes: […]
> 4.º Uso de llaves falsas.
> 5.º Inutilización de sistemas específicos de alarma o guarda.»

Art. 239: «Se considerarán llaves falsas: […]
A los efectos del presente artículo, se consideran llaves las *tarjetas, magnéticas o perforadas*, y los *mandos o instrumentos de apertura a distancia*».

Art. 240: «El culpable de robo con fuerza en las cosas será castigado con la pena de prisión de uno a tres años.»

B) Contenido

El delito de robo con fuerza en las cosas —el delito de robo con violencia o intimidación sería similar a estos efectos, excepto en relación con el dato añadido al apoderamiento patrimonial— implica también una sustracción, como en el caso del hurto, pero utilizando un medio comisivo de los descritos en el art. 238, especialmente desvalorado.

Se trae a este contexto únicamente para recordar, en primer lugar, que el robo puede utilizarse para apoderarse patrimonialmente del objeto que incorpore la información que permite el acceso a un sistema —una tarjeta magnética—, en cuyo caso la conducta siempre implicará la comisión de un delito —dándose los elementos que se han definido anteriormente— y no de una falta, sea cual sea el valor que se asigne al objeto, sin que en ello exista particularidad alguna que destacar.

En segundo lugar, téngase en cuenta que habiéndose obtenido mediante un delito de hurto o de apropiación indebida un objeto que incorpore información de seguridad digital —la tarjeta de identificación referida—, la misma puede utilizarse para la comisión de una infracción patrimonial, en cuyo caso ésta estará en el ámbito de aplicación del delito de robo en función de lo que prescriben los artículo 238.4.º y 239 pfo. 2.º. En el caso de que el posible apoderamiento patrimonial surja tras la quiebra de mecanismos de seguridad específicos estaremos igualmente en el ámbito del delito de robo, en función, en este caso, de lo que prescribe el art. 238.5.º. Siempre, y hay que insistir en ello, que a la utilización de la tarjeta o a la quiebra del sistema de seguridad siga —o se persiga— el apoderamiento patrimonial. No en otro caso, que nos obligaría a quedarnos únicamente con el hecho de la sustracción o apropiación de la tarjeta en sí o, en su caso, a acudir al ámbito de tutela de la intimidad, por ejemplo, en el caso de que lo que se persiga sea el acceso a una información no autorizada.

En tercer lugar, que sigue vigente, y a ello se aludirá posteriormente, la discusión sobre el tratamiento de incorporaciones patrimoniales mediante tarjetas que no permiten, sin clave de identificación, acceso a los activos ajenos.

Finalmente, obsérvese que en este contexto se entienden los delitos patrimoniales como delitos contra los sistemas informáticos en cuanto al valor que tienen estos en sí, con independencia de que también los delitos patrimoniales entren en juego cuando haya que calificar las defraudaciones patrimoniales cometidas mediante sistemas informáticos.

4. *Delitos de defraudación (acceso ilícito a equipos informáticos)*

A) Texto

> Art. 256: «El que hiciere uso de cualquier equipo *terminal de telecomunicación*, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses.»
>
> Art. 623.4: «[Serán castigados con localización permanente de cuatro a 12 días o multa de uno a dos meses] Los que cometan estafa […] o defraudación […] en equipos *terminales de telecomunicación* en cuantía no superior a 400 euros.»

B) Contenido

Al margen de cuanto se señale acerca de los delitos de estafa y otras defraudaciones en relación con la utilización de sistemas informáticos para obtener ventajas patrimoniales, en este grupo de delitos hay que aludir a los supuestos en los que lo que se pretende es la obtención de un beneficio derivado directamente de la utilización abusiva de un sistema digital, lo que en el Convenio de Budapest se denomina «acceso ilícito a sistemas informáticos» y, en su caso, «abuso de equipos o instrumentos informáticos», cuando tenga por finalidad dicho acceso.

En el Código Penal español es el art. 256 el que contempla la utilización no autorizada de un terminal de telecomunicación.

No es necesaria una utilización en la ubicación física del equipo informático, pues puede utilizarse el terminal a distancia, por ejemplo, mediante «troyanos» que se hacen con el control del ordenador. Ahora bien, téngase en cuenta que, por una parte, no es típico el mero uso indebido del terminal si de él, en sí mismo considerado, no se deriva perjuicio alguno, de más o menos de 400 euros —por lo que de nuevo aquí el denominado intrusismo informático en su versión de *hacker* blanco, que accede o interfiere de modo no autorizado en un sistema

informático o red de comunicaciones electrónica de datos, utilizando los mismos sin autorización o más allá de ella o que simplemente penetra en los sistemas informáticos por el placer de superar las barreras de seguridad, sin causación de perjuicio patrimonial alguno, tampoco puede subsumirse en este precepto—, y que, por otra, tampoco es típico el acceso a los servicios que pueda permitir el terminal si tampoco de ello se deriva tal perjuicio.

El precepto no pretende abordar o de hecho al menos no aborda esa intromisión ilícita en un ámbito ajeno, esa mera actuación sin permiso en el disfrute de un servicio por el que el titular ha de abonar un precio. No sanciona, en otros términos, el «acceso doloso y sin autorización a todo o parte de un sistema informático», en la terminología del art. 2 del Convenio de Budapest (que permite que los Estados, obligados a sancionar esta conducta, puedan exigir «que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva» o bien «que la infracción se perpetre en un sistema informático conectado a otro sistema informático»).

Tal como está redactado, sólo sanciona las conductas de utilización que generan un perjuicio patrimonial al titular legítimo del servicio que tiene que abonar un coste mayor o menor por dicha utilización no consentida, ya sea, por ejemplo, porque se produce una utilización de un teléfono de pago para acceder a redes informáticas, ya porque en sistemas de tarifa plana se produce un acceso a bases de datos u otros servicios por los que ha de pagar el titular; pero ni se penaliza el enriquecimiento del usuario ilícito (mera utilización temporal no consentida de un terminal de comunicación), ni la privación de la posibilidad de obtener un beneficio por la prestación de un servicio que no se contrata al disfrutarse de él gratuitamente (captación de señales de un *router* inalámbrico que evita altas en sistemas de banda ancha, aunque disminuya la capacidad del sistema que se interfiere), sino sólo el perjuicio del titular del terminal por el costo que le ocasiona la intervención ajena. Dudosos son los supuestos de utilización, por ejemplo, de tarjetas clonadas o de claves de acceso obtenidas ilícitamente con las que se logra disfrutar de un servicio por el que no se paga, que no afectan propiamente al sistema en sí, que no son actuaciones contra sistemas o datos informáticos, en sí mismos considerados y que habrá que remitir a los supuestos de defraudación ubicados en el grupo de los delitos cometidos a través de sistemas informáticos.

Por todo ello, y como ya antes se señalaba, cada vez se configura más como delito básico de carácter informático la mera utilización ilícita de un terminal de comunicación, el simple acceso ilegal al mismo.

Sin embargo, dicha normativa, que prescinde del aspecto patrimonial, encuentra mejor acomodo en el ámbito de la tutela de la privacidad —o quizás mejor en el de la tutela de lo que se entiende por libertad informática—, como veremos parece entender en parte el Proyecto de 2006 con el nuevo art. 197.3, vinculado no obstante a la tutela de la intimidad, ya se plantee sin ningún requisito adicional, ya exigiendo, por ejemplo, la vulneración de algún tipo de medida de seguridad diseñada *ex profeso*; la exigencia de alguna intencionalidad añadida obligaría a ubicar el precepto en sedes diferentes, dependiendo de cual fuera ésta: la vulneración de la intimidad, el daño del sistema, etc.

Y, en cualquier caso, siempre sería difícil entender subsumible en un precepto de estas características el aprovechamiento —sin acceso directo al terminal o a sus contenidos— de los servicios, por ejemplo, de banda ancha, que el mismo pueda prestar, para lo que sería necesario, lo que también en algún foro se reclama, en un exceso de rigor intervencionista, un tipo que sancionara la simple obtención indebida de prestaciones económicas, sin correlativo perjuicio alguno, que pueda procurar un terminal de comunicación.

5. *Delitos de falsificación (falsedades informáticas)*

A) Texto

> Art. 390: «[Se comete falsedad]:
> 1.º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.
> 2.º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad. […]»
>
> Art. 392: «El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses.»
>
> Art. 395: «El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390, será castigado con la pena de prisión de seis meses a dos años.»
>
> Art. 400: «La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, *programas de ordenador* o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.»

B) Contenido

Los delitos de falsedad, especiales en algún caso, comunes en los preceptos transcritos, tratan de tutelar la credibilidad social de que gozan ciertos signos, objetos o formas y, quizás de modo más preciso, la propia función del documento en el tráfico jurídico.

El problema fundamental que se plantea en este ámbito en los contextos digitales es únicamente el de si en el concepto de documento a que se refieren los artículo 392 y 395 o 393 y 396 —en cuanto al uso de los documentos a que se refieren los dos anteriores—, han de comprenderse los datos que se transmiten a través de redes informáticas.

El Convenio de Budapest, en su art. 7, dedicado al delito de falsedad informática, que junto con el art. 8 previsto para la estafa informática, integra el Título que el mismo destina a lo que en él se denominan «infracciones informáticas», en su sentido por tanto más estricto —según el criterio del Convenio—, atendiendo específicamente este ámbito obliga a sancionar «la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos», aceptando que los Estados puedan reservarse el derecho a exigir un ánimo cualquiera para que nazca la responsabilidad penal.

Si bien es cierto que el art. 26 del Código Penal, que es el que define el concepto de documento, no hace alusión alguna a esta cuestión, sí exige considerar documento sólo al soporte material que exprese o incorpore datos, hechos o narraciones con cualquier tipo de relevancia jurídica.

El material del soporte es indiferente mientras permita incorporar tales datos, hechos o narraciones; pero es necesario el mismo para garantizar la perdurabilidad del documento, que es lo que le otorga credibilidad y funcionalidad en el tráfico jurídico.

Hoy la doctrina y jurisprudencia penal aceptan sin discusión que el soporte informático permite integrar el concepto de documento, siempre por supuesto que, como en cualquier otro supuesto, se materialice una declaración de voluntad atribuida o atribuible a persona determinada o determinable destinada al tráfico jurídico o que pueda incorporarse a él.

La única cuestión a debatir es si la información —de imagen, texto o sonido— no contenida en un *diskette*, unidad de *USB* o soporte físico de otro tipo puede aceptarse como documento, lo que no parece plantear mayor problema siempre que la misma pueda ser visualizada o escuchada sin que se necesite su trascripción impresa.

En el caso de los sistemas de biometría e identidad digital, ningún problema hay en que se puedan falsificar aquellos soportes que incorporen algún tipo de información relevante para el sistema o utilizar los ya falsificados; la tutela penal será plena en estos casos.

Tampoco parece que en cuanto a las conductas a que alude el Convenio haya laguna alguna en la legislación española, que no requiere ulterior intencionalidad, con independencia de que, por regla general la falsificación o la utilización vengan asociadas a la comisión de un delito posterior, patrimonial o contra la intimidad, cuya penalidad habrá de entrar en concurso, normalmente de infracciones, con la que corresponda por el delito de falsedad cometido. En todo caso, en lo que es la falsificación en sí cabe hablar de un delito contra sistemas informáticos, siempre que de lo que se trate sea de alterar la veracidad o la autenticidad de los datos informáticos; no, por supuesto, si lo que se falsifican son meros soportes informáticos, en cuyo caso —como en general en todos los supuestos de piratería informática— habrá que remitirse, claro está, a los delitos contra la propiedad intelectual o, en su caso, industrial.

Llama la atención, por otra parte, la previsión del art. 400, cuyo contenido se acoge de modo similar, en otros contextos, en el art. 248.3 o 270.3, en cuanto punición de actos preparatorios, que también prevé el Convenio pero sólo para las «infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos» de sus arts. 2 a 6, entre los que no se incluyen las falsedades informáticas.

Interesa en este punto también hacer una alusión a la nueva previsión del art. 399 bis del Proyecto de 2006 (ténganse en la actualidad en cuenta los arts. 386 y 387 en relación a lo que es la falsificación de moneda en sus diversas formas), que contempla específicamente la sanción de las falsificaciones que tengan por objeto tarjetas de crédito o débito —en su sentido más estricto que no permite incluir tarjetas emitidas por entidades mercantiles no estrictamente financieras—, además de cheques de viaje, al margen —a diferencia del texto vigente— de la del resto de tarjetas —para la que se prevé una pena inferior—, con carácter autónomo y desligada también de lo que es la falsificación de moneda.

Siguiendo las indicaciones de la Decisión Marco 413/2001, de 28 de mayo de 2001, del Consejo de la Unión Europea, se prevé la sanción, con un concepto restrictivo y extensivo de falsificación al mismo tiempo, de la copia o reproducción de las tarjetas, pero no, por ejemplo, de la manipulación de tarjetas auténticas con finalidades fraudulentas —por ejemplo, incorporando datos obtenidos ilícitamente a la banda magné-

tica de la tarjeta auténtica, que, en su caso, habría que reconducir al ámbito de la estafa-; también de la tenencia «en cantidad que permita suponer están destinadas a la distribución o tráfico», anticipando la intervención penal aunque sin llegar al extremo de sancionar la posesión para su posterior uso propiamente mercantil; y, finalmente, del uso en perjuicio de otro y a sabiendas de la falsedad de la tarjeta falsificada, de forma similar a lo que penalizan los arts. 393 y 396.

III. **Delitos cometidos a través de la informática contra sistemas informáticos o informaciones digitalizadas**

1. *Delitos de descubrimiento y revelación de secretos (accesos informáticos ilícitos, interceptaciones de comunicaciones, intrusismo informático)*

A) Texto

> Art. 197.1: «El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, *mensajes de correo electrónico* o cualesquiera otros documentos o efectos personales o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de *cualquier otra señal de comunicación*, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.»
>
> Art. 197.2: «Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen *registrados en ficheros o soportes informáticos, electrónicos o telemáticos*, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.»
>
> Art. 197.3: «Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.»
>
> Art. 197.4: «Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, *soportes informáticos, electrónicos o telemáticos*, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su

mitad superior.» [Respecto a funcionarios, véanse los arts. 198, 413 ss. y 534 ss.; en el contexto de la defensa nacional, los arts. 598 ss.]

Art. 197.5: «Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.»

Art. 200: «Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.»

B) Contenido

Delitos comunes en la mayoría de los casos —excepto en el supuesto del art. 197.4—, todos perseguibles únicamente a instancia de parte, tratan de tutelar la intimidad y, en lo que a la securización digital se refiere, previenen la realización de conductas vinculadas al apoderamiento de datos contenidos en archivos informáticos, interceptación de comunicaciones telemáticas o acceso y en su caso distribución de datos contenidos en ficheros automatizados. Se enmarcan en la órbita de lo que prevén el art. 3 del Convenio de Budapest y, con matices, el art. 2 y el art. 4, dedicados respectivamente a la «interceptación ilícita», el «acceso ilícito» y los «atentados contra la integridad de los datos» dentro del Título 1 dedicado a las «infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos»

En el art. 197.1 está penalizado el apoderamiento de mensajes de correo electrónico o de cualesquiera otros documentos —incluidos los de carácter informático, esto es, en soportes informáticos o distribuidos a través de medios informáticos— (inciso 1.º), así como la interceptación de comunicaciones telemáticas y la utilización de artificios técnicos de acceso a señalas de comunicación telemáticas (inciso 2.º).

Ahora bien, de entrada el precepto, que contempla únicamente la vertiente dolosa de estos comportamientos —no imprudente—, sanciona tales conductas únicamente cuando se realicen «para descubrir los secretos o vulnerar la intimidad de otro», elemento subjetivo que hay que probar. De nuevo aquí debe negarse, por tanto, que puedan subsumirse en el tipo las conductas de mero intrusismo (*hackers* blancos) —salvo que el mismo represente el inicio de ejecución de un supuesto de apoderamiento de datos de carácter personal— y sí únicamente las de los accesos no autorizados aprovechando agujeros de seguridad u otras téc-

nicas de *hacking*, *sniffers*, «troyanos», siempre que se actúe con aquella finalidad.

Respecto al primer inciso, en absoluto se exige el apoderamiento del soporte material en que puede imprimirse el correo; lo que sí se exige en relación con los documentos es el apoderamiento —se dé o no el del soporte informático en que pueda aparecer incorporado—, de su contenido, que si es inaccesible no puede dar lugar a la apreciación de la conducta delictiva en grado de consumación.

Respecto al segundo inciso, aunque por regla general la utilización de algún tipo de artificio técnico será siempre necesaria —como presupuesto de hecho más que como requisito típico— para poder interceptar una comunicación, el precepto no exige el mismo. Al contrario, distingue —sancionando ambos casos—, ya la interceptación en sí —sin empleo de artificio alguno, si ello es posible y siempre que sea dolosa—, ya la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción sin conseguir las mismas.

En el art. 197.2 se sanciona el apoderamiento, utilización o modificación de datos reservados registrados en ficheros o soportes informáticos, electrónicos o telemáticos o el acceso a ellos sin autorización, conductas que afectan a la confidencialidad y la integridad de tales datos y que sólo se sancionan, al menos claramente en el caso de las conductas del primer apartado y en el de las del último inciso del segundo apartado del número —esto es, de todas menos de las de mero acceso—, si se pretende perjudicar al titular de los datos o a un tercero. En el art. 197.5 las conductas sancionadas son las mismas, pero referidas a datos que afectan a lo que se denomina núcleo esencial de la intimidad de las personas (ideología, religión, creencias, salud, origen racial o vida sexual), con lo que en aquél, donde se prevé pena menor, habrán de incluirse cualesquiera otros que no sean de público conocimiento.

El art. 197.3 sanciona con pena agravada la difusión de tales datos —cualesquiera de ellos— y el art. 197.4 agrava también la conducta de quien estando encargado o siendo responsable de este tipo de ficheros o soportes informáticos, electrónicos o telemáticos, realiza alguna de las conductas descritas (ténganse en cuenta también los arts. 198, 413 y ss., 534 y ss. y 598 y ss.).

A pesar de la amplitud con que están redactados los preceptos, la reiteración de conductas de carácter similar (alterar y modificar), la repetición de alguna de ellas (utilizar) y la confusión de los diferentes momentos y distintas perspectivas a que parecen referirse los preceptos dificultan en ocasiones su interpretación, dejando, por otra parte, lagunas de penalidad difíciles de colmar: así, por ejemplo, es difícil la

sanción de quien irrumpe en un ordenador ajeno visualizando un documento personal «no registrado» como tal o incluso obteniendo copia del mismo y es difícil, igualmente, la sanción de lo que se entiende por interceptación de comunicaciones no interpersonales (p. ej., en el caso de información generada de forma automática entre computadoras de diferentes entidades).

Tratando de responder a las exigencias del Convenio de Budapest, que permite, no obstante, considerar la necesidad de superar determinadas barreras de seguridad —así como de la Decisión Marco 2005/222/JAI— y siguiendo las tendencias internacionales en este ámbito, como ya se decía, el Proyecto de 2006 modifica el tenor del art. 197, creando un nuevo apartado 3 y desplazando los actuales apartados 3, 4, 5 y 6 a los nuevos números 4, 5, 6 y 7, para sancionar a quien «por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo», sin restricciones, por tanto, en cuanto al dato objeto de la intrusión y sin exigencias de finalidad ulterior alguna. Es cierto que el art. 197.2 sanciona el mero intrusismo, pero sólo en relación al acceso a datos reservados de carácter personal, no al acceso en sí a un sistema informático, o a parte de él, que no tiene por qué hacer referencia a los mismos y puede simplemente, por ejemplo, pretender la visualización de programas o archivos de direcciones públicas conocidas; es discutido, además, si dicho art. 197.2 exige o no, en cuanto a la conducta estricta de acceso, como antes se decía, actuar en perjuicio de tercero, lo que en modo alguno prevé ya el art. 197.3 del Proyecto. De hecho puede ser incluso cuestionable que este precepto deba ubicarse entre los delitos contra la intimidad pues lo que en realidad trata de tutelar es la privacidad en la utilización del propio sistema informático. Téngase en cuenta que buena parte de estas conductas podrán estar además preordenadas —al margen del intrusismo inocuo— al conocimiento del funcionamiento de un sistema con intencionalidades, más o menos explícitas, más o menos realizables en un tiempo cercano, defraudatorias, terroristas, etc., sin llegar a lo que pueda ser el ámbito de la ejecución imperfecta.

En todo caso, como previsión autónoma o dentro del ámbito de los delitos contra la intimidad, es el único precepto que podría acoger el mero intrusismo informático, el acceso de quien únicamente pretende demostrar pericia, motivaciones políticas no punibles, etc., tratando de garantizar más que otra cosa, y en el ámbito de lo que se conoce como securización digital, un uso libre de injerencias ajenas de los sistemas informáticos.

2. *Delitos contra el secreto de empresa (espionaje informático industrial)*

A) Texto

> Art. 278.1: «El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, *soportes informáticos* u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.»
>
> Art. 278.2: «Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.»
>
> Art. 278.3: «Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.»

B) Contenido

Con un contenido similar, pero en el ámbito de tutela no de la intimidad, sino del buen funcionamiento del mercado y de las instituciones que le son consustanciales —entre ellas, la capacidad competitiva de la empresa—, el art. 278, en sus diferentes números, sanciona como delito común perseguible también a instancia únicamente de parte, lo que se conoce como conductas contra el secreto de empresa o de espionaje industrial.

Conductas de apoderamiento de datos, documentos electrónicos o soportes informáticos donde se incluyan secretos de empresa o de interceptación de comunicaciones que afecten al mismo, realizadas con intención de descubrir tales secretos, que han de recaer sobre aspectos de la vida de la empresa —comercial, de desarrollo e investigación, de innovación, fiscal, industrial, laboral, publicitario, etc.— que tengan valor competitivo, esto es, cuyo conocimiento pueda ser valioso para los competidores, y no sean de público conocimiento; y de nuevo aquí la expresa finalidad excluye la sanción de supuestos de puro intrusismo.

Téngase en cuenta, sin embargo, que no se sanciona la destrucción, alteración u ocultación de la información, como sí ocurre en el caso de la intimidad (art. 197.2).

Finalmente, que el art. 278.3 alude también, aquí ya expresamente, a la sanción del apoderamiento o destrucción de los soportes informáticos que incorporan el secreto de empresa, pero remitiéndola a la aplicación del delito patrimonial correspondiente, en el intento por abarcar el desvalor total de la conducta que puede llevarse a cabo.

IV. **Delitos cometidos a través de sistemas informáticos**

1. *Delitos de defraudación (estafas o fraudes informáticos)*

A) Texto

> Art. 248.1: «Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.»
>
> Art. 248.2: «También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna *manipulación informática o artificio semejante* consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.»
>
> Art. 248.3: «La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren *programas de ordenador* específicamente destinados a la comisión de las estafas previstas en este artículo.»
>
> Art. 249: «Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros […].»
>
> Art. 255: «Será castigado con la pena de multa de tres a 12 meses el que cometiere defraudación por valor superior a 400 euros, utilizando […] *telecomunicaciones* u otro elemento, energía […] por alguno de los medios siguientes:
> 1.º Valiéndose de mecanismos instalados para realizar la defraudación.
> 2.º Alterando maliciosamente las indicaciones o aparatos contadores.
> 3.º Empleando cualesquiera otros medios clandestinos.»
>
> Art. 623.4: «[Serán castigados con localización permanente de cuatro a 12 días o multa de uno a dos meses] Los que cometan estafa […] o defraudación […] en equipos *terminales de telecomunicación* en cuantía no superior a 400 euros.»

B) Contenido

La estafa se define por la utilización de un engaño bastante que, generador de un error en otro, favorece una disposición patrimonial de éste, en perjuicio propio o de tercero.

En este contexto, ha sido largamente debatido el tratamiento que ha de darse a aquellos supuestos en que lo que se produce es una actuación fraudulenta en un aparato, con la que se consigue la disposición patri-

monial. Y en el ámbito estrictamente informático, el tratamiento que ha de darse a aquellos supuestos en que se produce una manipulación en sistemas digitales con la que se logra una transferencia patrimonial.

Este ámbito de la estafa informática (o, genéricamente, de los fraudes informáticos) ha sido abordado directamente por el legislador mediante la previsión de un art. 248.2 que expresamente contempla este tipo de supuestos exigiendo únicamente una manipulación informática o artificio semejante con los que se consiga una transferencia patrimonial no consentida en perjuicio de tercero. Aquí tendrán cabida, por ejemplo, tanto la quiebra de los sistemas de seguridad —por ejemplo, de identidad digital—, siempre que con ella se persiga la transferencia de activos descrita, como la obtención de transferencias mediante suplantaciones de identidad.

En cierta medida, los elementos de la estafa informática siguen siendo paralelos a los de la estafa genérica: así, la manipulación informática o artificio semejante equivaldría a la producción de engaño bastante y generación del consiguiente error, mientras que la transferencia lograda equivaldría al acto de disposición, siendo común a ambos supuestos la causación de un perjuicio patrimonial.

Estamos ante conductas de fraude mediante las que se logran transferencias de fondos no consentidas a través de órdenes falseadas o de la alteración del funcionamiento de los programas gestores de las operaciones contables. La manipulación puede producirse en el mismo programa, en cualquier momento del procesamiento o tratamiento automatizado de datos, ya sea en la entrada (*input*) o salida (*output*), ya en la trasmisión a distancia, mediante *modem*, red, etc., ya en la retroalimentación (*feedback*) o incluso en la obtención informática, pero personal, de los datos que permiten la transferencia patrimonial.

No se sanciona, por supuesto, sólo la utilización del sistema para, desde dentro, generar tales disposiciones a través de órdenes no autorizadas que emiten personas autorizadas a utilizar el sistema o de actuaciones no autorizadas por quienes no tienen permiso para acceder al sistema, sino incluso de actuaciones desde fuera que, por ejemplo, consiguen generar aleatoriamente números de tarjetas de crédito aceptadas para la realización de compras ficticias o que consiguen irrumpir en sistemas ajenos para alterar las órdenes de compra, inversión o transferencia de fondos que los mismos permiten o que, de cualquier otro modo, consiguen quebrar los sistemas de identidad digital generados al efecto de evitar utilizaciones del sistema o usurpaciones de identidad no deseadas. Siempre, ha de insistirse en ello, desde la perspectiva de la pretensión de causación de un perjuicio patrimonial derivado del correlativo enriquecimiento del infractor.

Las dudas sobre la posibilidad de ubicar este tipo de conductas en el ámbito clásico de la estafa activa la creación del delito de estafa informática. Pero si bien es cierto que lo único que requiere el precepto es la mera transferencia contable, que puede concretarse de las formas más variadas —no sólo obtención de un ingreso ficticio, sino generación de un derecho de crédito o de una orden de pago o cancelación de una deuda, etc.—, es dudoso, con todo, que permita incluir en él conductas en las que no se produce estrictamente una transferencia no consentida de un activo patrimonial; así, por ejemplo, en el supuesto de disfrute gratuito de servicios sin imputación de coste a un tercero, que remite en el ámbito de aplicación del art. 286, si se dan los elementos típicos que lo definen.

Por otra parte, parece que quedan también fuera del precepto aquellos supuestos en que no se produce manipulación informática o artificio semejante alguno, sino simplemente utilización de claves de acceso obtenidas lícita o ilícitamente, que nos conducen necesariamente a la comprobación de los elementos del tipo básico de estafa (como en el supuesto de obtención de bienes de modo fraudulento de un aparato automático) o del de robo con fuerza en las cosas, según las diferentes interpretaciones que se han mantenido en relación a este supuesto, o incluso, en su caso, a las nuevas previsiones del art. 286.

Téngase en cuenta que, y aunque la normativa española no haya recogido el mandato del Consejo, el Convenio de Budapest va quizás algo más allá al obligar a sancionar penalmente en el art. 8, como «estafa informática» y dentro del Título dedicado expresamente a las infracciones informáticas (que completa como se decía el art. 7 dedicado a la «falsedad informática»), tanto la «producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de la introducción, alteración, borrado o supresión de datos informáticos con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero», como la producción de dicho perjuicio con similar intencionalidad «a través de cualquier forma de atentado al funcionamiento de un sistema informático», que aunque no permite incluir usos indebidos o meros accesos ilícitos a sistemas de información, sí sancionar supuestos en que no existe estrictamente transferencia de activos. Ello es algo a lo que puede dar respuesta no obstante nuestro art. 255.

Interesa llamar la atención también de que, en este caso yendo más allá de lo que prevé el Convenio, el art. 248.3 sanciona la fabricación, introducción, posesión o facilitación de programas informáticos destinados específicamente a la comisión de estafas, tanto del número uno

como del número dos del art. 248 —no del art. 255—, lo que no obliga a hacer el Convenio que limita la obligación de sancionar las conductas de «producción, venta, obtención, importación, difusión u otras formas de puesta a disposición» o «posesión» de tales programas o dispositivos informáticos cuando estén preordenadas a la comisión no del art. 8 dedicado a la estafa informática, sino de los arts. 2 a 6 dedicados a accesos ilícitos, interceptaciones ilícitas, atentados contra la integridad de los datos o atentados contra la integridad del sistema.

Dentro de esta perspectiva digital del modo de comisión de una estafa, el Proyecto de 2006 introduce también aquí un nuevo precepto, el 248.2.c) —el actual art. 248.2 pasa a ser el 248.2 a) y el art. 248.3 el 248.2.b)— destinado específicamente a sancionar la utilización de tarjetas de crédito o débito, o los datos obrantes en ellas en perjuicio de su titular o de un tercero, tratando de solucionar los supuestos todavía controvertidos de accesos a cajeros mediante utilización no consentida de la tarjeta de un tercero, utilización abusiva de la tarjeta por su propio titular o utilización de tarjeta falseada o alterada o de los datos obrantes en ella, que la doctrina sigue discutiendo si ubicar en el art. 248.1 o en el art. 248.2 o incluso en el 238.5.º/239 pfo. 2.

Por supuesto, el art. 248.1 será de aplicación en todos aquellos supuestos en que el contexto digital para lo que sirve es únicamente para vehicular, sobre todo en supuestos de fraude en el comercio electrónico, el engaño generador del error. A este respecto, el Proyecto de 2006 incorpora igualmente un precepto dedicado a la estafa de inversiones en el art. 282 bis, que también puede darse con mayor facilidad en los contextos digitales.

En cuanto al art. 255, contempla como modalidad ya clásica de fraude patrimonial la defraudación en los sistemas de telecomunicaciones mediante manipulaciones clandestinas: conexión a redes sin pago, alteración para disfrutar de servicios no pagados, etc., que permite perfectamente abarcar los clásicos supuestos de artificios que desvían el pago por utilización de líneas 900, conexiones a direcciones de pago, desconexiones de servidores habituales redireccionados a otros servidores de pago o a otros números telefónicos más costosos, etc., con o sin quiebra de *firewalls*, con o sin quiebra de sistemas de autenticación digital, con o sin quiebra de cualquier mecanismo de protección frente a usos indebidos.

Finalmente, al art. 256 ya se ha hecho referencia en el epígrafe dedicado a los delitos contra los sistemas informáticos, por cuanto lo que refiere no es la causación de un perjuicio derivado de la utilización del terminal de comunicación, sino la propia autorización no consentida causante ella misma de un perjuicio.

2. *Delitos relativos al mercado y los consumidores (prestación ilícita de servicios restringidos)*

A) Texto

> Art. 286.1: «Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:
>
> 1.º La fabricación, importación, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier *equipo o programa informático*, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.
>
> 2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º.»
>
> Art. 286.2: «Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de *equipos de telecomunicaciones*, o comercialice equipos que hayan sufrido alteración fraudulenta.»
>
> Art. 286.3: «A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre el modo de conseguir el *acceso no autorizado a un servicio o el uso de un dispositivo o programa*, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista.»
>
> Art. 286.4: «A quien utilice los equipos o programas que permitan el acceso no autorizado a *servicios de acceso condicional o equipos de telecomunicación*, se le impondrá la pena prevista en el artículo 255 de este Código con independencia de la cuantía de la defraudación.»

B) Contenido

El nuevo delito del art. 286, incorporado al Código en 2003 y paradójicamente perseguible sólo a instancia de parte —aunque no se precise la denuncia, como dice el art. 287.2, si el delito afecta a intereses generales, que son los que en principio debieran considerarse objeto de tutela de un delito, recuérdese, situado entre los relativos «al mercado y los consumidores»— pretende en realidad, al margen de su ubicación sistemática la protección de los intereses de quienes prestan los servicios

de comunicación e información referidos. De ahí justamente la remisión penológica al art. 255 en el art. 286.4, y aun cuando en ningún momento se exija perjuicio alguno o, mucho menos, enriquecimiento o incluso ánimo de lucro —dependiendo esto último del número del artículo a aplicar—.

Se sancionan tanto conductas de prestación o facilitación del servicio como de preparación a ello, con fines comerciales —art. 286.1— o ánimo de lucro —art. 286.2— o sin él —art. 286.3—, en un intento por abarcar todo tipo de conductas vinculadas a lo que se conoce como *phreaking* —incluyendo la del usuario del servicio, siempre no obstante que se sirva de servicios o programas informáticos, por ejemplo, mediante tarjetas clonadas, pero no, en cambio, salvo en una interpretación extensiva del precepto que no entiendo sin embargo desacertada en este caso, cuando utilice combinaciones de series numéricas ilícitamente facilitadas— con o sin artificios técnicos, y con una redacción que permite abarcar muchos comportamientos hasta ahora sólo de modo forzado vehiculados a través de la estafa del art. 248.1 o de la defraudación del art. 255.

3. *Falsedades personales (adopción fraudulenta de identidad digital falsa)*

A) Texto

> Art. 401: «El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.»

B) Contenido

Interesa también en este ámbito al menos aludir a la previsión del art. 401, un tanto incorrectamente ubicado entre los delitos de falsedades, atendiendo la diversidad de objetos de tutela, donde se sanciona la atribución de un estado civil que no es el propio.

Apenas se ha planteado hasta ahora la subsunción de conductas relacionadas con la criminalidad informática en este ámbito, pero téngase en cuenta que, al margen de lo que es el acceso ilícito a soportes informáticos o terminales de comunicación y de la propia falsificación de los equipos que tratan de garantizar su utilización segura mediante el control de la identidad digital de quien accede a ellos, en todas sus variantes, el «hacerse pasar por otro» a través de un contexto digital, a los efectos de la más diversa índole, y siempre que ello tenga algún tipo de desvalor por la relevancia de la actuación, puede subsumirse per-

fectamente en este tipo. De nuevo aquí con independencia de que a la pena por esta tipología delictiva quepa añadir la que corresponda por la infracción de otra índole que pueda seguir a la adopción de la identidad falsa o incluso la que corresponda a la manipulación que haga posible la suplantación de identidad.

Téngase en cuenta también que el Proyecto de 2006 prevé un nuevo art. 392.2 en que sanciona expresamente el uso de documento de identidad falso, sin especificar el tipo de documento a que se refiere —por tanto, también de contenido digital— y un nuevo art. 400 bis que sanciona asimismo el uso de documento auténtico por quien no esté legitimado para ello. La posibilidad de incluir en esta sede, y al margen de otras ubicaciones en función de la motivación del autor, utilizaciones fraudulentas de documentos con claves de autenticación, *passwords*, bandas magnéticas con incorporación de datos personales, etc., debería tomarse en consideración.

4. *Delitos de difusión de contenidos lesivos para intereses diversos: libertad, libertad sexual, honor, correcto funcionamiento del mercado, derechos fundamentales y libertades públicas (delitos de difusión informática: webs de contenido sexual respecto a menores, ciberterrorismo, etc.)*

Si algo caracteriza en esta nueva época la problemática penal de Internet es la amplia posibilidad que ésta presta para la difusión de contenidos lesivos de intereses objeto de tutela penal, ya en el ámbito de la pornografía, la publicidad engañosa, la apología de la violencia, el terrorismo o el genocidio. Por supuesto, y al margen de cuestiones de competencia de jurisdicción, etc., si bien pudiera parecer que este ámbito de criminalidad no afecta ni a lo que es el ámbito de la securización digital en sí ni al del correcto uso de los sistemas informáticos conforme a los fines que les son propios —no estamos en el ámbito de infracciones contra contextos digitales—, los problemas pueden surgir cuando sistemas de titularidad o uso compartido se utilizan para dicha difusión —o recepción—, en el contexto de la dificultad que puede generar la determinación de las responsabilidades derivadas de ello.

En todo caso es ésta ciertamente una problemática menor en comparación con lo que implican estos medios para la proliferación de actuaciones delictivas o para su mayor facilidad de comisión o de ocultamiento. La ventaja que ofrecen las tecnologías de la comunicación para la realización de determinada clase de conductas, no sólo de opinión, que será lo más frecuente —delitos de amenazas, contra el honor, de

provocación a la discriminación, el odio o la violencia o de terrorismo—, sino de afección a ámbitos especialmente sensibles como el de la tutela de la libertad sexual en cuanto a la protección de los menores se refiere, es indudable. A este último ámbito se hará una especial referencia por ser quizás aquél en que mayor incidencia ha tenido de hecho el desarrollo de este tipo de tecnología.

A) Texto

> Art. 186: «El que por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.»
>
> Art. 189.1: «Será castigado con la pena de prisión de uno a cuatro años:
> a) El que utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico cualquiera que sea su soporte, o financiare cualquiera de estas actividades.
> b) El que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o los poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.»
>
> Art. 189.2: «El que para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.»
>
> Art. 189.7: «Será castigado con la pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada».

B) Contenido

En el ámbito de la indemnidad sexual, el Código Penal permite contemplar hechos punibles relativos a materiales pornográficos que puedan tener una especial vinculación con medios informáticos: en el art. 186 en relación a supuestos de pornografía dirigida a menores —también en el art. 185 en cuanto a ejecución de actos de exhibición obscena ante

menores— y en el art. 189 en relación a supuestos de pornografía infantil. En ninguno de ambos preceptos se menciona expresamente el ámbito informático, pero al sancionarse la venta, difusión o exhibición, en un caso, y la elaboración, producción, venta, distribución, exhibición, facilitación de las anteriores conductas, financiación, posesión con aquellas finalidades o para uso propio, sin diferenciar el tipo de soporte e incluso utilizando la expresión en el caso del art. 189.1 a) «cualquiera que sea su soporte», la regulación perfectamente permite sancionar la realización de cualesquiera de los anteriores comportamientos a través de redes informáticas.

El problema que plantea la utilización de estos preceptos, prescindiendo de discusiones habituales en su seno ajenas a lo estrictamente informático, es, en primer lugar, y en el caso del art. 186, que se requiere utilización de un medio directo lo que, aunque no impediría la sanción de conductas de venta, difusión o exhibición de material entre menores a través de correos, foros o *chats* con menores concretos, imposibilita la prevención cuando se utilizan páginas no dirigidas expresamente a menores. A ello puede añadirse la cuestión del posible desconocimiento de la edad del usuario.

En cuanto a la aplicación del art. 189.1, que permite sancionar conductas de elaboración de material pornográfico con menores a través de procedimientos informáticos y de posterior distribución en sentido amplio de dicho material, el problema va a plantearse —solucionada ya la cuestión de la jurisdicción, al tratarse de delitos de justicia universal, perseguibles sea cual sea el lugar donde se cometan— a la hora de determinar, sobre todo, la autoría y el concepto de «facilitación», que, interpretado en sentido amplio, permite la sanción de cualquier tipo de comportamiento (creación de listados, información a terceros, etc., e incluso en opinión de algunos —hoy por hoy, minoritaria— la procuración de medios técnicos). La problemática del tratamiento del proveedor del servicio o del proveedor del acceso es objeto todavía de controversia en la doctrina, lo que a mi juicio debería depender más del conocimiento que se tenga del hecho que de la falta de adopción de medidas tendentes a evitarlo. Más compleja si cabe es la cuestión de la posesión a que se refiere el art. 189.2, en relación, por ejemplo, con el visionado directo de páginas de pornografía infantil y el significado de los «archivos temporales» o el acceso a páginas compartidas —que debería solucionarse atendiendo el sentido de la expresión «para su propio uso»— al no existir una redacción tan explícita como la del art. 9 del Convenio de Budapest, que únicamente exige la obtención del material pornográfico.

La minuciosa atención que a este delito presta dicho art. 9 prevé la sanción penal obligatoria de distintos comportamientos de producción,

ofrecimiento, puesta a disposición, difusión o transmisión de pornografía infantil a través de un sistema informático, eximiendo de dicha obligatoriedad en el caso de las conductas, cuya sanción penal también prevé, de procurarse, procurar a otro o poseer mediante un sistema informático o en un medio de almacenamiento de datos informáticos material de esa índole, entendiendo por pornografía infantil la representación visual de un menor adoptando un comportamiento sexualmente explícito, así como —lo que deja a la opción de los Estados firmantes— la representación visual de una persona que sin serlo aparece como un menor —lo que se conoce como pornografía técnica— o la de imágenes que representen un menor adoptando tal comportamiento —lo que se denomina pseudopornografía o pornografía simulada—. El legislador español ha modificado recientemente su legislación, siguiendo la tendencia en esta sede, acogiendo la sanción de todas la conductas descritas en el Convenio, si bien todavía, con un concepto más estricto de pornografía infantil en cuanto al objeto de la representación visual, que sólo abarcaría la primera referencia y, debido a la matización del art. 189.7, la tercera, donde pueden incluirse conductas denominadas de *morphing* —vinculadas a lo que se entiende por pseudopornografía—, que en realidad poco tienen que ver con el hecho sexual en sí en cuanto a la vulneración de los intereses del menor, y sí más, quizás, con su dignidad personal. Merece destacarse también la expresa previsión del art. 189.3 d), en relación con el material pornográfico en que se representan menores víctimas de violencia física o sexual, de creciente distribución a través de la red.

En el ámbito del resto de ilícitos, téngase en cuenta que lo que garantiza la cibernética es la rápida y amplia difusión de contenidos lesivos en los diferentes delitos referidos —amenazas, informaciones injuriosas o calumniosas, publicidad engañosa, incitación al odio o a la violencia, terrorismo o genocidio— y que lo que dificulta es el conocimiento de quien los difunde y la delimitación de la responsabilidad de quien contribuye a ello, sin que la interpretación de las distintas infracciones plantee particularidad alguna por el hecho de cometerse en un contexto informático en lo que hace referencia a sus distintos elementos típicos.

5. *Otros delitos*

Téngase en cuenta que además de estos campos más específicos de actuación delictiva en el mundo de la informática, es posible, como ya se señalaba, la comisión de numerosos delitos ajenos a él que se favo-

recen, sin embargo, a través de los déficits de seguridad que generan la implantación de las tecnologías de la información y de la comunicación o los meros sistemas de securización digital de los entornos públicos o privados.

Por aludir a algún supuesto característico, téngase simplemente en cuenta, por ejemplo, la mayor facilidad de comisión de atentados patrimoniales (robos o estafas) o de atentados contra la libertad y seguridad (detenciones ilegales o secuestros) que se deriva del conocimiento del modo de actuación de los directivos o empleados de una empresa que pueda obtenerse a través de la incursión en sus sistemas informáticos, supuestos que, de no llevarse a cabo la actuación delictiva proyectada, deben ser tratados como actos preparatorios previos a los propiamente dichos de ejecución delictiva, en la mayoría de los casos no obstante impunes, supuestos de receptación o de blanqueo de bienes o incluso supuestos vinculados a delitos tradicionales de homicidio, lesiones, daños, incendios, etc., en los que el medio informático se utiliza para alterar información, bloquear sistemas de alarma o generar, por ejemplo, cortocircuitos, que es lo que producirá el resultado pretendido. El hecho informático, sin embargo, en todos ellos, no va a plantear en sí problemas de interpretación típica específicos más allá de los propios de la delimitación de la responsabilidad individual y, en su caso, de la concreción de la vinculación causal entre acción y resultado.

V. **Delitos contra la gestión de derechos digitales**

La tutela de la propiedad intelectual e industrial, como interés merecedor y necesitado de protección penal, se garantiza frente a los ataques más graves para el conjunto de facultades que se derivan de la creación de obras de diversa naturaleza, entre ellas la que hacen referencia a programas de ordenador, patentes, modelos de utilidad o topografías de semiconductores.

Sin que exista una expresa alusión a la perspectiva informática en la descripción de los distintos delitos y faltas que en el Capítulo XI del Título XIII se ocupan en el Código Penal, dentro de los delitos contra el patrimonio, de la tutela de la propiedad intelectual e industrial, salvo en la referencia del art. 270.3, es en la descripción genérica de los distintos comportamientos de los arts. 270 y siguientes donde han de tratar de ubicarse las conductas que puedan materializar los riesgos idóneos para menoscabar los derechos que se derivan de la gestión de derechos digitales.

1. *Delitos contra la propiedad intelectual (pirateo informático)*

A) Texto

> Art. 270.1: «Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística *fijada en cualquier tipo de soporte o comunicada a través de cualquier medio*, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.»
>
> Art. 270.2: «Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien intencionadamente exporte o almacene ejemplares de las obras, producciones o ejecuciones a que se refiere el apartado anterior sin la referida autorización. Igualmente incurrirán en la misma pena los que importen intencionadamente estos productos sin dicha autorización […].»
>
> Art. 270.3: «Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier *dispositivo técnico que se haya utilizado para proteger programas de ordenador* o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.»
>
> Art. 271: «Se impondrá la pena de prisión de uno a cuatro años, multa de 12 a 24 meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias: […].»

B) Contenido

Delitos comunes y en la actualidad perseguibles de oficio, los delitos contra la propiedad intelectual refieren en este ámbito, entre otras, conductas denominadas de pirateo informático.

Por una parte, el art. 270.1 permite sancionar copias no autorizadas de obras de cualquier tipo o distribución de ellas, «fijadas en cualquier tipo de soporte o comunicadas a través de cualquier medio»; aun sin mención expresa del legislador, ningún problema hay para incluir en el precepto actuaciones delictivas vinculadas a programas de ordenador o informaciones de cualquier naturaleza distribuidas a través de red —comunicaciones de texto, audio o vídeo— respecto de las que existan derechos de autor.

La protección de los derechos de autor sobre programas de ordenador, definidos en el art. 96.1 LPI, se efectúa a través de su asimilación a estos efectos a las obras literarias, comprendiendo tanto el *software* como la documentación técnica y manuales de uso, ya en relación a los derechos de creación de la obra (plagio, distribución o comunicación, al margen de la reproducción aquí menos relevante), ya a los de su explotación (distribución y transformación no consentida de la obra, al margen de la reproducción y la comunicación pública).

Siempre, en todo caso, que las conductas tengan relevancia para afectar a los derechos de propiedad intelectual y no se agote el desvalor en la utilización privada de lo que se copia o distribuye. Suponiendo que en cuanto al objeto material de la conducta podamos estar en el ámbito de lo que trata de tutelar la Ley de Propiedad Intelectual y que en lo que concierne a las modalidades de la conducta podamos entender que se ha producido, por ejemplo, un plagio, una reproducción o una distribución —con todos los supuestos conflictivos que en este tema se presentan en los contextos digitales— el precepto exige explícitamente además el actuar con ánimo de lucro y en perjuicio de tercero, sin que puedan entenderse comprendidos en el delito los supuestos en que el lucro procede exclusivamente de la ausencia de desembolso por parte de quien utiliza en beneficio propio un producto —con el correlativo lucro cesante para el titular del derecho—, en la absoluta privacidad.

Así, sí se incluye la venta de programas informáticos pirateados, pero no, por ejemplo, la introducción del programa en la memoria interna del ordenador de un usuario ni la copia de seguridad que éste pueda obtener de un programa por él adquirido o ni siquiera la cesión de copias a terceros que lo utilizarán también para fines privados; mucho menos copias necesarias técnicamente para realizar determinadas transmisiones.

La protección de los derechos de autor sobre creaciones de audio, vídeo o audiovisuales tiene el mismo ámbito de aplicación. Pero, que exista soporte informático o no, es irrelevante.

Por eso, además de los clásicos supuestos de *top manta*, aquí caben las ventas a través de la red de copias de *software* y, dependiendo de los casos —en función de cómo se explique el ánimo de lucro—, distribuciones masivas sin enriquecimiento económico directo, que no exige el precepto, pero no la distribución gratuita en círculos restringidos, al margen de la ilegalidad del comportamiento. Más discutida es la descarga en operaciones de intercambio horizontal de archivos entre particulares conocidas como *peer to peer* (*P2P*), lo que a mi juicio dependerá de la existencia o no de ánimo de lucro y claramente impune la mera reproducción, sin significado económico relevante alguno en todos aquellos

casos en que la misma, asociada a un proceso de comunicación (hiperenlaces, etc.), es transitoria.

También entran en el ámbito de protección del art. 270 —según los casos, del art. 273— conductas vinculadas a bases de datos o diseños de páginas *web* o utilización de cualesquiera contenidos obtenidos de páginas, ficheros, etc., ajenos y no públicos.

En todo caso, la conducta del beneficiario de los comportamientos que sí tengan encaje en el precepto queda al margen de la sanción y es susceptible de penalización únicamente a través de la previsión de los delitos que sancionan el encubrimiento o la receptación.

La regulación incorpora en el art. 270.3 un tipo específico previsto especialmente para impedir la desprotección de programas de ordenador que, respondiendo a exigencias armonizadoras en el seno de la Unión Europea adelanta la intervención penal a conductas meramente preparatorias, en la línea antes aludida del art. 6 del Convenio de Budapest, tampoco previsto para infracciones vinculadas a atentados a la propiedad intelectual y derechos afines de su art. 10, artículo que, por otra parte, exime además a los Estados miembros de la obligación de sancionar penalmente este tipo de conductas si disponen de otros recursos eficaces para su represión.

Es necesario llamar también la atención sobre las agravaciones del art. 271, para supuestos de especial trascendencia, que impedirán la remisión condicional de la pena y obligarán al consiguiente ingreso en prisión, ineludible, dada la entidad de la pena privativa de libertad prevista y sobre la remisión del art. 272 para establecer la responsabilidad civil derivada del delito a la Ley de propiedad Intelectual y, en concreto, a sus arts. 138 a 143 dedicados a la adopción de acciones y medidas cautelares urgentes, el cese de la actividad ilícita, el carácter de la indemnización, la adopción de medidas cautelares generales y el modo de adoptarlas en la causa criminal.

2. *Delitos contra la propiedad industrial*

A) Texto

> Art. 273.1: «Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos.»

Art. 273.2: «Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.»

Art. 273.3. «Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados a favor de tercero por un modelo o dibujo industrial o artístico o *topografía de un producto semiconductor*.»

Art. 274.1: «Será castigado con la pena de seis meses a dos años de prisión y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro, reproduzca, imite, modifique o de cualquier otro modo utilice un signo distintivo idéntico o confundible con aquél, para distinguir los mismos o similares productos, servicios, actividades o establecimientos para los que el derecho de propiedad industrial se encuentre registrado. Igualmente, incurrirán en la misma pena los que importen intencionadamente estos productos sin dicho consentimiento […].»

Art. 276: «Se impondrá la pena de prisión de uno a cuatro años, multa de 12 a 24 meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias: […].»

B) Contenido

De carácter absolutamente similar a los delitos contra la propiedad intelectual la única diferencia con ellos de los delitos relativos a la propiedad industrial viene dada por el distinto objeto del delito, sujeto en un caso a derechos de autor, sujeto en otro a la normativa sobre propiedad industrial en la que tendría cabida, por ejemplo, la tutela del nombre de dominio en Internet o cualquier mecanismo de securización diseñado para su explotación comercial.

En este sentido, y obsérvese que la descripción típica es muy parecida en el caso de los arts. 270.1 y 273.1, 2 y 3 y en el caso de los arts. 270.2 y 274.1, e idéntica en el caso de los arts. 271 y 276, la propiedad industrial lo que básicamente refiere son invenciones —ya sea en cuanto a un objeto patentado ya en cuanto al procedimiento para crearlo, también patentado— relacionadas con el ámbito económico, comercial o industrial de determinados productos.

Acostumbra a señalarse que en lo que afecta a la propiedad intelectual el autor concibe y aplica lo concebido, siendo además la

creación de una obra un fin en sí misma, sin perjuicio de su valor de mercado, mientras que en la propiedad industrial la originalidad y personalidad de la creación se somete a la finalidad de proporcionar un servicio o utilidad, que a su vez cumplirá el objeto concebido, que podrá ser producido a gran escala por otros, lo que no es imaginable en la creación intelectual o artística. En todo caso, se admite que existen objetos problemáticos, difíciles de encajar en uno u otro tipo de propiedad, como justamente los programas de ordenador, por ejemplo, que por decisión legal corresponden al ámbito de la propiedad intelectual, como recoge el art. 10 de la Ley de Propiedad Intelectual, a pesar de que perfectamente podrían considerarse objetos de propiedad industrial. Obsérvese, en todo caso, que las penas previstas en los arts. 270 y siguientes, por una parte, y 273 y siguientes, por otra, son las mismas.

Interesa, por último, simplemente llamar también la atención sobre la expresa alusión en el art. 273.3 a la tutela de la topografía de productos semiconductores por su vinculación directa, aunque no sólo, al ámbito de la digitalización.

Bibliografía

Álvarez Vizcaya, M., «Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red», en *Cuadernos de derecho judicial*, 10, 2001, 255-280.

Andrés Domínguez, A.C./Huerta Tocildo, S., «Intimidad e informática», en *Revista de Derecho Penal*, 6, 2002, 11-72.

Climent Barberá, J., «La justicia penal en Internet. Territorialidad y competencias penales», en *Cuadernos de derecho judicial*, 10, 2001, 645-663.

Choclán Montalvo, J.A., «Fraude informático y estafa por computación», en *Cuadernos de derecho judicial*, 10, 2001, 305-352.

Choclán Montalvo, J.A., «Infracciones patrimoniales en los procesos de transferencia de datos», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 69-95.

De Alfonso Laso, D., «El hackerin blanco. Una conducta ¿punible o impune?», en *Cuadernos de derecho judicial*, 10, 2001, 509-524.

De Urbano Castrillo, E., «El documento electrónico: aspectos procesales», en *Cuadernos de derecho judicial*, 10, 2001, 525-632.

Fernández Teruelo, J.G., «Respuesta penal frente a la piratería en Internet: subsunción típica y criterios de imputación subjetiva de los ISPs», en *Revista de Derecho Penal*, enero, 2003, 31-57.

Fernández Teruelo, J.G., «La sanción penal de la distribución de pornografía infantil a través de Internet», en *Boletín de la Facultad de Derecho de la UNED*, 20, 2002, 249-276.

GALLARDO RUEDA, A., «Delincuencia informática: la nueva criminalidad de fin de siglo», en *Cuadernos de Política Criminal*, 65, 1998, 365-374.

GÓMEZ MARTÍN, V., «La protección penal de los derechos de autor sobre los programas informáticos: un ejemplo de la naturaleza patrimonialista de los delitos contra la propiedad intelectual en el CP de 1995», en *Poder Judicial*, 66, 2002, 143-212.

GÓMEZ MARTÍN, V., «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3.º CP)», en *Revista electrónica de ciencia penal y criminología*, 4, 2002.

GÓMEZ TOMILLO, M., *Responsabilidad penal y civil por delitos a través de Internet. Especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces*, Cizur Menor (Navarra), 2006.

GONZÁLEZ RUS, J.J., «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *Revista de la Facultad de Derecho de la Universidad Complutense*, 12, 1986, 107-164.

GONZÁLEZ RUS, J.J., «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», en *Revista electrónica de ciencia penal y criminología*, 1, 1999.

GONZÁLEZ RUS, J.J., «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 Cp)», en *La Ciencia del Derecho penal ante el nuevo siglo. Homenaje al Profesor Dr. D. José Cerezo Mir*, Madrid, 2002, 1281 ss.

GONZÁLEZ RUS, J.J., «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 241-269.

GUTIÉRREZ FRANCÉS, M.L., *Fraude informático y estafa*, Madrid, 1991.

GUTIÉRREZ FRANCÉS, M.L., «Delincuencia económica e informática en el nuevo Código Penal», en *Cuadernos de derecho judicial*, 11, 1996, 247-306.

GUTIÉRREZ FRANCÉS, M.L., «Problemas de aplicación de la ley penal en el espacio virtual», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, pp. 43-68.

JAREÑO LEAL, A./DOVAL PAÍS, A., «Revelación de datos personales, intimidad e informática», en *El Nuevo Derecho Penal Español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz*, Cizur Menor (Navarra), 2001, 1475-1495.

LEZERTUA RODRÍGUEZ, M., «El proyecto de convenio sobre el cybercrimen del Consejo de Europa», en *Cuadernos de derecho judicial*, 10, 2001, 15-62.

LÓPEZ MORENO, J./FERNÁNDEZ GARCÍA, E.M., «La world wide web como vehículo de delincuencia: supuestos frecuentes», en *Cuadernos de derecho judicial*, 10, 2001, 399-456.

LÓPEZ ORTEGA, J.J., «Libertad de expresión y responsabilidad por los contenidos en Internet», en *Cuadernos de derecho judicial*, 10, 2001, 83-126.

LÓPEZ ORTEGA, J.J., «Intimidad informática y derecho penal (la protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)», en *Cuadernos de derecho judicial*, 9, 2004, 107-142.

MAGRO SERVET, V., «La responsabilidad civil y penal en el campo de la informática», en *Cuadernos de derecho judicial*, 7, 2003, 379-432.
MARCHENA GÓMEZ, M., «El sabotaje informático: entre los delitos de daños y desórdenes públicos», en *Cuadernos de derecho judicial*, 10, 2001, 353-366.
MARTÍN-CASALLO LÓPEZ, J.J. (Dir.), *Problemática jurídica en torno al fenómeno de Internet*, Madrid, 2000.
MATA Y MARTÍN, R.M., *Delincuencia informática y Derecho penal*, Madrid, 2001.
MATA Y MARTÍN, R.M., «Algunos aspectos de la delincuencia patrimonial en el comercio electrónico», en *El comercio electrónico*, Madrid, 2001, 441-462.
MATA Y MARTÍN, R.M., «Criminalidad informática: una introducción al cibercrimen (1)», en *Actualidad Penal*, 37, 2003, 935-961.
MATA Y MARTÍN, R. M., «Perspectivas sobre la protección penal del software», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 97-152.
MAZA MARTÍN, J.M., «La intervención judicial de las comunicaciones a través de Internet», en *Cuadernos de derecho judicial*, 10, 2001, 633-644.
MATELLANES RODRÍGUEZ, N., «Algunas notas sobre las formas de delincuencia informática en el Código Penal», en *Hacia un derecho penal sin fronteras*, Madrid, 2000, 129-150.
MIR PUIG, C., «Sobre algunas cuestiones relevantes del Derecho penal en Internet», en *Cuadernos de derecho judicial*, 10, 2001, 281-304.
MIRÓ LLINARES, F., «La protección penal de los derechos de explotación exclusiva sobre el software», en *Revista Penal*, 13, 2004, 67-84.
MORALES GARCÍA, O., «Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios en la sociedad de la información», en *Revista de Derecho y Proceso Penal*, 2001, 139-167.
MORALES PRATS, F., *La tutela penal de la intimidad: privacy e informática*, Barcelona, 1984.
MORALES PRATS, F., «La protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995», en *Cuadernos de derecho judicial*, 3, 1996, 147-196.
MORALES PRATS, F., «Pornografía infantil e Internet: la respuesta en el Código Penal», en *Cuadernos de derecho judicial*, 4, 2000, 175-205.
MORALES PRATS, F., «Internet: riesgos para la intimidad», en *Cuadernos de derecho judicial*, 10, 2001, 63-82.
MORALES PRATS, F., «El derecho penal ante la pornografía infantil en Internet», en *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*, Madrid, 2002, 95-118.
MORALES PRATS, F., «Los ilícitos en la red (II): pornografía infantil y ciberterrorismo», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 271-296.
MORÓN LERMA, E., *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, Cizur Menor (Navarra), 2.ª ed., 2002.
MORÓN LERMA, E., «Derecho Penal y nuevas tecnologías: panorama actual y perspectivas futuras», en *Internet y pluralismo jurídico: formas emergentes de regulación*, Madrid, 2003, 93-120.

ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001.

PERARNAU MOYA, J., «Internet amenazada», en *Cuadernos de derecho judicial*, 10, 2001, 127-144.

PICOTTI, L., «Fundamento y límites de la responsabilidad penal de los proveedores de acceso y servicio en Internet», en *Revista de derecho y proceso penal*, 3, 2000, 211-232.

PIÑAR MAÑAS, J.L., «La protección de los datos personales y ficheros automatizados», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 153-166.

QUINTERO OLIVARES, G., «Internet y propiedad intelectual», en *Cuadernos de derecho judicial*, 10, 2001, 367-398.

RODRÍGUEZ MOURULLO, G./LASCURAÍN SÁNCHEZ, J.A./ALONSO GALLO, J., «Derecho Penal e Internet», en *Régimen jurídico de Internet*, Madrid, 2001, 257-310.

ROMEO CASABONA, C., *Poder informático y seguridad jurídica*, Madrid, 1988.

ROMEO CASABONA, C., «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, 2, 2002, 123-149.

ROMEO CASABONA, C., «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 1-42.

ROMEO CASABONA, C., «Los datos de carácter personal como bienes jurídicos penalmente protegidos», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 167-190.

ROVIRA DEL CANTO, E., «Tratamiento penal sustantivo de la falsificación informática», en *Cuadernos de derecho judicial*, 10, 2001, 457-508.

ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Granada, 2002.

RUEDA MARTÍN, M.A., *Protección penal de la intimidad personal e informática*, Barcelona, 2004.

RUIZ MARCO, *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*, Madrid, 2001.

SÁNCHEZ GARCÍA DE PAZ, I./BLANCO CORDERO, I., «Problemas de derecho penal internacional en la persecución de delitos cometidos a través de Internet», en *Actualidad Penal*, 7, 2002, 165-192.

SIERRA LÓPEZ, M.V, *Análisis jurídico-penal de la publicidad engañosa en Internet*, Valencia, 2003.

SILVA SÁNCHEZ, J.M., «La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad», en *Cuadernos de derecho judicial*, 9, 2002, 113-141.

ZÚÑIGA RODRÍGUEZ, L./MÉNDEZ RODRÍGUEZ, C./DIEGO DÍAZ-SANTOS, M.R. (Coord.), *Derecho penal, sociedad y nuevas tecnologías*, Madrid, 2001.

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos

Esther Morón Lerma
Titular de Derecho Penal. Universidad Autónoma de Barcelona

I. **Introducción**

Internet se ha consolidado como pieza clave de la infraestructura mundial de la información y desempeña un papel crucial en el desarrollo económico. Algunos de los avances técnicos proporcionados por las redes telemáticas de comunicación podrían sintetizarse en la enorme facilidad y rapidez con la que se accede, copia, modifica y distribuye información, a distancia y desde la intimidad. Estas características han hecho de Internet una herramienta insustituible para cualquier tipo de usuario[1]. En la actualidad, los sistemas informáticos resultan de extraordinaria importancia para organismos públicos, infraestructuras básicas, sanidad (en su vertiente de gestión y de investigación científica[2]), particulares y, por supuesto, empresas. En este sentido, la integración de Internet en las actividades empresariales y el proceso de globalización que caracteriza la economía moderna han permitido nuevas formas de organización de la producción y de la comercialización[3].

---

[1] La doctrina destaca, unánimemente, la afectación transversal de Internet. *Vid*., al respecto, entre otros., Morales Prats, F., «Internet: riesgos para la intimidad», en *Internet y derecho penal*, CGPJ, CDJ, X, 2001, p. 70; Matellanes Rodríguez, N., «Algunas notas sobre las formas de delincuencia informática en el Código Penal», en *Hacia un derecho penal sin fronteras* (Diego Díaz-Santos/Sánchez López, Coord.) Colex, 2000, p. 129; Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, «Derecho penal e Internet», en *Régimen jurídico de Internet* (Cremades/Fernández-Ordóñez/Illescas, Coord.), Madrid, 2002, p. 257.

[2] Baste citar, como ejemplo paradigmático, la influencia que ha tenido el uso de específicos programas informáticos en la secuenciación del genoma humano.

[3] Ello permite, entre otras ventajas, la toma de decisiones con un considerable ahorro de tiempo. Así, por ejemplo, en 1995, un número de *Business Week,* ensalzaba la alta competitividad de la empresa Inditex, al ser capaz de concebir un modelo y ponerlo a la venta en sólo diez días. En el análisis de su éxito, se señalaba como esencial la rapidez de adaptación a los gustos del mercado, lo que le había permitido aumentar su «círculo de clientela» a costa de otro grande de la confección, Benetton, en ciudades importantes como París o Nueva York. Y tomando como punto de partida la pieza clave del éxito comercial de Inditex, baste reproducir las sugestivas reflexiones de Terceiro, J.B., *Socied@d Digi@tl,* Madrid, 1996,

Lo anterior conduce a que, en casi todos los ámbitos de la vida, se dependa, de forma parecida, de la tecnología informática y telemática y de los bancos de datos[4]. Y a medida que las redes de comunicación se hacen más convergentes y prestan mayores servicios, aumenta, también, su vulnerabilidad, de modo que ambos factores —dependencia y vulnerabilidad— se han ido incrementando progresivamente desde los años 90[5]. Por tanto, se trata de una tendencia que implica numerosas ventajas pero que también va acompañada de nuevos riesgos.

En general, los riesgos generados por Internet pueden reconducirse a dos grandes categorías. En primer lugar, las amenazas sobre bienes jurídicos tradicionales cuya peculiaridad deriva del empleo de las nuevas tecnologías informáticas. Así, por ejemplo, en la protección de la intimidad, los peligros derivados del empleo de *sniffer*s, programas espía, etc; en el caso del patrimonio, de las técnicas de *phishing*, *pharming*; en los supuestos de pornografía infantil, las nuevas formas de producción y distribución de material a través del uso de *webcam*s, móviles, plataformas *P2P*, canales *Chat*, comunidades virtuales, correo electrónico, etc.; y, por último, en la tutela de los derechos de autor, el especial impacto que ha tenido en los mismos la generalización y comercialización de aparatos de grabación que permiten copias masivas, la utilización de las plataformas *P2P*, etc.

En segundo lugar, los riesgos que pesan sobre las propias infraestructuras informáticas cuando son atacadas con el objetivo de alterar o impedir el normal funcionamiento de los sistemas de información. Estos

---

pp. 215-216, sobre las consecuencias que conllevaría reducir aún más ese corto espacio de tiempo (diez días) entre la ideación, producción y comercialización del bien. Pensemos en una cadena de ropa que desarrolle nuevos estilos o modas: empleados con videocámaras acuden a las principales exhibiciones de moda en todo el mundo. Si encuentran una prenda que creen que encaja en su nicho de mercado, envían electrónicamente el vídeo a la oficina central, donde se seleccionan los diseños prometedores, que son detallados y creados en formato digital y mandados a copiar, con especificaciones de material y color, a productores de Hong Kong, Korea, Singapur y Taiwan. Los proveedores, a su vez, envían por avión un juego de muestras. Si se decide ir adelante, se hace el pedido telemáticamente. La empresa puede tener un nuevo modelo en la tienda en menos de ocho días. Se ha reducido el tiempo en más del 20%, logro que puede determinar la ventaja competitiva de esa empresa (*vid*., exhaustivamente, Morón Lerma, E., *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías,* Navarra, 2002, pp. 174 y ss.)

[4] Así Carrión Zorzoli, H., señala que sin la informática las sociedades actuales se colapsarían, generándose lo que se conoce como la *computer dependency*, en «Presupuestos para la incriminación del hacking», en *Revista de Derecho Informático*, n.º 37, agosto 2001, p. 2. *Vid*., en igual sentido, Rovira del Canto, E., *Delincuencia informática y fraudes informáticos*, Granada, 2002, p. 9.

[5] Morón Lerma/Rodríguez Puerta, «Traducción y breve comentario del Convenio sobre Cibercriminalidad», en *Revista de Derecho y Proceso Penal*, n.º 7, 2002, p. 167 y Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, «Derecho penal e Internet», en *op. cit.,* p. 257.

incidentes suelen ejemplificarse en conductas como el acceso no autorizado, la difusión de programas informáticos perjudiciales —en sus múltiples modalidades de «virus», «bombas lógicas», «caballos de troya», «gusanos»— y los ataques intencionados de «denegación de servicio» (DoS), que perturban los servicios ofrecidos por Internet y pueden causar daños a las empresas que cuentan con un portal propio desde el cual realizan operaciones con sus clientes.

En cualquier caso, las diversas manifestaciones de conductas abusivas vinculadas a las tecnologías informáticas han planteado importantes retos y desafíos jurídicos, frente a los cuales ha habido ya respuestas normativas, de ámbito estatal e internacional.

Por lo que se refiere a los delitos objeto de este comentario, también se ha reaccionado legislativamente. Sin embargo, sigue reinando cierta confusión en cuanto a la naturaleza de estos ilícitos y a la interpretación de algunos de sus elementos. Probablemente, esas incertidumbres desvelan un interrogante mayor que surge en este ámbito con especial nitidez, a saber, si está aflorando un nuevo interés —vinculado a los sistemas de información— merecedor de reproche penal y, en ese caso, cómo debe arbitrarse su tutela.

Buena muestra de esa situación de incertidumbre resulta el propio título del trabajo, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos»[6], rúbrica hasta ahora extraña para el Derecho Penal español. Dicha nomenclatura proviene de instrumentos internacionales atinentes a la materia y, como norma paradigmática de todos ellos, el Convenio de Cibercriminalidad, suscrito en Budapest, el 23 de noviembre de 2001[7], que expresamente contempla, en su título primero, las «Infracciones contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos». En concreto, se prevén en el mismo las conductas de acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad de los sistemas y abuso de equipos e instrumentos técnicos. Estos ilícitos han sido objeto de regulación, en términos similares, por la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

Teniendo en cuenta esas directrices legislativas internacionales, conviene ya acotar el contenido de lo que debemos entender por «delitos

---

[6] Este trabajo se corresponde con la conferencia impartida en Bilbao, en el marco de las IV Jornadas de Derecho Penal en Homenaje a José María Lidón «Delito e Informática: algunos aspectos», cuyo título fue propuesto por la organización.

[7] Para un breve comentario sobre el mismo, *vid*. Morón Lerma/Rodríguez Puerta, «Traducción y breve…», *op. cit*., pp.178 y ss.

contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos». Y, en esencia, dichos delitos engloban las conductas de «acceso ilícito»[8] o «acceso ilegal a los sistemas de información»[9] (conocidas también como conductas de mero intrusismo informático o de *hacking*), las conductas de «atentados contra la integridad de los datos»[10] o «intromisión ilegal en los datos»[11] y «atentados contra la integridad del sistema»[12] o de «intromisión ilegal en los sistemas de información»[13] (conductas estas últimas reconducidas hasta el momento, en nuestro derecho, a las de daños informáticos).

De ahí que, metodológicamente, se haya decidido estudiar ambas conductas por separado: acceso ilegal o no autorizado, de una parte y atentados contra los datos y sistemas, de otra. A tal efecto, se examinará, respecto de cada una de ellas, la normativa internacional y europea referida a la materia. Tras lo anterior, se formulará un breve análisis de derecho comparado, ceñido a los países más próximos de nuestro entorno, al objeto de comprobar si se detecta alguna tendencia político-criminal al respecto. Seguidamente, se estudiará el Código Penal español vigente. A continuación, se dará cuenta de los cambios que opera en estos delitos el reciente Proyecto de reforma del Código Penal. Y, por último, se formularán algunas conclusiones.

Empezaremos por la primera de dichas conductas, a saber, la de acceso ilegal o no autorizado a los sistemas de información.

II. **Conductas de acceso ilegal o no autorizado a los sistemas de información**

1. *Marco internacional y europeo*

A) Consideraciones generales

Es éste uno de los ámbitos de criminalidad que ha merecido una respuesta inmediata por parte de la comunidad internacional. Múltiples han sido las iniciativas emprendidas por organismos internacionales y, en

[8] Ésta es la terminología empleada por el Convenio de Cibercriminalidad, en su artículo 2 (en adelante, CCiber.).

[9] Ésta es la terminología empleada por la Decisión Marco 2005/222, de 24 de febrero de 2005, en su artículo 2 (en adelante, DM 2005/222).

[10] Ésta es la terminología empleada por el CCiber, en su artículo 4.

[11] Ésta es la terminología empleada por la DM 2005/222, en su artículo 4.

[12] Ésta es la terminología empleada por el CCiber, en su artículo 5.

[13] Ésta es la terminología empleada por la DM 2005/222, en su artículo 3.

concreto, por las Naciones Unidas, la OCDE, el G8 y la Unión Europea[14], entre las que, a los efectos que interesan, destacan dos, a saber, el Convenio de Cibercriminalidad suscrito en el marco del Consejo de Europa y la Decisión Marco 2005/222, de 24 de febrero, relativa a los ataques a los sistemas de información, en el ámbito europeo.

Esta acción internacional se justifica en el serio peligro que suponen los ataques contra los sistemas de información, para la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia. No obstante, debe subrayarse que otras circunstancias relacionadas con las anteriores han contribuido notablemente a este impulso.

De una parte, la dimensión transnacional y transfronteriza del fenómeno. Los ataques contra los sistemas de información pueden lanzarse desde cualquier parte del planeta en la que uno se halle hacia el resto del mundo, lo que plantea la necesidad de abordar la aproximación de las legislaciones penales.

De otra, la preocupación grave que por el uso que de Internet puedan hacer organizaciones criminales y, sobre todo, tras lo ocurrido el 11-S en Nueva York, organizaciones terroristas[15]. En efecto, tanto el Convenio de Cibercriminalidad como la Decisión Marco atribuyen la existencia de ataques contra los sistemas de información, en particular, a la amenaza de la delincuencia organizada y se hacen eco de la creciente inquietud ante posibles ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros[16]. Asimismo, se advierte, desde estas normas, que la distancia y las divergencias significativas que existen entre las legislaciones de los Estados miembros puede dificultar la lucha contra la delincuencia organizada y el terrorismo y complicar la cooperación eficaz de los servicios de policía y las administraciones de justicia en materia de ataques contra los sistemas de información[17].

En virtud de lo anterior, esto es, al objeto de contribuir a la «lucha contra el terrorismo y la delincuencia organizada»[18], se reclaman medi-

---

[14] *Vid.* Plan de Acción europeo relativo a «Seguridad de las Redes y de la Información: Propuesta para una perspectiva política europea» [COM (2001) 298] y Resolución del Consejo de la Unión Europea, de 6 de diciembre de 2001, sobre planteamiento común y acciones específicas en el ámbito de la seguridad en la Red y en la información.

[15] *Vid*., exhaustivamente, Morales Prats, F., «Los ilícitos en la Red (II): Pornografía infantil y ciberterrorismo», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona, C.M., Coord.), Granada, 2006, pp. 273 y ss.

[16] *Vid*. Considerando (2) de la DM.

[17] *Vid*. Considerando (5) de la DM.

[18] *Vid*. Considerando (8) de la DM.

das legislativas contra este tipo de delincuencia, lo que implica definiciones, tipificaciones y sanciones comunes[19].

Se constata, en efecto, una voluntad férrea de fomentar definiciones comunes de los elementos normativos de los tipos penales (concepto de «datos informáticos», de «sistemas informáticos», etc.), de los elementos constitutivos de las infracciones penales («acceso no autorizado» e «intromisión ilegal en datos y sistemas») y de que se prevean para los mismos sanciones proporcionadas, eficaces y disuasorias, como instrumento de lucha contra el ciberterrorismo[20].

Teniendo en cuenta el marco general descrito que ha presidido el nacimiento de esta normativa, procede ya concentrarse en el examen de algunos de esos elementos objeto de armonización.

B) Convenio de Cibercriminalidad[21]

El Convenio sobre Cibercriminalidad ha optado por aglutinar en un título autónomo (Capítulo II, Sección 1, Título 1) las «infracciones contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos» y, posteriormente, en otro título distinto (Capítulo II, Sección 1, Título 2), las «infracciones informáticas». Se trata de una sistemática diferente a la seguida por el Código Penal español, que

---

[19] La DM pretende ser el complemento a los trabajos del G8 sobre la cooperación transnacional en el ámbito de la delincuencia de alta tecnología, que ya dieron lugar a la Comunicación de la Comisión Europea sobre «Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de la información y la lucha contra los delitos informáticos», Bruselas, 26.01.2001, COM (2000) 890 final.

[20] Morales Prats, F. «Los ilícitos en la Red (II): Pornografía infantil…», *op. cit.*, p. 274.

[21] El Convenio sobre Cibercriminalidad, adoptado por el Consejo de Europa, se abrió a la firma en Budapest el 23 de noviembre de 2001 (http://coe.conventions.int). Hasta el momento, ha sido firmado y ratificado por 18 Estados miembros del Consejo de Europa (Albania, Armenia, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Francia, Hungría, Islandia, Lituania, Holanda, Noruega, Rumania, Eslovenia, Macedonia y Ucrania). Asimismo, ha sido ratificado por Estados Unidos. Por tanto, cumplido el quórum requerido por el propio Convenio para su eficacia, esto es, la ratificación por 5 Estados, tres de los cuales deben ser miembros del Consejo de Europa, el Convenio está en vigor para los países mencionados. Sin embargo, dicha norma ha sido firmada pero no ratificada por 20 Estados miembros del Consejo de Europa (Austria, Bélgica, República Checa, Finlandia, Alemania, Grecia, Irlanda, Italia, Latvia, Luxemburgo, Malta, Moldavia, Polonia, Portugal, Serbia, Eslovaquia, España, Suecia, Suiza y Reino Unido) y por 4 Estados no miembros del Consejo (Canadá, Japón, Montenegro y Sudáfrica), para los cuales el Convenio no ostenta aún fuerza vinculante. El estado actual de firmas y ratificaciones del Convenio puede consultarse en http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/04&CL=ENG.

contempla algunas de dichas conductas (interceptación, atentados a la integridad de los datos, abuso de dispositivos), como modalidades comisivas en preceptos destinados a proteger, fundamentalmente, otros bienes jurídicos (intimidad, intereses económicos vinculados a los secretos empresariales, intereses atinentes a la propiedad intelectual, intereses relativos a la función pública).

Concretamente, la conducta de «acceso ilícito» se halla prevista en el artículo 2, que reza como sigue:

> «Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Los Estados podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático».

El «acceso ilícito» (artículo 2 Ccibcr.) según se halla recogido en el Convenio en el primer inciso, es decir, como modalidad delictiva desprovista de cualquier intención específica, constituye una conducta impune en derecho español.

En el siguiente inciso, se contempla la posibilidad de que los Estados firmantes exijan la comisión de la conducta delictiva con vulneración de medidas de medidas de seguridad, con concurrencia de especiales elementos subjetivos o en un sistema informático conectado a otro.

No puede abundarse, en este momento, en una valoración crítica de dicha regulación[22]. Sin embargo, baste señalar que, en el segundo de los casos mencionados —esto es, exigiendo la comisión de la conducta delictiva con propósitos adicionales, como, por ejemplo, la intención de obtener los datos—, estaríamos ante de un delito contra la intimidad o contra los secretos de empresa, que se hallan previstos como tales infracciones en el Código Penal español, en los artículo 197.1 y 278.1, respectivamente.

En cuanto a las otras dos previsiones del segundo inciso (vulneración de medidas de seguridad y conexión del sistema a otro sistema), tampoco encuentran acomodo en la literalidad del derecho español.

---

[22] Para una valoración crítica de dicha regulación, *vid*. Morón Lerma, E., *Internet y derecho penal: hacking y otras conductas ilícitas en la Red,* 2.ª edición, Navarra, 2002, pp. 70 y ss.

C) Decisión Marco 2005/222, de 24 de febrero, relativa a los ataques a los sistemas de información[23]

La conducta de acceso ilegal a los sistemas de información está prevista en el artículo 2, que prevé lo siguiente:

> «1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
>
> 2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad».

Conforme a la Decisión Marco, los Estados miembros deberán sancionar como infracción penal el acceso ilegal a los sistemas de información. La DM contiene una redacción semejante a la del Convenio de Cibercriminalidad, aunque más acertada desde un punto de vista de técnica legislativa.

Al respecto, baste destacar un par de cuestiones. De una parte, se infiere que el acceso ilegal a los sistemas de información debe ser entendido como un acceso doloso y no autorizado al conjunto o a una parte de un sistema de información. Se destierran, pues, concepciones que contribuyen a desdibujar el marco teórico de esta conducta, exigiendo para la comisión del delito la presencia de elementos subjetivos, tales como la intención de obtener los datos o de causar un daño. De otra, se permite que los casos de menor gravedad no queden sometidos a reproche penal. En este sentido, se insta desde el Preámbulo a que no se produzca una tipificación penal excesiva[24]. A ello parece dirigirse, también, la facultad otorgada a los Estados para exigir que la conducta se cometa transgrediendo medidas de seguridad, como instrumento a través del cual reivindicar un plus de gravedad.

Por tanto, de dicha normativa pueden extraerse dos importantes conclusiones que convendrá tener presentes. De una parte, la definición de la conducta como el acceso intencionado sin autorización a un sistema informático. De otra, la necesidad de respetar el principio de intervención mínima y de evitar una sobrecriminalización en la regulación de esta conducta.

A continuación, se formulará una breve perspectiva acerca de cómo se halla regulado este comportamiento en algunos países de nuestro entorno.

---

[23] La DM entrará en vigor el 17 marzo de 2007.

[24] *Vid*. Considerando (13) de la DM.

2. *Derecho comparado*

A) Francia

Francia es uno de los Estados que ha regulado con mayor profusión las conductas vinculadas a los abusos informáticos. En 1988, se aprobó la Ley n.º 88-19, de 5 de enero, sobre el fraude informático, en cuya virtud se introdujo, en el Código Penal entonces vigente, el acceso fraudulento a un sistema de tratamiento automático de datos, la alteración indebida de datos, los daños informáticos y la falsificación de documentos informáticos[25].

En la actualidad, el Código Penal francés de 1992 —en vigor desde el 1 de marzo de 1994— ha mantenido básicamente dicha regulación. Esas conductas se hallan contempladas en un capítulo autónomo, rubricado «De los atentados contra los sistemas de tratamiento automatizado de datos» (Capítulo III), ubicado en el Título II («Otros atentados contra los bienes»), del Libro III («Crímenes y delitos contra los bienes»). Las principales novedades del Código Penal de 1992 se cifraron en el incremento de las penas de los diversos delitos, la introducción, en este ámbito, de la responsabilidad de las personas jurídicas y la inclusión de nuevos ilícitos, como, por ejemplo, el delito de tenencia, importación, ofrecimiento, venta o puesta a disposición de instrumentos concebidos específicamente para la comisión de las conductas reguladas en este capítulo[26].

Así pues, la conducta de acceso ilícito, tipificada en el art. 323-1 CP, establece lo siguiente:

> «El acceso o mantenimiento, fraudulentamente, en todo o en parte de un sistema de tratamiento automatizado de datos se castigará con pena de dos años de cárcel y multa de 30.000 euros[27].
>
> Cuando como resultado se produzca la supresión o la modificación de datos contenidos en ese sistema o una alteración del funcionamiento del sistema, la pena será de tres años de cárcel y multa de 45.000 euros[28]».

Se castiga, pues, la conducta de acceso ilícito y únicamente se exige que el acceso sea fraudulento, entendiéndose por tal cualquier modo de penetración irregular en un sistema automático de datos.

---

[25] Artículos 462.2 a 462.6 del antiguo Código Penal francés.

[26] Este precepto fue introducido en 2004, por la Ley n.º 2004-575, de 21 de junio.

[27] En la anterior redacción, la pena era de un año de cárcel y multa de 15.000 euros.

[28] En la anterior redacción, la pena era de dos años de cárcel y multa de 30.000 euros.

Sin embargo, no se requiere ni la presencia de tendencias subjetivas en el ánimo del sujeto ni tampoco la vulneración de especiales medidas de seguridad.

Además, se sanciona la producción de daños contra los datos contenidos en ese sistema o contra el propio sistema al que se accede. En este caso, se sanciona la conducta más gravemente cuando quien lleva a cabo el acceso ocasiona de forma sobrevenida daños sobre los datos o el sistema. Éste parece ser el ámbito de vigencia del art. 323-1, segundo inciso CP, dado que el castigo autónomo de tales conductas, llevadas a cabo de forma intencionada, se prevé en preceptos posteriores[29].

B) Italia

En el ordenamiento penal italiano, el acceso ilícito a un sistema informático constituye un comportamiento punible desde 1993. Concretamente, este delito fue introducido por la Ley n.º 547, de 23 de diciembre de 1993, relativa a las modificaciones e integraciones en las normas del Código Penal y de la Ley de Enjuiciamiento Criminal en materia de criminalidad informática[30].

El artículo 615 *ter* CP italiano, regulador del acceso abusivo a un sistema informático o telemático, se halla ubicado sistemáticamente en la Sección IV, relativa a los delitos contra la inviolabilidad del domicilio, integrada en el Capítulo III («Delitos contra la libertad individual») del Título XII («Delitos contra la persona»).

El artículo 615 *ter* CP italiano establece:

> «El que abusivamente se introduzca en un sistema informático o telemático protegido por medidas de seguridad o bien se mantenga contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo, será castigado con pena privativa de libertad de hasta tres años».

Asimismo, este precepto contiene algunos tipos agravados, entre los cuales reviste especial interés el siguiente:

> «Será castigado con pena de cárcel de 1 a 5 años: (…)
> 3) si del hecho se deriva la destrucción o el daño del sistema o la interrupción total o parcial de su funcionamiento, o bien la destruc-

[29] *Vid.* arts. 323-2 y 323-3 CP.

[30] En concreto, *vid*. art. 4 de la Ley n.º 547, de 23 de diciembre de 1993.

> ción o el daño de los datos, de la información o de los programas contenidos en él (…)[31]».

La regulación del delito de acceso abusivo en el Código Penal italiano sugiere algunas reflexiones. En primer lugar, destaca la ubicación sistemática de este ilícito entre los delitos destinados a proteger la inviolabilidad del domicilio. De ahí que gran parte de la doctrina[32] y de la jurisprudencia[33] consideren el «domicilio informático» como el bien jurídico protegido en este delito[34].

Por otra parte, el Código Penal italiano exige que el sistema se halle protegido con «medidas de seguridad». La exigencia de que la conducta sea cometida con vulneración de medidas de seguridad plantea interesantes problemas (concepto de medida de seguridad, exigencia de un determinado nivel de eficacia o adecuación de las mismas, entidad autónoma o carácter instrumental de las mismas, entre otros) que, sin embargo, no pueden abordarse en este momento.

En derecho italiano, el legislador entiende por tales —según la Relación Ministerial de acompañamiento a la Ley n.º 547 de 1993— aquellos

---

[31] El texto íntegro del art. 615 *ter* del CP italiano es el siguiente:

«Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio».

[32] En la literatura italiana, *vid*. Borruso, R., en R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, *Profili penali dell'informatica*, Giuffré, Milano, 1994, p. 28.

[33] Así, por ejemplo, sentencia *Cass. Pen.* 3067/1999 y, recientemente, sentencia *Trib. Pen. Bologna, I Sez*, 21.07.2005.

[34] No puede abundarse en el análisis de esta interesante cuestión, aunque, posteriormente, al formular las conclusiones se llevará a cabo una breve consideración crítica al respecto.

medios de protección lógicos o físicos, materiales o personales, que revelen la voluntad del titular de reservar el acceso y/o la permanencia en el sistema a aquellas personas que él autorice.

Por último, debe subrayarse que, al igual que el Código Penal francés, existe un tipo agravado para el supuesto de que con el acceso se ocasionen daños sobre los datos o el sistema, previsión objeto de crítica en la literatura italiana[35].

C) Alemania

En Alemania, la Segunda Ley para la Lucha contra la Criminalidad Económica (*2.ª WiKG*), de 15 de mayo de 1986, introdujo en el Código Penal diversos ilícitos vinculados a los abusos informáticos. Así, por ejemplo, el espionaje de datos (§ 202a *StGB*), el fraude informático (§ 263a *StGB*), la alteración de datos (§ 303a *StGB*) y el sabotaje informático (§ 303b *StGB*).

Con carácter general, se considera que el acceso ilícito se halla previsto en el parágrafo destinado a regular el espionaje de datos (202a *StGB*)[36], que establece lo siguiente:

> «(1) El que, sin estar autorizado, se procure para sí o para otro, datos que no están destinados a él y que se hallan especialmente asegurados contra el uso indebido, será castigado con pena privativa de libertad de hasta tres años o con pena de multa.
>
> (2) Sólo constituyen datos a los efectos del párrafo anterior los almacenados o transmitidos de modo electrónico o magnético o, por lo demás, de modo no inmediatamente perceptible».

Como puede observarse, el delito del § 202a *StGB* castiga el espionaje informático, esto es, el acceso ilícito a datos contenidos en soporte informático. Este precepto se halla ubicado en la Sección decimoquinta, reguladora de la violación de la vida personal y de la privacidad, que contempla un amplio elenco de conductas atentatorias del derecho a la

---

[35] Esta circunstancia agravante ha sido censurada, por castigar la mera producción del daño sobre datos o sistemas, bastando que el resultado dañoso sea causalmente conectable a la conducta material. Así, *vid*. Muciarelli, F., «Commento all'art.4 della legge n.547 del 1993», en *Legislazione Penale*, 1996, p. 109 y Perfetti, T. «Del delitto di accesso abusivo ad un sistema informatico o telematico (art. 615 ter cp)», en *ScintLex, Diritto e Società dell'Informazione* (www.scintlex.it), p.4.

[36] Así, *vid*. González Rus, J.J., «Los ilícitos en la Red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en *El cibercrimen: nuevos retos jurídico-penales…, op. cit.,* p. 244.

intimidad, como, por ejemplo, la grabación clandestina de voz o imagen (§ 201 *StGB*) y el apoderamiento de documentos en soporte material (escritos, cartas, etc.) (§ 202 *StGB*). Así, *prima facie*, el ilícito previsto en el § 202a *StGB* constituye otra de las formas posibles de vulnerar la intimidad cifrada en acceder de forma ilícita a datos almacenados o transmitidos en un equipo de proceso electrónico.

Sin embargo, la doctrina alemana considera que, en este caso, no se protege la esfera privada sino un interés formal en la conservación del secreto de la persona autorizada a disponer de los datos[37].

En cualquier caso, sin poder abundar en el examen de esta cuestión, lo que resulta indudable es que el precepto castiga a quien de modo no autorizado se procure a sí mismo o a otro datos que no van dirigidos a él y que están especialmente asegurados contra un acceso indebido. Por tanto, no parece que este delito esté dirigido a sancionar el mero acceso ilícito a un sistema, sino a datos especialmente protegidos.

De ahí que, a mi juicio, no pueda entenderse que este precepto castiga de forma expresa y autónoma el acceso ilegal a sistemas de información, a salvo de adoptar una definición de acceso que no se corresponde con la propuesta por la DM.

D) Portugal

En Portugal, la Ley n.º 109/91, de 17 de agosto de 1991, sobre Criminalidad Informática, desarrolló exhaustivamente los comportamientos ilícitos vinculados a las nuevas tecnologías de la comunicación. Así, en el Capítulo II, se tipifican diversos delitos como, por ejemplo, la falsedad informática (art. 4), los daños a datos o programas informáticos (art. 5), el sabotaje informático (art. 6), el acceso ilegítimo (art. 7), la interceptación ilegítima (art. 8) y la reproducción ilícita de programas protegidos (art. 8).

Concretamente, el artículo 7 regula el acceso ilegítimo del siguiente modo:

> «1. Quien, sin autorización, y con la intención de obtener, para sí o para un tercero, un beneficio o ventaja ilícita, acceda de cualquier modo a un sistema o red informática, será castigado con pena de privativa de libertad de hasta un año o multa de hasta 120 días.
>
> 2. Si el acceso se llevase a cabo con violación de medidas de seguridad, la pena de prisión será de hasta tres años o multa.

---

[37] Así, *vid*. Möhrenschlager, M.E., «El nuevo derecho penal informático en Alemania», en Mir Puig, S. (Comp.), *Delincuencia informática*, Barcelona, 1992, pp.137-138.

3. La pena de prisión será de uno a cinco años cuando:
a) Mediante el acceso, el autor haya tenido conocimiento de secretos comerciales o industriales o de datos confidenciales protegidos por la ley;
b) El beneficio o ventaja patrimonial obtenidos fuese de un valor considerablemente elevado, (…)».

La regulación del delito de acceso ilícito en derecho portugués merece algunas reflexiones críticas. De una parte, la modalidad básica contiene un elemento de tendencia subjetiva cifrado en obtener, para sí o para tercero, un beneficio o ventaja ilícita, previsión que suscita problemas. En esas hipótesis, en las que se persigue algún otro propósito, el acceso se convertirá en *modus operandi* de otros ilícitos, perdiendo entidad como ilícito autónomo. Y, en este caso, en que el elemento relativo a la obtención del provecho o la ventaja será interpretado en términos patrimoniales, se producirán solapamientos normativos y concursos de normas con los delitos de esa naturaleza[38].

De otro lado, la agravante incriminada en el párrafo 3 a), exige que el autor haya tenido conocimiento de secretos comerciales o industriales o de datos confidenciales, lo que supone introducir elementos extraños al acceso, al margen de los problemas exegéticos respecto de si por «datos confidenciales», deberá entenderse datos personales o empresariales. Surgen dudas, también, sobre el fundamento de la agravante. Podría considerarse que radica en que el autor ha tomado conocimiento *de forma imprudente* de los datos, hipótesis que no parece muy viable. De otro lado, cabría pensar que el autor ha accedido dolosamente a los secretos empresariales o datos confidenciales, en cuyo caso deberían aplicarse esos otros delitos consistentes en descubrir secretos. Por tanto, se trata de un previsión que originará problemas concursales y que, incluso, podría llegar a comprometer el principio de *non bis in idem*.

E) Conclusiones

El panorama legislativo expuesto permite constatar una reacción legislativa generalizada frente a la criminalidad informática. Ante la inadecuación e insuficiencia de las legislaciones penales tradicionales para combatir este fenómeno, se han aprobado por parte de la mayoría de los países de nuestro entorno leyes específicas destinadas a regular esta materia.

[38] La agravante prevista en el párrafo 3 b), aconseja interpretar dicho elemento subjetivo en clave patrimonial.

En concreto, por lo que se refiere a las conductas de acceso ilícito, se detecta una clara tendencia criminalizadora al respecto. Sin embargo, la regulación de este delito es concebida de forma dispar respecto a su ubicación sistemática (en la mayor parte de casos se reconduce al derecho a la intimidad en sus diversas vertientes —intimidad personal, intimidad domiciliaria[39]—), a los elementos que configuran su definición (medidas de seguridad, elementos subjetivos) y a las circunstancias que pueden agravar esa conducta (daños a los datos; conocimiento de secretos comerciales, industriales o personales; ventajas patrimoniales, etc.).

A continuación, corresponde examinar qué encaje tienen las conductas de acceso ilícito en Derecho Penal español.

3. *Derecho español vigente*

Las conductas de mero intrusismo informático, esto es, conductas de acceso no autorizado a sistemas informáticos, despojadas de cualquier elemento de tendencia subjetiva ulterior y distinto al acceso mismo, no gozan de una protección específica y autónoma en el nuevo Código Penal[40].

Sin embargo, esa falta de tipificación expresa no supone la impunidad, en todo caso, de accesos no autorizados a un sistema informático ajeno[41].

Puede ocurrir que el acceso persiga un propósito ulterior y más grave, en cuyo caso la intrusión se concibe como un medio necesario para atacar otros intereses. Así, por ejemplo, se accede para vulnerar la intimidad ajena, destruir datos, apoderarse de un secreto de empresa, descubrir un documento secreto relativo a la Administración Pública, entre otros. En estos casos, la conducta queda consumida por estos delitos, como fase o estadio típico inicial de los mismos. La principal dificultad radicará en la prueba del elemento subjetivo, esto es, del ánimo que ha guiado esas conductas, mediante el correspondiente juicio de inferencias[42].

---

[39] Es así en todos los ordenamientos, excepto en el caso del derecho francés.

[40] De este parecer se muestran los escasos pronunciamientos jurisprudenciales, a saber, el Auto de 29.1.2002 (J.I. n.º 2 Lorca); Sentencia de 28.5.1999 (J.P. n.º 2 Barcelona) (caso Hispahack), en la que, sin embargo, se aboga por una futura incriminación autónoma del acceso ilícito. Y, recientemente, Sentencia de 15.02.2006 (J.P. Extremadura, Badajoz), aunque en ella se considera que el descubrimiento de *passwords* integra la conducta de interceptación, prevista en el art. 197.1 CP.

[41] Así, *vid*., en igual sentido, González Rus, J.J., «Los ilícitos en la Red (I): hackers, crackers…», *op cit.,* p. 246.

[42] Es decir, la dificultad radicará en demostrar que no se obra sólo con un deseo de demostración de pericia técnica, sino también con la finalidad, pongamos por caso, de apoderarse de un secreto de empresa.

Por tanto, los accesos no autorizados, concebidos como medio comisivo para obtener resultados ulteriores más graves, encuentran encaje en las correspondientes figuras típicas, respecto de las cuales hay consenso en torno a su punición[43].

Ahora bien, frente a la falta de incriminación expresa de los accesos ejecutados sin adicionales propósitos, han surgido en España propuestas tendentes a reconducir su castigo a los tipos penales existentes. En concreto, se postula el encaje del intrusismo en los delitos contra la intimidad (concretamente, en el art. 197.1 CP)[44]. Se considera que las conductas desarrolladas por el *hacker* quebrantando las claves de acceso ponen de manifiesto, de manera palmaria, el dolo o ánimo específico requerido por esa figura delictiva, caracterizado por el ánimo tendencial de invadir la esfera de privacidad. Asimismo, se considera que las claves de acceso integran el derecho a la intimidad[45].

Desde nuestro punto de vista, dicha solución no resulta compartible por diversos motivos. De una parte, comporta deformar el marco teórico propuesto para el acceso, al presuponer que, en aquellos casos en los que se rompe una clave de acceso, se lleva a cabo siempre con el ánimo de descubrir la intimidad. Ya se ha insistido en que el acceso, en efecto, puede ser *modus operandi* de otros muchos delitos para los que se han propuesto diversas soluciones típicas, pero ni es siempre así ni en los casos en que se produce se ciñe a vulneraciones de la intimidad. Antes bien, puede romperse un *password* para descubrir secretos de empresa, para dañar los datos, etc.

De otro lado, tampoco parece convincente considerar, en todo caso, la contraseña como un dato que integra el derecho a la intimidad. Dicha cuestión dependerá de cuál sea la información utilizada para conformar el *password*. Generalmente, las claves de seguridad asumen carácter instrumental y adquieren sentido en la medida en que se vinculan con un bien jurídico que puede variar (derecho a la intimidad, secretos de empresa, intereses públicos, etc.), pero en el que no se integran necesariamente.

Por último, debe señalarse que, frente a estas dificultades para subsumir el acceso en el Código Penal español, se ha subrayado, desde algunos sectores, la conveniencia político-criminal de introducir un tipo

---

[43] Sobre el encaje que dichas conductas tienen en derecho español, *vid*., exhaustivamente, Morón Lerma, E., *Internet y derecho penal: hacking…, op. cit.*, pp. 54 y ss.

[44] Magro Servet, V., «La delincuencia informática. ¿Quién gobierna en Internet?», en *La Ley,* n.º 6077, 2 de septiembre de 2004, p.4.

[45] Así, por ejemplo, *vid*. De Alfonso Laso, D. «El hackering blanco. Una conducta ¿punible o impune?», en *Internet y derecho penal, op. cit.,* pp. 520-521.

penal autónomo para su castigo[46]. Y, en esa dirección se enmarca la normativa internacional (Convenio europeo sobre Cibercriminalidad) y comunitaria (Decisión-Marco 222/2005) reseñada, puesto que prevén, específicamente, la incriminación de esta conducta.

Fruto de lo anterior, el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 19/1995, de 23 de noviembre, del Código Penal, ha incorporado la conducta de acceso. Al estudio de dicha reforma se dedicará el epígrafe siguiente.

4. *Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 19/1995, de 23 de noviembre, del Código Penal*[47]

El Proyecto de reforma del Código Penal transpone la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información e incrimina, por primera vez, en el Código Penal español, las conductas de acceso ilícito.

En concreto, el apartado cuadragésimo tercero del artículo único del Proyecto, modifica el artículo 197 CP e introduce el acceso, en sede de delitos contra la intimidad[48].

En efecto, el proyecto incorpora un nuevo apartado 3 en el artículo 197 CP, desplazando los actuales apartados 3, 4, 5 y 6 a los puestos 4, 5, 6 y 7, respectivamente:

> «El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena privativa de libertad de seis meses a dos años».

La previsión del artículo 197.3 CP obedece al mandato armonizador contenido en la DM 2005/222 (artículo 2), que exige de los Estados miembros de la Unión Europea la adopción de «las medidas necesarias

---

[46] Así, por ejemplo, *vid*. Gutiérrez Francés, M.L., «El intrusismo informático (Hacking): ¿Represión penal autónoma?», en *Informática y Derecho*, vol. 12-15, pp. 1179-1180 y Mir Puig, C., «Sobre algunas cuestiones relevantes del Derecho Penal en Internet», en *Internet y derecho penal, op. cit.,* p. 303.

[47] El Proyecto de Ley 121/000119 Orgánica por la que se modifica la Ley Orgánica 19/1995, de 23 de noviembre, del Código Penal, puede consultase en el BOE de 15.01.2007.

[48] Se añade, también, una circunstancia agravante cifrada en la pertenencia a organización criminal.

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

Como se ha analizado previamente, la normativa europea y de derecho comparado en esta materia hacían insoslayable la adaptación del derecho español incriminando esta conducta. Sin embargo, la concreta regulación por la que se ha optado en el Proyecto merece algunas reflexiones críticas respecto de la ubicación sistemática y de algunos elementos (objeto material y elemento subjetivo).

1. En primer lugar, el legislador ha ubicado este delito en el Título X, destinado a los delitos contra la intimidad, lo que condiciona la selección e identificación del bien jurídico protegido, así como la interpretación de los distintos elementos típicos.

Respecto de la primera de las cuestiones apuntadas, el legislador ha considerado que el bien jurídico protegido con el castigo de estas conductas es el derecho a la intimidad. Al respecto, resulta esclarecedor lo manifestado en la Exposición de Motivos:

> «La tutela penal de la intimidad y de los secretos ha sido tradicionalmente fragmentaria, y condicionada a la realización de conductas de apoderamiento de papeles, cartas o mensajes, o de instalación de aparatos de captación de imagen o sonido, pero a la vez que la importancia fundamental de ese bien jurídico exige cada vez mayor atención y medidas legales, como son esencialmente las recogidas en la legislación sobre protección de datos, crecen los riesgos que lo rodean, a causa de las intrincadas vías tecnológicas que permiten violar la privacidad o reserva de datos contenidos en sistemas informáticos. Esa preocupante laguna, que pueden aprovechar los llamados *hackers* ha aconsejado, (…), incorporar al artículo 197 del Código Penal un nuevo apartado que castiga a quien por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático».

Se persigue proporcionar tutela a la intimidad y, en concreto, a la intimidad informática, frente a un nuevo tipo de riesgos, a saber, los suscitados por las conductas de acceso no autorizado a un sistema. No se ignora que la identificación del bien jurídico protegido en las conductas de acceso constituye una controvertida cuestión, pero, desde luego, no puede compartirse la opción plasmada en el Proyecto, como se razonará posteriormente[49].

[49] *Vid*. *infra,* apartado 2.5.

2. En segundo lugar, por lo que atañe al objeto material del delito, debe advertirse que la adaptación del art. 2 de la DM ha supuesto la ampliación de su ámbito típico. El tenor del nuevo apartado tercero castiga *el acceso sin autorización a datos* o programas informáticos contenidos en un sistema informático o en parte del mismo, mientras que la DM se refiere *al acceso al conjunto o a una parte del sistema informático,* sin mención expresa de los datos.

La DM define, en su artículo 1 a), los «sistema de información», como cualquier 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.

Por tanto, el concepto de «sistemas de información» adoptado es amplio, ya que incluye los datos que estos contienen. Ahora bien, cuando, en esa definición, la DM alude a «datos» parece hacer referencia a aquellos que resultan indispensables para que los programas y sistemas funcionen. En cambio, cuando la DM define «datos informáticos» alude a la representación de hechos, informaciones o conceptos.

Es decir, que los «datos» del art. 1 a) DM y los «datos informáticos» del art. 1 b) DM asumen contenido diverso.

De ahí que la amplitud con la que ha sido redactado el nuevo artículo 197.3 incluyendo el acceso a datos o programas informáticos resulte confusa[50]. En la exégesis del contenido de dicho objeto material caben, pues, dos posibilidades. De una parte, un entendimiento de los «datos» en el sentido expuesto, esto es, restringido a los datos o información necesaria para el correcto funcionamiento de los sistemas, en cuyo caso resultaría una interpretación forzada y contraria a la ubicación del precepto. De otra, interpretar el concepto de «datos» en toda su extensión, hipótesis que, sin embargo, desencadena los siguientes dislates y contradicciones.

El «acceso a datos» —sin limitación— ya se halla previsto en el artículo 197.2 del vigente Código Penal, que castiga, con pena privativa de libertad de uno a cuatro años y multa de doce a veinticuatro meses, a quien, sin estar autorizado, acceda por cualquier medio a los datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

---

[50] De opinión contraria se muestra Galán Muñoz, A. «Ataques contra sistemas informáticos», en *Boletín de Información, La Armonización del Derecho Penal español: una evolución legislativa,* Ministerio de Justicia, Suplemento al n.º 2015, 15 de junio de 2006, pp. 225 y ss.

Podría esgrimirse que el ámbito material de estos delitos no coincide, puesto que el art. 197.2 CP se ciñe a la protección de los datos de carácter personal y la nueva redacción del apartado tercero no, conclusión que, sin embargo, decae dada la ubicación sistemática de ambos.

Por tanto, se suscita la contradictoria situación de que el vigente art. 197.2, segundo inciso CP, castiga la misma conducta que el futuro art. 197.3, con dos perturbadoras particularidades. El art. 197. 3 CP exigirá un plus para su comisión cifrado en la vulneración de medidas de seguridad; pero, la pena que llevará aparejada —prisión de seis meses a dos años— es notablemente menor que la del art. 197.2 CP —prisión de uno a cuatro años y multa de doce a veinticuatro meses—.

La consecuencia es la creación de un subtipo especial privilegiado, de medios determinados, que supone una reducción del marco penal cuando la injerencia en el ámbito de la intimidad informática se perpetra mediante la neutralización o invalidación de las medidas de seguridad del sistema[51].

3. Por último, tampoco resulta satisfactoria la parte subjetiva del tipo. La inserción del acceso en el art. 197 CP y la simetría con el resto de modalidades típicas previstas en dicho artículo conducen a reclamar el elemento subjetivo del injusto cifrado en el ánimo de descubrir la intimidad, lo que desvirtúa la definición de acceso propuesta.

En suma, pues, la ubicación sistemática del precepto en sede de delitos contra la intimidad y la previsión autónoma del acceso «a datos» da lugar a solapamientos normativos y a dislates valorativos con otras modalidades típicas atentatorias de la intimidad informática, lo que merece una valoración crítica.

5. *Conclusiones respecto de la regulación de las conductas de acceso ilegal a los sistemas de información*

La importancia de las redes de comunicación, la complejidad y lesividad de la criminalidad informática, las directrices internacionales y comunitarias en la materia, así como la respuesta ofrecida por los países de nuestro entorno, obligan inexcusablemente al debate y al replanteamiento acerca de la necesidad de introducir un nuevo precepto penal,

[51] *Vid*., en igual sentido, Informe al Anteproyecto de Ley Orgánica por el que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, emitido por el Consejo General del Poder Judicial, Comisión de Estudios e Informes, en fecha de 18.10.2006, p.133. Puede consultarse en:
http://www.poderjudicial.es/eversuite/GetRecords?Template=cgpj/cgpj/principal.htm.

destinado a incriminar las conductas de acceso no autorizado a los sistemas de información.

Se trata de una controvertida cuestión, en la que lo prioritario debería ser la *identificación* (y/o decisión) *del interés* que se protege al castigar estas conductas. A nuestro juicio, algunas de las propuestas formuladas hasta ahora como la relativa a la intimidad[52], el «domicilio informático»[53] o ciertos intereses patrimoniales[54], no se muestran satisfactorias.

De esas propuestas la que, quizá, ha adquirido mayor predicamento es la que selecciona el domicilio informático como bien jurídico protegido, formulándose un paralelismo respecto de la protección otorgada al domicilio físico[55]. A nuestro parecer, dicho símil no resulta compartible por diversos motivos en los que ahora no puede abundarse. Sin embargo, baste subrayar la distinta arquitectura de ambas dimensiones (domicilio físico/domicilio informático), en la medida que la configuración técnica de los sistemas y redes informáticas, de naturaleza esencialmente abierta y descentralizada o distribuida, nada tiene que ver con la del domicilio físico, definido como un lugar cerrado, en el que existe una clara demarcación de sus límites y en el que estos no son meramente simbólicos, sino que representan un obstáculo efectivo para el acceso de terceros al interior[56]. El concepto de sistema informático es demasiado elástico y está compuesto por demasiados componentes como para ser encorsetado en estructuras físicas[57].

A mi juicio, la incriminación del acceso con carácter autónomo no tiene como objeto inmediato la tutela de la intimidad personal del titular o usuario del sistema de información, la confidencialidad de los datos incorporados al mismo o el patrimonio o intereses económicos del titular del sistema, aunque de forma mediata se vean todos ellos igualmente protegidos.

---

[52] Así, *vid*. Magro Servet, V., «La delincuencia informática…», en *La Ley,* n.º 6077, 2 de septiembre de 2004, p. 4 y De Alfonso Laso, D. «El hackering blanco…», en *op. cit*., pp. 518 y ss.

[53] Así, *vid*. Matellanes Rodríguez, N., «El intrusismo informático como delito autónomo: razones», en *Revista General de Derecho Penal*, n.º 2, 1994, p. 4.

[54] Así, *vid*. Matellanes, N., «Algunas notas sobre las formas de delincuencia…», *op. cit.,* p. 141.

[55] Así, *vid*. Matellanes Rodríguez, N. «El intrusismo informático como …», *op. cit.,* p. 4.

[56] Escalona Vázquez, E., «El hacking no es (ni puede ser) delito», en *Revista Chilena de Derecho Informático,* n.º 4, 2004, p.157.

[57] Al respecto, *vid*., exhaustivamente, Dias, P., «O hacking enquanto crime de acesso ilegítimo. Das suas especialidades à utilizaçào das mesmas para a fundamentaçào de um novo direito», en *Actualidad Jurídica Uría & Menéndez*, n.º 14, 2006, p. 59.

Según la normativa internacional y europea reguladora del acceso, el interés cuya tutela parece interesarse no es ninguno de los mencionados, sino la seguridad de los sistemas informáticos o del propio sistema informático. Se trata de proteger la indemnidad de los sistemas y de preservarlos frente a posibles injerencias no autorizadas de terceros, con independencia de la naturaleza y contenido de los datos comprendidos en los mismos. Dicha protección, a su vez, perseguiría evitar la puesta en peligro de otros bienes jurídicos[58], configurándose el delito de acceso ilícito como un delito barrera u obstáculo[59].

La seguridad de los sistemas informáticos se configuraría, pues, como un bien jurídico supraindividual[60], en cuya virtud se persigue conjurar un peligro grave y cercano para múltiples bienes individuales y, así, impedir la producción de lesiones de estos últimos[61]. Ciertamente, los ataques o incidentes sobre los datos y los propios sistemas pueden incidir no sólo ya en tradicionales bienes jurídicos individuales (intimidad, patrimonio, secretos de empresa) sino también en otros de distinto tenor, como podrían ser la seguridad del tráfico jurídico en Internet, la confianza en las comunicaciones electrónicas (valor quizá comparable a la fe pública o la seguridad fiduciaria), el desarrollo del comercio electrónico, etc.

No se cuestiona, pues, la emergencia de ese bien jurídico, pero sí se albergan dudas sobre si existe necesidad de incriminar autónomamente el acceso no autorizado, para contribuir a su tutela.

Debe recordarse que el motivo básico que justifica la creación de estos nuevos bienes, de carácter supraindividual, es la vulnerabilidad de determinados valores frente a especiales modalidades de ataque contra ellos. Es decir, se constata que, ante determinados bienes, si el Derecho Penal sólo interviniese cuando ya se han lesionado, se producirían daños

---

[58] Se sanciona penalmente una actuación considerada peligrosa (el acceso) para impedir la realización de otras conductas más graves. Qué duda cabe que en la decisión de incriminar esta conducta ha influido el temor de que con los accesos ilícitos se ocasiones daños más graves. Así lo demuestra la previsión de esa posibilidad, como circunstancia agravante, en gran parte los ordenamientos examinados (así, Francia, Italia y Portugal).

[59] Así, *vid*. Morón Lerma, E., *Internet y derecho penal: hacking…, op. cit.,* p. 75 y Puente Alba, L.M., «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», en *Nuevos retos del Derecho Penal en la era de la globalización* (Faraldo Cabana, Dir.), Valencia, 2004, p. 400.

[60] Así, *vid*. Martínez-Buján Pérez, C., *Derecho Penal Económico, Parte General*, Valencia, 1998, p. 105, que admite la configuración de bienes jurídicos supraindividuales a condición de que se mantenga una referencia al individuo.

[61] Así, Rodríguez Mourullo/alonso Gallo/Lascuráin Sánchez, «Derecho penal e Internet», en *Régimen jurídico, op. cit*., p. 261, ha señalado que se trataría de un bien jurídico con carácter instrumental respecto a otros intereses jurídicamente relevantes.

muy graves, situación que justifica adelantar las barreras de protección castigando determinadas conductas peligrosas, previas a la causación de tales daños[62].

En el supuesto objeto de análisis —injerencias en los sistemas consistentes en accesos—, los mencionados presupuestos de legitimación —del bien jurídico— no se verifican respecto de los posibles bienes jurídicos individuales afectados (patrimonio individual, intimidad, etc.)[63]. Únicamente, cabría imaginar esa situación excepcional respecto de conductas de daños producidos a datos y sistemas y, en concreto, respecto de los dirigidos contra infraestructuras especialmente sensibles[64].

Lo anteriormente expuesto conduce a cuestionar la tipificación de esta conducta, lo que no significa que no merezca reproche a través de otros cauces como el civil o el administrativo.

En cualquier caso, si finalmente se opta por introducir este delito, convendría que se ubicase sistemáticamente en un título distinto del que protege la intimidad. Ello permitiría desterrar confusiones y solapamientos normativos con las numerosas modalidades comisivas previstas en ese ámbito. En realidad, de abordarse una reforma en profundidad, lo más ordenado sería crear un título autónomo destinado a castigar los atentados a los sistemas informáticos, en el que se ubicara éste y otros incidentes relativos a los mismos, como los daños a los datos y a los sistemas, de forma parecida a la regulación del derecho francés. Sin embargo, no conviene ignorar que esa opción conllevaría una clara ampliación de la intervención penal.

Asimismo, sería recomendable que el objeto material se redujese a los accesos a sistemas informáticos sin mención expresa de los datos, asumiendo el concepto de sistemas propuesto por la DM, que comprende los datos y programas indispensables para que los sistemas funcionen correctamente.

Además, el ámbito típico de este delito no debería trazarse con elementos subjetivos referentes a intenciones, sino con elementos de carácter objetivo, como, por ejemplo, la exigencia de que el acceso haya supuesto la vulneración de medidas de seguridad de eficacia certera.

Por último, el principio de intervención mínima y fragmentariedad aconseja circunscribir la punibilidad del acceso a casos de especial gra-

---

[62] Martínez-Buján Pérez, C., *Derecho Penal Económico, Parte General, op. cit.,* pp 104 y ss.

[63] *Vid*., más exhaustivamente, Puente Alba, L.M., «Propuestas internacionales de criminalizar el acceso ilegal…», *op. cit.,* pp. 402 y ss.

[64] Me estoy refiriendo, por ejemplo, a los daños previstos en el delito de desórdenes públicos.

vedad[65], como podrían ser aquellos en que el acceso se lleve a cabo sobre sistemas de especial relevancia o sensibilidad, que formen parte de las infraestructuras vitales de un Estado. En este sentido, la DM declara expresamente, en la parte expositiva, que el objetivo es armonizar y aproximar la legislación penal en materia de ataques contra sistemas, tomando en especial consideración la posibilidad de ataques terroristas o de grupos organizados contra sistemas que forman parte de las infraestructuras vitales de los Estados miembros, lo que puede comprometer seriamente la realización de una sociedad de la información segura.

Concluido el examen del acceso no autorizado, corresponde, a continuación, abordar las conductas de «atentados contra la integridad de los datos» o «intromisión ilegal en los datos» y «atentados contra la integridad del sistema» o de «intromisión ilegal en los sistemas de información», reconducidas, en nuestro derecho, a los delitos de daños informáticos.

III. **Conductas de intromisión ilegal en los datos y en los sistemas de información**

1. *Precisiones conceptuales*

La expresión «sabotaje» o «daños informáticos» alude a dos tipos de incidentes, a saber, aquellos que se ejecutan sobre los datos o programas de un sistema informático y los que se dirigen contra el propio sistema.

Esto es, de una parte, conductas de destrucción o modificación de datos o programas, por ejemplo, mediante la introducción en el sistema de algún tipo de virus[66]; y, de otra, comportamientos dirigidos a ocasionar perturbaciones sobre los sistemas de información, por ejemplo, me-

---

[65] Así. *vid*. la DM que exige que no se castiguen infracciones de menor gravedad.

[66] La implementación de virus resulta cada vez mayor y más sofisticada. Así, entre éstos, pueden distinguirse los siguientes:

—bombas lógicas (*time bombs*): progamas autoejecutables que se activan cuando el usuario realiza una determinada acción o se cumplen unos parámetros (por ejemplo, de tiempo);

—gusanos (*worms*): programas que consumen la memoria del ordenador y que se propagan por sistemas de comunicaciones, como el *email*; algunos se ejecutan sin necesidad de interacción (*Zoher, Welyah, Bubbelboy, BadTrans.B, Klez*);

—caballos de troya (*trojan horse*): programas que se ocultan en otros (generalmente, ficheros anexos) y si se ejecutan, producen efectos dañinos; actualmente, programas de control remoto (*back orifice, netbus, deep throath*);

diante ataques masivos de denegación de servicio (DoS)[67]. Estos ataques persiguen sobrecargar o saturar, por medio de artificios informáticos (por ejemplo, creando redes de sistemas esclavos), algunos de los recursos limitados del sistema objeto del ataque hasta hacerlo inoperativo, logrando con ello el bloqueo o interrupción temporal de dicho sistema[68].

Estas conductas han sido objeto de regulación por parte de normativa internacional y comunitaria, en cuya aparición han confluido varios factores. De una parte, la constatación del aumento en la creación, divulgación e infección de sistemas a causa de virus informáticos y de los cuantiosos daños económicos provocados por estos[69]; asimismo, la del incremento de los ataques contra encaminadores y de denegación de servicio; por último, la alarma social suscitada ante los peligros que encierra la utilización de las nuevas tecnologías y, en concreto, de la red, por delincuentes informáticos y, sobre todo, a tenor de lo acontecido el 11-S, por organizaciones terroristas; esto es, la inquietud creciente —enfatizada por una opinión pública alarmada— ante la amenaza de lo que se ha venido a denominar «ciberterrorismo»[70].

—bacterias (*rabitts*): programas que se replican hasta detener por completo las máquinas;

—virus puros: fragmentos de códigos que se unen a un programa (virus de archivos, virus de sector de arranque, macrovirus, virus multiplataforma que provocan una vulnerabilidad muy alta y virus de enlace o de directorio), activándose y replicándose al ejecutarse el programa.

Vid., más exhaustivamente, MORÓN LERMA, E*., Internet y derecho penal: hacking…, op. cit.,* pp. 42 y 43 y CORCOY BIDASOLO, M., «Protección penal del sabotaje informático. Especial consideración de los delitos de daños», en MIR PUIG, S. (Comp.), *Delincuencia informática*, Barcelona, 1992, pp. 150 y ss.

[67] *Vid*. exhaustivamente, MORÓN LERMA, E. *Internet y derecho penal: hacking…, op.cit.,* pp. 43 y ss. y RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, «Derecho penal e Internet», en *Régimen jurídico, op. cit*., pp. 278 y ss.

[68] En los casos en los que se utilizan «máquinas esclavas» para llevar a cabo el ataque, éstas también son objeto del ataque y pueden verse afectadas.

[69] Los virus informáticos han causado importantes daños económicos. Así, por ejemplo, en 2001, *Nimda* provocó pérdidas de 630 millones de dólares, *Code Red*, de 2620 millones, *SirCam*, de 1150; en 2000 *I love You*, de 8750 millones y, en 1999, *Melissa* causó pérdidas de 1100 millones y *Explorer* de 1020 millones de dólares (vid. Ciberp@ís, jueves 9 mayo 2002, p.9 y jueves 23 mayo 2002, p.5).

[70] Junto a la normativa objeto de comentario *vid*., asimismo, Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y social y al Comité de las Regiones «Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos», Bruselas, 26.1.2001, COM(2000)890 final y Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y social y al Comité de las Regiones «Seguridad de las redes y de la información: Propuesta para un enfoque político europeo», Bruselas, 6.6.2001, COM(2001)298 final.

2. *Marco internacional y europeo*

A) Convenio de Cibercriminalidad

El Convenio sobre Cibercriminalidad prevé los «atentados contra la integridad de los datos», en su artículo 4, y los «atentados contra la integridad del sistema», en su artículo 5.

Concretamente, el artículo 4 establece que:

> «1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.
>
> 2. Los Estados podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves».

El artículo 5, regulador de los atentados contra la integridad del sistema, prevé que:

> «Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos».

B) Decisión Marco 2005/222, de 24 de febrero, relativa a los ataques a los sistemas de información

La Decisión Marco contempla una regulación similar a la recogida en el Convenio, variando la terminología empleada.

El artículo 4, relativo a la intromisión ilegal en los datos, establece que:

> «Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad».

Y el artículo 3, referente a la intromisión ilegal en los sistemas de información, prescribe que:

> «Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad».

Por lo que atañe a nuestro derecho, el encaje de las conductas descritas se reconduce al delito de daños informáticos (art. 264.2 CP), cuya previsión, sin embargo, no se halla exenta de consideraciones críticas e interpretaciones diversas, a las que se aludirá más tarde[71].

La amplitud con la que ha sido redactado este precepto (art. 264.2 CP) permite subsumir en él las modalidades descritas en el art. 4 DM, relativo a las intromisiones en los datos[72].

De hecho, aunque los asaltos contra los sistemas no se hallan tipificados como delito autónomo, tienen encaje en el antecitado delito, en la medida en que el entorpecimiento o alteración del funcionamiento del sistema se produzca a través de alguna de las modalidades comisivas recogidas en el art. 264.2 (destrucción, alteración, inutilización o cualquier otro daño sobre los datos).

En suma, pues, aunque el CCiber y la DM incorporan un elenco de conductas más amplio (introducción, transmisión, daño, borrado, deterioro, alteración, supresión e inutilización de datos), la mayor parte de ellas coinciden con las previstas en el Código español, a salvo de las matizaciones que, posteriormente, se formularán.

---

[71] Acerca del delito de daños o sabotaje informático, *vid*. González Rus, J.J.,»Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos», en *Revista Electrónica de Derecho Penal y Criminología*, 1-14, 1999 (http://www.recpc.com); del mismo autor, «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (Artículo 264.2 del Código Penal)», en *La ciencia del Derecho Penal ante el nuevo siglo. Libro homenaje al Profesor Doctor Don José Cerezo Mir,* Madrid, 2002, pp. 1281 y ss.; del mismo autor, «El cracking y otros supuestos de sabotaje informático», en *Estudios Jurídicos del Ministerio Fiscal*, II-2003, pp. 209 y ss.; del mismo autor, «Los ilícitos en la Red (I): hackers, crackers…», *op. cit.,* pp. 241 y ss.; Romeo Casabona, C.M., «Los delitos de daños en el ámbito informático», en *Cuadernos de Política Criminal,* n.º 43, 1991, pp. 91 y ss.; Corcoy Bidasolo, M., «Protección penal del sabotaje informático…», *op. cit.,*; Marchena Gómez, M. «El sabotaje informático: entre los delitos de daños y desórdenes públicos», en *Internet y derecho penal*…, *op. cit.,* pp. 355 y ss. Para un análisis crítico del art. 264.2 CP, *vid*. Andrés Domínguez, A.C., «Los daños informáticos en la Unión Europea», en *LL,* n.º 4725, 2 de febrero de 1999, pp. 3-4 y Morón Lerma, E., *El secreto de empresa: protección penal…, op. cit.,* pp. 341-346.

[72] Así, *vid*. Galán Muñoz, A. «Ataques contra sistemas informáticos», en *Boletín de Información, op. cit.,* p.232.

Examinadas las directrices internacionales y comunitarias en la materia, a continuación, se abordará una breve perspectiva de derecho comparado.

3. *Derecho comparado*

A) Francia

El Código Penal francés contempla, en el capítulo rubricado «De los atentados contra los sistemas de tratamiento automatizado de datos», las conductas objeto de análisis.

De una parte, en el art. 323-2 CP, se castiga a quien perturbe o deteriore un sistema de tratamiento automatizado de datos con la pena privativa de libertad de 5 años y multa de 75.000 euros[73].

Este precepto permite, pues, sancionar las conductas de interferencia o daños sobre los sistemas, a condición de que se produzca alguna perturbación efectiva. Así, por ejemplo, tendrán cabida aquellas perturbaciones que acarrean una ralentización de la capacidad de los servidores (París, 5 abril 1994), pero no el envío masivo y simultáneo de mensajes no solicitados, que no llegan a alterar de forma sensible el funcionamiento de los medios informáticos (París, 18 diciembre 2001).

Además, el art. 323-3 CP, prevé la introducción fraudulenta de datos en un sistema automatizado o la supresión o modificación fraudulenta de los datos contenidos en él, con una pena de prisión de 5 años y multa de 75.000 euros[74].

En este delito tienen cabida los atentados contra los datos, esto es, la introducción, modificación o supresión de datos contenidos en el sistema, sin que se exija la concurrencia en el autor de un especial ánimo de dañar[75].

Por último, debe recordarse que el art. 323-1, regulador del acceso ilícito a un sistema, contempla como tipo agravado la comisión de atentados o daños contra los datos contenidos en ese sistema o contra el propio sistema. Esto es, se sanciona la conducta más gravemente cuando quien lleva a cabo el acceso ocasiona de forma sobrevenida e imprudente daños sobre los datos o el sistema.

---

[73] Este precepto fue modificado en 2004, por la Ley n.º 2004-575, de 21 de junio. Anteriormente a la reforma, la pena era de prisión de 3 años y pena de 45.000 euros.

[74] Al igual que el precepto anterior, el art. 323-3 fue modificado por la Ley n.º 2004-575, incrementando la pena de prisión 3 a 5 años y la de multa de 45.000 a 75.000 euros.

[75] Así, *vid*. *Code pénal, Annotations de jurisprudence par* Mayaud, Y., 104 ed. Dalloz, 2007, p. 775.

B) Italia

En el ordenamiento penal italiano, estas conductas se hallan previstas de manera dispersa en varios preceptos. En concreto, los atentados contra daños y sistemas encuentran sanción en el artículo 635 *bis* CP, relativo a los daños sobre los sistemas informáticos y telemáticos, en el art. 615 *quinquies* CP referente a la difusión de programas dirigidos a dañar o interrumpir un sistema informático y en el art. 615 *ter* CP, que prevé como tipo agravado del acceso ilícito la producción de daños a datos o sistemas, ocasionados al perpetrar el acceso.

1. El art. 635 *bis* CP italiano se halla previsto en el Capítulo I (Delitos contra el patrimonio mediante violencia sobre las cosas o las personas), del Titulo XIII, regulador de los delitos contra el patrimonio.

El precepto establece, en su inciso primero, que:

> «Quien destruya, deteriore o inutilice, en todo o en parte, sistemas informáticos o telemáticos ajenos, o bien, programas, información o datos ajenos, será castigado, salvo que el hecho constituya otro delito más grave, con pena privativa de libertad de seis meses a tres años».

Este delito castiga conjuntamente los incidentes contra los datos y contra los sistemas, puesto que la conducta —destrucción, deterioro o inutilización— se proyecta sobre un amplio objeto material, a saber, los sistemas informáticos o telemáticos y los programas, información o datos ajenos.

2. El art. 615 *quinquis* CP italiano, que contiene el delito de difusión de programas dirigidos a dañar o interrumpir un sistema informático, goza de una ubicación sistemática diversa a la anterior. Se halla previsto en el ámbito de los delitos contra la libertad personal y, en concreto, en la Sección IV, relativa a los delitos contra la inviolabilidad del domicilio.

En él se prevé que:

> «Quien difunde, comunica o pone a disposición un programa informático creado por él o por otros, teniendo por finalidad o por efecto el daño de un sistema informático o telemático, de datos o de programas contenidos o pertenecientes al mismo, o bien la interrupción, total o parcial, o la alteración de su funcionamiento, será castigado con pena privativa de libertad de hasta dos años y con multa de hasta veinte millones de liras».

Este ilícito castiga la conducta técnica previa —o antesala— del delito previsto en el art. 635 *bis*. Se presume el carácter peligroso de estos comportamientos para los datos y sistemas y se elevan a la categoría de

delito autónomo conductas que constituyen, en realidad, tentativas del injusto previsto en el art. 635 *bis* CP Italiano. Se configura, pues, como un delito de peligro, cuya relevancia típica se ve colmada por la concurrencia del ánimo de causar daños sin que sea necesario que éstos se produzcan[76].

Las conductas tipificadas consisten en la difusión (a través de Internet, por ejemplo), la comunicación a alguien (a través de e-mail, por ejemplo) o la puesta a disposición o entrega (a través de soporte analógico, por ejemplo, un CD) de dichos programas[77]

3. Por último, hay que recordar que el art. 615 *ter* CP italiano, regulador del acceso no autorizado a un sistema, tipifica como tipo agravado la producción de daños sobre los sistemas o los datos, derivados de la propia conducta de acceso.

Así, el art. 615 *ter* CP señala que:

> «Será castigado con pena de cárcel de 1 a 5 años:
> (…)
> 3) si del hecho se deriva la destrucción o el daño del sistema o la interrupción total o parcial de su funcionamiento, o bien la destrucción o el daño de los datos, de la información o de los programas contenidos en él (…)».

El examen de estos preceptos permite constatar la opción político-criminal del legislador italiano de una amplia intervención penal en la materia. De otra parte, sorprende la distinta ubicación otorgada a las conductas de intromisión ilegal en datos y sistemas, en sede de delitos contra el patrimonio, y a las conductas de difusión de programas y de atentados contra datos y sistemas de carácter imprudente, en el ámbito de los delitos contra la inviolabilidad domiciliaria.

C) Alemania

El ordenamiento penal alemán castiga en el parágrafo *§* 303a del *StGB* la alteración de datos y en el *§* 303b, el sabotaje informático. Ambos preceptos se hallan ubicados en la Sección vigesimoséptima, rubricada como «Daños materiales».

---

[76] En esta línea de anticipación del Derecho Penal, recientemente, se ha detenido en China, por primera vez, a los creadores de un virus, que llenaba de osos panda las pantallas de los ordenadores (14.02.2007, Agencia Efe). En este caso, se adelanta la intervención penal a la creación del *software*.

[77] Así, *vid*. Farolfi, F., «I crimini informatici», en http://ei.unibo.it/materie/pdf/reati_informatici.pdf, p. 4.

El § 303a relativo a la alteración de datos establece que:

> «(1) El que, ilícitamente, borre, oculte, inutilice, o altere datos (§ 202 a, inciso 2), será castigado con pena privativa de la libertad de hasta dos años o multa».

Según la doctrina especializada, lo protegido aquí es la utilización de los datos en perfecto estado[78].

El § 303b, regulador del sabotaje de computadoras señala que:

> «(1) El que perturbare un procesamiento de datos que sea de importancia esencial para una empresa o establecimiento industrial ajeno o para la Administración,
>
> 1. cometiendo un hecho de los referidos en el § 303 a, inciso 1, o
>
> 2. destruyendo, dañando, inutilizando, eliminando o alterando un equipo de procesamiento de datos o un soporte será castigado con pena privativa de la libertad de hasta cinco años o con multa».

En este caso, se sancionan las conductas de intromisión en sistemas aunque limitando el objeto material a los procesos de datos que resulten de vital importancia para una empresa o establecimiento industrial o para la Administración. Por tanto, se considera que lo protegido en este precepto es el interés de empresarios y autoridades en un funcionamiento libre de perturbaciones de sus sistemas informáticos[79].

D) Portugal

En Portugal, la Ley n.º 109/91, de 17 de agosto de 1991, sobre Criminalidad Informática, introdujo los delitos de daños a datos o programas informáticos (art. 5) y el delito de sabotaje informático (art. 6).

El artículo 5 establece:

> «1. El que, sin autorización, y actuando con intención de causar perjuicio a otro o de obtener un beneficio ilegítimo para sí o para terceros, borre, destruya, en todo o en parte, dañe, suprima o inutilice datos o programas informáticos ajenos o, de cualquier forma, incida sobre su capacidad de uso será castigado con pena privativa de libertad de hasta tres años o con pena de multa.
>
> 2. La tentativa es punible.

---

[78] Así, *vid*. Möhrenschlager, M.E., «El nuevo derecho penal informático…», *op. cit.,* p. 140.

[79] Así, Möhrenschlager, M.E., «El nuevo derecho penal informático…», *op. cit*., p. 142.

> 3. Si el daño causado fuese de valor elevado, la pena será de prisión de hasta cinco años o multa de hasta 600 días.
> 4. Si el daño causado fuese de valor considerablemente elevado, la pena será de prisión de uno a diez años (…)».

El artículo 6, regulador del sabotaje informático, prevé:

> «1. El que introduzca, altere, borre o suprima datos o programas informáticos o, de cualquier forma, interfiera en un sistema informático, actuando con intención de dificultar o perturbar el funcionamiento de un sistema informático o de una comunicación de datos a distancia, será castigado con pena de prisión de hasta cinco años o con pena de multa de hasta 600 días.
> 2. La pena será de prisión de hasta cinco años si el daño emergente de perturbación fuese de valor elevado.
> 3. La pena será de prisión de uno a diez años si el daño emergente de perturbación fuese de valor considerablemente elevado».

La regulación de estos preceptos suscita algunas reflexiones. La modalidad básica introduce un elemento de tendencia subjetiva cifrado en obtener, para sí o para tercero, un beneficio o ventaja ilícita. Se trata de un elemento extraño a la dinámica comisiva de estos delitos, que no encuentra parangón en la normativa internacional ni tampoco en los ordenamientos examinados.

Además, tanto el delito de daños a datos o programas como el delito de sabotaje informático introducen circunstancias agravantes que pueden mermar la seguridad jurídica. No resultará fácil hallar herramientas interpretativas que permitan un deslinde nítido entre la producción de un «daño elevado» y un «daño considerablemente elevado» (art. 5.3 y 5.4 y art. 6.2 y 6.3). Esta cuestión cobra especial relevancia dada la gravedad de las penas imponibles en esos casos, que pueden llegar hasta diez años de prisión.

E) Conclusiones

Los ordenamientos examinados permiten constatar una incriminación generalizada de las conductas de intromisión ilegal en los datos y de intromisión ilegal en los sistemas

En concreto, se ha comprobado que la mayor parte de países lleva a cabo una regulación de ambas conductas por separado. La ubicación sistemática de estos ilícitos no es homogénea, pero, generalmente, son concebidos como delitos de daños, reconducibles a la protección del patrimonio, excepto en el caso del derecho francés, que los ubica en

un título autónomo y en uno de los supuestos del derecho italiano, que entiende el delito de difusión de programas, como un atentado contra la inviolabilidad domiciliaria.

En cuanto a los requisitos que configuran el ámbito típico de estas infracciones, no se requieren especiales elementos subjetivos, a excepción del ánimo de dañar (en derecho italiano y portugués) ni tampoco perjuicios económicos evaluados cuantitativamente, a excepción del derecho portugués que contempla como circunstancia agravante la producción de daños de valor elevado o considerablemente elevado.

Por último, destaca la regulación del derecho alemán que restringe la protección de los sistemas informáticos a aquellos que resulten de vital importancia para la empresa y para la Administración.

A continuación, corresponde examinar qué encaje tienen las conductas de daños a datos y sistemas informáticos en Derecho Penal español.

4. *Derecho español vigente*

El precepto que sanciona los daños informáticos es el art. 264.2 CP, en cuya virtud se imponen penas de uno a tres años de prisión y multa de doce a veinticuatro meses a quien, por cualquier medio, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El delito se ubica en el título destinado a proteger el patrimonio (Título XIII) y, en concreto, en el capítulo regulador de los daños, respecto de cuya figura básica —que sanciona los daños en propiedad ajena, siempre que éstos sean superiores a 400 euros (art. 263 CP)—, toma la penalidad.

Así pues, las peculiaridades de este ilícito (ubicación sistemática en sede de delitos contra el patrimonio, concreción de la propiedad como bien jurídico protegido, regulación de la conducta en un precepto cuya penalidad se asigna por remisión a la del delito de daños materiales y exigencia de producción de un daño económico superior a 400 euros) han dado lugar a divergencias doctrinales respecto de la naturaleza, el ámbito de aplicación y el objeto material del mismo.

En síntesis, se han sugerido tres interpretaciones posibles al respecto. De una parte, la consideración del art. 264.2 CP como un subtipo agravado del delito de daños en elementos lógicos[80]; de otra, la concepción de

[80] Así, *vid*. Mata y Martín, M., *Delincuencia informática y derecho penal*, Madrid, 2001, p. 60 y 77-79; Matellanes, N., «Algunas notas sobre las formas de delincuencia…», *op. cit.,* p. 142; Marchena Gómez, M. «El sabotaje informático: entre…», *op. cit.,* p. 358;

este ilícito como una modalidad autónoma, cuya ubicación entre los daños resulta errónea[81]; y, por último, su entendimiento como un delito de daños referido a elementos informáticos de naturaleza lógica y física[82].

La mayor parte de estas interpretaciones han sido objeto de crítica, por abocar a soluciones insatisfactorias[83].

La primera de las propuestas enunciadas, que entiende el art. 264.2 CP como un subtipo agravado y, por tanto, como un delito de daños en elementos lógicos exclusivamente, ha sido censurada por varios motivos. De un lado, supone ciertos dislates valorativos, al considerar más grave la conducta de destrucción de elementos lógicos (datos, por ejemplo) que la de elementos físicos (unidad de proceso, por ejemplo). Asimismo, en los casos en que se viesen afectados ambos componentes (lógicos y físicos) debería dar lugar a la aplicación de un concurso de delitos entre los artículo 263 y 264.2 CP, lo que provocaría, en ocasiones, consecuencias poco deseables desde el punto de vista de la pena resultante a hechos de la misma significación lesiva.

Asimismo, el entendimiento del delito de daños como un tipo autónomo ha motivado similares reflexiones críticas. Se pone de manifiesto que obliga a prescindir de la cuantía del objeto dañado como elemento del delito, con lo que se desbordarían los límites de una intervención penal razonable en este ámbito. Además, conduciría a la apreciación de un concurso de delitos entre el art. 263 y 264.2 CP, cuando con la misma conducta se afectaran elementos lógicos y físicos.

Por último, la consideración del delito de daños referido a elementos informáticos de naturaleza lógica y física, como un tipo especial

---

Orts Berenguer/Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia 2001, pp. 80 y 81; García Arán, M., en AA VV, *Comentarios al Código Penal, Parte Especial*, (Córdoba Roda/García Arán, Dir.), Tomo I, Madrid, 2004, pp. 930-931; Mestre Delgado, en *Derecho Penal, Parte Especial* (Lamarca Pérez, Coord.), 3.ª ed., Madrid, 2005, p. 309; Calderón Cerezo/Choclán Motalvo, *Código Penal comentado,* Barcelona: Deusto, 2005, p. 270, entre otros.

[81] Andrés Domínguez, A.C., «Los daños informáticos en la Unión Europea», en *LL,* n.º 4725, 2 de febrero de 1999; Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, «Derecho penal e Internet», en *op. cit.,* p. 282; Morón Lerma, E.*, Internet y derecho penal: hacking…, op. cit.*, p. 68; Madrigal Martínez-Pereda, C., AA VV, *Código penal (Comentarios y jurisprudencia)* (Del Moral García/Serrano Butragueño, Coord.), Tomo II, Granada, 2002, p.1819.

[82] Así, *vid*. González Rus, J.J., «El cracking y otros supuestos de sabotaje informático», en *Estudios Jurídicos del Ministerio Fiscal*, II-2003, p. 223; del mismo autor, «Los ilícitos en la Red (I): hackers, crackers…», *op. cit.,* p.253.

[83] Para una aproximación crítica a dichas interpretaciones, *vid*. exhaustivamente González Rus, J.J., «El cracking y otros supuestos…», *op. cit.,* pp. 217 y ss. y del mismo autor «Los ilícitos en la Red (I): hackers, crackers…», *op. cit.,* pp. 252 y ss.

respecto del art. 263 CP presenta, también, algunas limitaciones. La restricción del objeto material a los datos, programas o documentos electrónicos y la exigencia de un perjuicio con valor económico superior a 400 euros, dificultan la aplicación del delito a los ataques a los sistemas que provocan una denegación de servicio (DoS) o que, sin llegar a inutilizarlo totalmente, distorsionan de forma significativa su funcionamiento.

Es decir, en los casos en que esa perturbación no se lleve a cabo mediante la destrucción o la alteración de los datos o programas, se advierte que no será posible encajar la conducta en este precepto.

Además, se subraya la dificultad de satisfacer el requisito del daño económico superior a 400 euros, debido a los obstáculos para evaluar, más o menos mediatamente, el daño producido, así como al hecho de que las pérdidas patrimoniales no puedan integrar el concepto de daño en el sentido del art. 264.2 CP, dada la tradicional distinción entre el concepto penal de daño y el de perjuicio, de naturaleza más civil. Lo anterior, determina, por tanto, que, en ciertas ocasiones, se antoje difícil brindar protección a los sistemas a través del art. 264.2 CP.

En suma, los incidentes contra los datos tienen cabida, con carácter general, en el art. 264.2 CP. Sin embargo, el castigo de las intromisiones en los sistemas plantea, en algunos supuestos —determinadas modalidades de ataques de denegación de servicio y perturbaciones en su funcionamiento—, mayores problemas de encaje por la limitación del objeto material y la demostración del daño evaluable económicamente en cuantía superior a 400 euros.

Concluido el análisis de *lege lata*, corresponde, en este momento, abordar el texto del Proyecto de reforma, puesto que, como se sabe, tanto el Convenio sobre Cibercriminalidad como la Decisión-Marco 222/2005 prevén, específicamente, estas conductas, otorgando protección autónoma a ambos tipos de intromisiones y, específicamente, a las que se dirigen contra los sistemas. A continuación, pues, se examinará la transposición que se ha hecho de dicha normativa.

5. *Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 19/1995, de 23 de noviembre, del Código Penal*

El apartado quincuagésimo quinto del Proyecto otorga un nuevo contenido al artículo 264 CP, incorporando diversos supuestos de daños a datos, programas y sistemas informáticos. Asimismo, se desplaza el redactado actual del artículo 264.1 a un nuevo apartado del artículo 263, donde se integra con el texto del vigente art. 263.1 CP.

El nuevo artículo 264 CP establece, en sus dos primeros incisos, lo siguiente[84]:

> «1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos o programas informáticos ajenos, será castigado, en consideración a la gravedad del hecho, con la pena de prisión de seis meses a dos años.
>
> 2. El que sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema de información ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, será castigado, atendiendo a la gravedad del hecho, con la pena de prisión de seis meses a tres años».

Así, el Proyecto ha regulado las intromisiones ilícitas en los datos y en los sistemas informáticos por separado, dotando de autonomía típica a cada una de ellas.

1. El art. 264.1 CP incrimina, en correlación con lo prescrito en el artículo 4 de la DM, los atentados contra los datos o programas informáticos. Las principales novedades introducidas en este delito se concretan en el objeto material y en la reducción del rigor punitivo[85].

Respecto del objeto material, se elimina la referencia a los documentos electrónicos, puesto que se hallan incluidos en el concepto de dato, de carácter omnicomprensivo.

Asimismo, se reduce el marco penal aplicable al delito base, pues varía de prisión de uno a tres años y multa de doce a veinticuatro meses a prisión de 6 meses a 2 años.

2. El art. 264.2 CP ha incorporado, desligadamente de los atentados contra los datos, las intromisiones en los sistemas de información,

---

[84] El art. 264 del Proyecto, establece, en sus incisos 3 y 4:

«3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.º Se hubiese cometido en el marco de una organización criminal.

2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

4. Cuando los delitos comprendidos en este artículo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en los apartados 1 y 2, y del tanto al décuplo en el supuesto del apartado 3».

[85] Para una valoración crítica al respecto, *vid*. Informe del CGPJ, pp. 135-136.

acatando lo dispuesto en el artículo 3 de la DM, que reproduce casi literalmente.

Estas conductas, que son castigadas con pena prisión de seis meses a tres años, sufren un reproche más severo que las anteriores[86]. La diversa penalidad otorgada a ambos tipos de comportamiento está presente en la Decisión Marco, que fija un mínimo para las intromisiones a los sistemas (prisión de uno a tres años como mínimo en su grado máximo) y, sin embargo, omite cualquier referencia al tipo de pena que debe adoptarse para los daños a los datos y programas, a salvo del genérico mandato de que las sanciones sean efectivas, proporcionadas y disuasorias.

Esa diferente valoración penológica se halla, también, en otros ordenamientos europeos. Así, por ejemplo, en Alemania y Portugal, los incidentes sobre los datos son castigados con menor pena (prisión de hasta 2 años, en Alemania) (prisión de hasta 3 años, en Portugal) que las intromisiones en los sistemas (prisión de hasta 5 años, en Alemania y Portugal). Por el contrario Francia e Italia sancionan con igual rigor ambas conductas.

Dicha distinción traduce la potencialidad lesiva asociada a los ataques contra los medios de comunicación telemáticos y el riesgo que generan para otros bienes jurídicos (piénsese, por ejemplo, en asaltos contra programas de gestión de correo electrónico, ataques de denegación de servicio sobre grandes prestadores —Amazon, CERT - Centro de Seguridad de Internet, etc—.)[87]. En último término, quizá subyazca el temor a un ataque contra los sistemas informáticos de infraestructuras de vital importancia, fruto de actividades de grupos organizados o terroristas.

Junto a la reducción del rigor punitivo de la conducta de daños a los datos, destaca, en el Proyecto, la omisión al requisito de la producción de un daño económicamente evaluable. Se soslayan, así, algunas de las controversias originadas respecto a la exigencia e interpretación de dicho elemento.

Según se ha expuesto, la configuración del vigente art. 264.2 CP (ubicación sistemática, bien jurídico protegido, penalidad de la con-

---

[86] En el Proyecto, la escala punitiva de los arts. 263 y 264 sería la siguiente: los daños materiales genéricos del art. 263.1 CP se castigarán con una pena de multa de 6 a 24 meses; los daños ocasionados a datos y programas previstos en el art. 264.1 CP, con pena de prisión de 6 meses a 2 años y las intromisiones a los sistemas informáticos, con pena de prisión de 6 meses a 3 años. Además, ambos preceptos (arts. 263 y 264 CP) contienen modalidades agravadas.

[87] *Vid*., exhaustivamente, Marchena Gómez, M. «El sabotaje informático: entre…», *op. cit.,* pp. 356 y ss.

ducta por remisión a la del delito de daños y exigencia de daño económico superior a 400 euros) ha favorecido soluciones discutibles, como ocurre respecto del encaje de algunos incidentes contra los sistemas informáticos[88].

El problema relativo a si debe exigirse, en estos delitos, algún tipo de lesión patrimonial evaluable económicamente es de difícil resolución y revela la compleja naturaleza de estos ilícitos, todavía, en cierta forma, por definir.

Qué duda cabe que tanto las intromisiones en los datos como en los sistemas revisten una particular capacidad plurilesiva, idónea para poner en peligro una multitud de intereses. Y tampoco hay duda de que, aun así, es necesario exigir para su tipificación en el Código Penal un plus de ofensividad que permita castigar sólo aquellas conductas de especial gravedad a fin de no comprometer principios básicos de nuestro sistema penal (principio de intervención mínima y de ultima ratio) y acatar los dictados de la Decisión Marco que insta a no castigar las conductas de menor gravedad. Sin embargo, ni es fácil acotar cuál es la naturaleza del interés que, de forma más directa o mediata, se ve afectado por estas conductas ni tampoco resulta sencillo definir qué elementos permiten garantizar ese plus de gravedad.

Probablemente, los intereses que se ven afectados, de forma más generalizada, revistan naturaleza económica o patrimonial. Sin embargo, arbitrar la tutela de los mismos exigiendo una concreta y cuantificada lesión patrimonial deja cierta insatisfacción. Aunque no resulte fácil identificar esos parámetros, uno de ellos podría ser el propuesto por el ordenamiento alemán, que, requiere para sancionar las conductas de sabotaje informático, que se cometan en sistemas «de importancia esencial para una empresa o establecimiento industrial ajeno o para la Administración».

En todo caso, la indicación de criterios que permitan concretar la gravedad de la conducta se revela un trámite indispensable, puesto que, conforme a la redacción típica del nuevo art. 264.1 y 264.2 CP, sólo adquirirán significación penal aquellos supuestos considerados como graves.

El Proyecto mantiene la ubicación sistemática del precepto, cuyo traslado hubiese generado serios problemas (identificación del título de acogida) y, quizá, hubiese obligado a acometer una profunda —y controvertida— reforma que discurriese por la creación de un nuevo título, destinado a castigar los ataques a datos y sistemas, aglutina-

[88] *Vid*. *supra*, apartado 3.4., donde se ha dado cuenta de dicha situación.

dor de estos y otros comportamiento vinculados a los abusos informáticos.

Por último, la regulación del proyecto deja subsistentes algunos de los problemas ya mencionados, como el relativo a las hipótesis concursales que podrán suscitarse entre estos preceptos (arts. 263 y 264 CP).

Concluido el examen de derecho positivo y de *lege lata* de estas conductas, procede ya formular algunas conclusiones finales.

6. *Conclusiones respecto de la regulación de las conductas de intromisión ilegal en los datos e intromisión en los sistemas de información*

La importancia de los elevadísimos perjuicios que las conductas de intromisión ilícita en los datos y en los sistemas de información pueden ocasionar ha motivado una respuesta legislativa unánime. La normativa internacional, europea y regional analizada incorpora, como infracción penal, los atentados contra los datos, programas y sistemas informáticos.

La ubicación sistemática de estos preceptos suele hallarse en el ámbito de los delitos patrimoniales o de los daños materiales, a excepción del derecho francés, que dispone de un título autónomo destinado a los atentados contra los sistemas informáticos en donde encuentran pacífica cabida. Sin duda, esa ubicación revela la concepción del legislador a la hora de afrontar estas conductas, alzaprimando el patrimonio como bien jurídico protegido.

Se ha manifestado ya la dificultad que entraña la incardinación sistemática de estos ilícitos y se ha subrayado, también, su capacidad pluriofensiva. En este sentido, las dos opciones adoptadas por los ordenamientos de nuestro entorno más inmediato se erigen en las únicas posibles. O bien se acepta que estas conductas adquieren, en general, una significación fundamentalmente económica —lo que no significará reducir dicha vertiente al ámbito individual de la propiedad y de la exigencia de lesión cuantificada económicamente— y se les procura una ubicación coherente con esa naturaleza económica o patrimonial. O bien se reconoce el nacimiento de un nuevo bien jurídico, cifrado en la seguridad de los sistemas informáticos, que sería el inmediatamente afectado (con su puesta en peligro o lesión, dependiendo de los casos) por estas conductas. En este caso, debería dotarse de una protección autónoma y expresa en el Código a este bien jurídico, mediante la creación de un nuevo título.

Desde luego, esta última propuesta no se vería exenta de problemas añadidos a los actuales (hipótesis concursales con otros delitos —y no

sólo respecto del delito de daños—, relación sistemática y racional con las otras ramas del ordenamiento jurídico y, en especial, con la administrativa, entre otros), cuya complejidad, en estos momentos, sólo puede insinuarse.

Por lo que se refiere a su configuración típica, tal como recomiendan las directrices internacionales y europeas, convendría otorgar una regulación por separado de las conductas de intromisión en los datos y de las de intromisión en los sistemas.

Asimismo, deviene absolutamente necesario la identificación de criterios de tenor objetivo que permitan delimitar los ataques molestos pero penalmente insignificantes de aquellos otros que revistan relevancia penal por su mayor gravedad. Hasta el momento, se ha optado por exigir la producción de una lesión patrimonial cifrada en una cuantía superior a 400 euros.

Probablemente, razones de coherencia sistemática de *lege lata* han contribuido a la propuesta de esa solución, pero al haber sido concebida análogamente a la protección de objetos materiales, entorpece en algunas ocasiones la aplicación del precepto. De ahí que las particularidades e idiosincrasia de estos delitos y, en especial, de los incidentes contra los sistemas de información, desaconsejen perpetuar ese elemento.

No se desconoce la dificultad de dicha tarea y lo arduo de formular criterios o propuestas alternativas a la que se censura. Quizá, éstas deberían discurrir por circunscribir la significación penal a aquellos supuestos en que los incidentes se dirijan a sistemas de esencial relevancia o de especial vulnerabilidad. En este sentido, el Código Penal alemán ha restringido el delito de sabotaje informático a que se verifique sobre sistemas de importancia esencial para una empresa o establecimiento industrial ajeno o para la Administración. Y es que, en efecto, esos parecer ser los supuestos en que se concretan los ataques contra los sistemas de información. Esto es, dichos incidentes pueden perseguir causar daños a las empresas, haciendo caer sus servidores, por ejemplo o, quizá, desestabilizar las infraestructuras básicas de un Estado, temor que parece subyacer en la normativa internacional y comunitaria en la materia. La fórmula del Código Penal alemán permitiría reprimir el primer grupo de incidentes y ofrecería un criterio de deslinde de este delito con el de desórdenes públicos, marco en el que probablemente encajaría el segundo de los escenarios apuntado. Asimismo, se lograría establecer un umbral razonable de la intervención penal.

En suma, los delitos analizados plantean interrogantes que son afrontados con menor rapidez de aquella con la que se suscitan y que traen causa de desafíos jurídicos mayores.

IV. **La emergencia de un ámbito de criminalidad autónomo**

La necesidad de reacción penal frente a los múltiples y novedosos riesgos derivados de las nuevas tecnologías resulta, a estas alturas, incontrovertible. Mayores dudas suscita cómo arbitrar una respuesta que no orille ni debilite principios y garantías penales irrenunciables (principio de intervención mínima, *ultima ratio*, principio de proporcionalidad, etc.).

En el fondo, se trata de una disyuntiva planteada hace ya tiempo, en cuya virtud deberá elegirse de qué modo se reprimen los abusos informáticos[89]: mediante la creación de «tipos de equivalencia», es decir, incorporando tipos penales que complementen a los ya existentes, corrigiendo en la descripción de la acción típica las carencias detectadas en aquellos. O bien, a través de la descripción de nuevas conductas normalmente peligrosas para el correcto funcionamiento de los sistemas y sus componentes.

Ambas técnicas legislativas reúnen ventajas y adolecen de inconvenientes[90]. La primera de ellas permite la concreción del tipo y la vinculación a bienes jurídicos merecedores de protección penal bien perfilados, lo que redunda en una mayor seguridad jurídica. Por el contrario, presenta la desventaja de favorecer el casuismo y la aparición de lagunas, al dejar sin cobertura conductas que aparecen con gran rapidez en este ámbito y que resultan dignas de intervención penal.

El segundo sistema, en cambio, se adapta a las nuevas formas de criminalidad, pero puede perder de perspectiva los bienes jurídicos que se desean proteger y llegar a conferir una protección tal vez excesiva en este campo. Ello supone riesgos para la seguridad jurídica y el debilitamiento del principio de intervención mínima.

El análisis de derecho comparado llevado a cabo permite constatar que los países de nuestro entorno, incluido el derecho español, han optado mayoritariamente, por el primer sistema. Sin embargo, las directrices internacionales y europeas en la materia tienden a la segunda fórmula legislativa, que, como en el caso francés, debería conducir a la

---

[89] Así, *vid*. Romeo Casabona, C.M., «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», en *Poder Judicial*, n.º 31, 1993, pp. 180 y ss. y del mismo autor, «Los delitos de daños en el ámbito informático», en *Cuadernos de Política…, op. cit.,* pp. 113 y ss.

[90] Así lo pone de manifiesto Romeo Casabona, C.M., «Los delitos de daños…», en *op. cit.*, p. 114. Posteriormente, se han hecho eco Álvarez Vizcaya, M., «Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red», en *Internet y derecho pena*l, *op. cit.,* pp. 268 y ss. y, siguiendo a esta autora, Magro Servet, V., «La delincuencia informática…», en *La Ley, op. cit.,* p. 5.

creación de un título independiente, destinado a castigar los ataques contra los sistemas de información.

La elección a favor de una de estas opciones se desvela compleja puesto que también lo es determinar si nos hallamos ante un ámbito de criminalidad necesitado de autonomía, en cuya virtud se reconozca y respalde la tutela de ese nuevo bien jurídico[91].

En los últimos tiempos, se ha señalado la posibilidad de compatibilizar ambos sistemas. Se pretende afrontar respuestas específicas pero sin pérdida de garantías, lo que, en este caso, exige el escrupuloso respeto del principio de intervención mínima y de *ultima ratio*, así como el de las reglas de imputación penal.

Por ello, aunque el reconocimiento de ese nuevo valor resulta casi indiscutible, el temor de privilegiar la eficacia en detrimento de la legitimidad aconseja, por el momento, acudir para su tutela a otros mecanismos de protección menos severos que el orden penal. Asimismo, no conviene olvidar la extraordinaria relevancia que asumen, en este ámbito, las medidas de seguridad a efectos de prevención[92]. Estamos todavía en una fase de desarrollo tecnológico y de asimilación de una cultura no consolidada. Y, como ha subrayado ya la doctrina, los procesos de creación normativa discurren a un ritmo mucho menos acelerado que el de Internet[93].

Bibliografía

ÁLVAREZ VIZCAYA, M., «Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red», en *Internet y derecho penal*, CGPJ, CDJ, X, 2001.

ANDRÉS DOMÍNGUEZ, A.C., «Los daños informáticos en la Unión Europea», en *La Ley,* n.º 4725, 2 de febrero de 1999.

---

[91] En nuestra doctrina, se muestran favorables a la aparición de este nuevo bien jurídico, entre otros, QUINTERO OLIVARES, G., «Internet y propiedad intelectual», *en Internet y derecho penal, op. cit.,* p. 371 y ÁLVAREZ VIZCAYA, M., «Consideraciones político…», *op. cit.,* p. 271. En la doctrina italiana, a favor del reconocimiento de un nuevo bien jurídico, cifrado en la seguridad del sistema informático como objeto de extraordinaria relevancia en la actual sociedad, *vid*. BERGHELLA/BLAIOTTA, «Diritto penale dell'informatica e dei beni giuridici», in *Cassazione Penale*, 1995, p. 2334.

[92] Resultan significativos los datos ofrecidos por Naciones Unidas, en su Manual de prevención y fiscalización de los delitos relacionados con las computadoras (1997). En él se hace constar que el 90% de los delitos informáticos son cometidos por empleados de las empresas o instituciones afectadas. Por tanto, buena parte de dichos incidentes podrían evitarse con un plan de seguridad adecuado.

[93] QUINTERO OLIVARES, G., «Internet y propiedad intelectual», *en Internet y derecho penal, op. cit.,* p. 355.

CARRIÓN ZORZOLI, H., «Presupuestos para la incriminación del hacking», en *Revista de Derecho Informático*, n.º 37, agosto 2001.

DE ALFONSO LASO, D. «El hackering blanco. Una conducta ¿punible o impune?», en *Internet y derecho penal,* CGPJ, CDJ, X, 2001.

DIAS, P., «O hacking enquanto crime de acesso ilegítimo. Das suas especialidades à utilizaçào das mesmas para a fundamentaçào de um novo direito», en *Actualidad Jurídica Uría & Menéndez*, n.º 14, 2004.

ESCALONA VÁZQUEZ, E., «El hacking no es (ni puede ser) delito», en *Revista Chilena de Derecho Informático,* n.º 4, 2004.

FAROLFI, F., «I crimini informatici», en http://ei.unibo.it/materie/pdf/reati_informatici.pdf.

GALÁN MUÑOZ, A. «Ataques contra sistemas informáticos», en *Boletín de Información, La Armonización del Derecho Penal español: una evolución legislativa,* Ministerio de Justicia, Suplemento al n.º 2015, 15 de junio de 2006.

GONZÁLEZ RUS, J.J., «El cracking y otros supuestos de sabotaje informático», en *Estudios Jurídicos del Ministerio Fiscal*, II-2003.

GONZÁLEZ RUS, J.J., «Los ilícitos en la Red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA, C.M., Coord.), Granada, 2006.

GUTIÉRREZ FRANCÉS, M.L., «El intrusismo informático (Hacking): ¿Represión penal autónoma?», en *Informática y Derecho*, vol. 12-15.

MAGRO SERVET, V., «La delincuencia informática. ¿Quién gobierna en Internet?», en *La Ley,* n.º 6077, 2 de septiembre de 2004.

MARCHENA GÓMEZ, M. «El sabotaje informático: entre los delitos de daños y desórdenes públicos», en *Internet y derecho penal,* CGPJ, CDJ, X, 2001.

MATA Y MARTÍN, M., *Delincuencia informática y derecho penal*, Madrid, 2001.

MATELLANES RODRÍGUEZ, N., «El intrusismo informático como delito autónomo: razones», en *Revista General de Derecho Penal*, n.º 2, 1994.

MATELLANES RODRÍGUEZ, N., «Algunas notas sobre las formas de delincuencia informática en el Código Penal», en *Hacia un derecho penal sin fronteras* (DIEGO DÍAZ-SANTOS/SÁNCHEZ LÓPEZ, Coord.) Colex, 2000.

MIR PUIG, C., «Sobre algunas cuestiones relevantes del Derecho Penal en Internet», en *Internet y derecho penal,* CGPJ, CDJ, X, 2001.

MÖHRENSCHLAGER, M.E., «El nuevo derecho penal informático en Alemania», en MIR PUIG, S. (Comp.), *Delincuencia informática*, Barcelona, 1992.

MORALES PRATS, F., «Internet: riesgos para la intimidad», en *Internet y derecho penal*, CGPJ, CDJ, X, 2001.

MORALES PRATS, F., «Los ilícitos en la Red (II): Pornografía infantil y ciberterrorismo», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA, C.M., Coord.), Granada, 2006.

MORÓN LERMA, E*., Internet y derecho penal: hacking y otras conductas ilícitas en la Red,* 2.ª edición, Navarra, 2002.

MORÓN LERMA, E., *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías,* Navarra, 2002.

MORÓN LERMA/RODRÍGUEZ PUERTA, «Traducción y breve comentario del Convenio sobre Cibercriminalidad», en *Revista de Derecho y Proceso Penal*, n.º 7, 2002.

MUCIARELLI, F., «Commento all'art.4 della legge n.547 del 1993», en *Legislazione Penale*, 1996.

ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia 2001.

PERFETTI, T. «Del delitto di accesso abusivo ad un sistema informatico o telematico (art. 615 ter cp)», en *ScintLex, Diritto e Società dell'Informazione* (www.scintlex.it).

PUENTE ALBA, L.M., «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», en *Nuevos retos del Derecho Penal en la era de la globalización* (FARALDO CABANA, Dir.), Valencia, 2004.

RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, «Derecho penal e Internet», en *Régimen jurídico de Internet* (CREMADES/FERNÁNDEZ-ORDÓÑEZ/ILLESCAS, Coord.), Madrid, 2002.

ROMEO CASABONA, C.M., «Los delitos de daños en el ámbito informático», en *Cuadernos de Política Criminal,* n.º 43, 1991.

ROMEO CASABONA, C.M., «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», en *Poder Judicial*, n.º 31, 1993.

ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Granada, 2002.

Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo)*

Ricardo M. Mata y Martín
Profesor Titular de Derecho Penal. de la Universidad de Valladolid

Constituye para mi un alto honor la invitación para participar en las IV Jornadas de Derecho Penal en homenaje a D. José M.ª Lidón. Cuando la desaparición de la persona que da lugar al homenaje se produce por la voluntad de utilización sistemática de la violencia para coaccionar y amedrentar a la sociedad, y lograr así objetivos «políticos», aquella muerte adquiere una significación especial. En estos casos el homenaje no puede reducirse a un mero recuerdo de su persona, sino que se presenta como imprescindible una reafirmación de los valores y presupuestos de la convivencia que también se atacan con un asesinato de este signo. Sólo si se percibe claramente que el ataque terrorista en sus múltiples versiones daña a la sociedad en su conjunto y no solamente a la víctima inmediata se adoptará la perspectiva adecuada para afrontar el problema.

Frente a la barbarie, la civilización representada en la ley. Estado de Derecho que para ser real debe ser estable en su aplicación y no sometido a conveniencias del momento. Frente a la violencia, aplicación pacífica de la ley que permita la paz social. Frente a la coacción, libertad para los ciudadanos. Libertad real para expresar opciones y opiniones en el marco del respeto a la ley. Valores del Estado de Derecho, paz social y libertad todos ellos recogidos en la Constitución de 1978 que marcan el camino acertado y eficaz par el logro de una convivencia social que no admita como un agente político más a quienes esgrimen directa o indirectamente como argumento la violencia y el miedo.

* El trabajo que se presenta a continuación es parte de las labores de investigación realizadas en el seno del Grupo de Investigación Reconocido sobre Derecho de las Nuevas Tecnologías y Delincuencia Informática para los Proyectos de Investigación VA 111/04 (Junta de Castilla y León) y SEJ 2004-3704 (Planes Nacionales I+D/I+D+i), sobre medios electrónicos de pago.

I. **Criminalidad informática. Los delitos cometidos mediante sistemas informáticos**

La primera reacción ante los nuevos hechos irregulares que el desarrollo tecnológico permitía realizar fue la de la sorpresa. Y no es de extrañar pues las posibilidades que se abren para el ser humano y los cambios que puede generar han sido equiparados a la revolución industrial[1]. La llamada revolución cibernética instaura una nueva filosofía de la tecnología con repercusión en todos los ámbitos de la vida humana mediante la creación de sistemas automatizados de información y de control[2].

A la hora del estudio y tratamiento jurídico la sorpresa se traducía en la búsqueda acelerada de nuevas categorías con las que lograr sistematizar mejor estos nuevos hechos. En el terreno penal se proponían nuevos bienes jurídicos a los que asociar las emergentes conductas (libertad informática, intangibilidad informática, etc.), abandonando los esquemas y bienes jurídicos ya acuñados en los que se pensaba no se podían incluir los ataques y agresiones contra las personas y la sociedad realizados mediante las Nuevas Tecnologías.

Este impulso inicial llevó a establecer en los países de legua española la denominación de «delito informático», en parte consecuencia de verse un todo nuevo en el fenómeno y, también en parte, por arrastre de la terminología anglosajona (*computer crime*).

No demasiado tarde se advirtió que en realidad las múltiples conductas que se podían realizar por medios informáticos poseían también un variado reflejo legal. La gran diversidad de hechos relacionados con lo informático afectaban de manera plural a los bienes jurídicos y a tipos penales de la parte especial del Código Penal. Pero, como se pudo comprobar, tal «delito informático» no resultaba ni único ni unidireccional. En realidad la principal novedad del conocido inicialmente como «delito informático» era la de un nuevo, y de gran magnitud, factor criminógeno. Desde este punto de vista aparece la informática como factor criminógeno: permite el acceso y el manejo de bases de datos con ingentes cantidades de datos, realización de operaciones desde lugares lejanos y no visibles directamente a una gran velocidad y sobre un número potencial de víctimas enorme en muchos casos, siendo más costosa y compleja técnicamente la averiguación del autor y la prueba de los hechos.

---

[1] Sieber, U. *Computerkriminalität und Strafrecht*. Manchen, 1977, p. 23.

[2] Morón Lerma, E. *Internet y Derecho penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi, 222, p. 25.

En la sistematización del conjunto de hechos de la criminalidad informática pueden distinguirse dos grandes grupos[3]. En primer lugar aquellos en los que la informática o los sistemas informáticos constituyen el instrumento para cometer los hechos previstos en la ley penal, el medio de comisión para la lesión de un determinado bien jurídico. En este primer grupo podemos incorporar, entre otros, las estafas electrónicas, la difusión de ciertos materiales pornográficos o el ciberterrorismo. Estos son los hechos que vamos a desarrollar con posterioridad. Por otra parte aquellos en los que el hecho delictivo recae precisamente sobre algún tipo de elemento informático, el objeto material lo integran por tanto los propios soportes o sistemas informáticos. En este grupo se integran, por ejemplo, los ataques de denegación de servicio a un servidor (posible delito de daños), la descarga o la copia de una obra protegida en ciertos casos (delitos contra la propiedad intelectual) o el borrado o alteración de datos reservados incluidos en algún tipo de archivo informático en los delitos contra la intimidad.

Pese a lo indicado anteriormente respecto a esta clasificación no se puede ser excesivamente rígido pues la realidad resulta mucho más compleja. En los delitos relativos a la propiedad intelectual se puede actuar sobre una obra electrónica —en cuyo caso lo que destaca es el objeto de naturaleza electrónica— pero a la vez resulta necesario en muchos otros casos la Red como medio de ejecución del hecho punible. Igual sucederá con los delitos contra la intimidad relacionados con la informática en los que en ocasiones lo relevante será el medio electrónico de ejecución y en otros el archivo o dato reservado de naturaleza electrónica sobre el que se actúa —en realidad para estos delitos parece necesaria ambas vertientes—.

Aún así quedaría por perfilar cuando un hecho concreto pertenece a esta delincuencia informática, pues no basta que exista un delito en el que de alguna manera aparezcan elementos informáticos. Hace un tiempo apareció en la prensa universitaria que en la Facultad de Derecho de la Universidad de Zaragoza había sido sustraído un ordenador que contenía la única copia de una tesis doctoral en marcha, curiosamente sobre el tema de la rehabilitación del delincuente. Se trata de un hurto simple (respecto a la mera sustracción del equipo informático),

---

[3] Mata y Martín, R.M. *Delincuencia informática y Derecho penal*. Edisofer, 2001, p. 23. También Orts/Roig. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, 2001, p. 13. Respecto al Derecho suizo y austriaco, véase Javato Martín, A. M.ª «La tutela penal del consumidor en el comercio electrónico en el Derecho suizo». *RECPC,* n.º 7, pp. 1 y ss.; del mismo, «La protección penal del consumidor en el comercio electrónico en el Derecho austriaco». *CPC,* n.º 90, pp. 69 y ss.

en el que el ordenador no representa más que el objeto material de la sustracción como lo podía haber sido cualquier otro. Por eso entiendo que únicamente cabe hablar de delincuencia informática cuando bien como medio de ejecución o como objeto sobre el que recae el delito, los elementos informáticos alcanzan en la realización del mismo un papel relevante. Es necesario que se den las notas o características de lo informático de modo relevante. Por eso no calificaremos de delitos informáticos las amenazas o injurias que pueden realizarse a través de Internet, pero en los que en general —a salvo el caso concreto— no aportan las condiciones que hacen de los medios y objetos informáticos un factor criminógeno de primer orden.

Con todo lo discutible de las categorías que hemos mencionado vamos a pasar a estudiar con algo más de detalle ciertos supuestos pertenecientes al primer grupo, en cuyo caso no es especialmente el contenido lo que fundamenta el injusto penal sino la transmisión o difusión de ese contenido, en este caso mediante procedimientos electrónicos, es decir de modo especialmente relevante mediante Internet.

II. **Las estafas: utilización fraudulenta de tarjetas de pago**

1. *Situación actual*

Las tarjetas constituyen el medio de pago más difundido, incluso resulta más habitual que el pago en efectivo. Este uso masivo de las distintas clases de tarjetas en múltiples ámbitos ha propiciado también el uso fraudulento de las mismas. Conforme a la regulación actual del Código Penal, en el que no existe una previsión específica —salvo para el caso de las falsedades, art. 387, que las considera moneda—, el uso fraudulento de una tarjeta puede dar lugar a distintos tipos penales.

En principio el lugar natural para el tratamiento penal de un pago irregular realizado mediante tarjeta sería el delito de estafa. Este es el tipo central de las acciones defraudatorias en el ámbito patrimonial y la tarjeta en el contexto de un pago deliberadamente invalido representa el medio de ejecución de una perjuicio patrimonial. Inicialmente el tipo penal aplicable es el de la estafa convencional del art. 248.1 del Código Penal. Estamos hablando de los casos en los que la tarjeta ajena se presenta como medio de pago en el comercio en el que se adquiere un bien o un servicio de forma que el comerciante acepta el pago en la creencia de que se trata del auténtico titular de la tarjeta. En realidad quien la presenta no es el titular sino alguien que se hace pasar por él y que emplea la tarjeta como medio de engaño para que le sea facilitado

el bien o prestado el servicio. Con ello se cumplen los requisitos de la estafa convencional del art. 248.1, cuando señala «Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno».

Esta formulación de la estafa representa el paso de las anteriores construcciones casuísticas del delito sobre la base de la descripción de distintas modalidades de engaño a otra en la que se establece una noción general de estafa y se señalan los distintos elementos constitutivos en un orden lógico y secuencial.

La estafa requiere en primer lugar una conducta engañosa por parte del autor del hecho (en nuestro caso la presentación de la tarjeta afirmando así aparentemente la capacidad y voluntad de pago, así como la solvencia suficiente). El engaño llevado a cabo por el sujeto activo debe ser bastante y producir en otro una situación de error (el comerciante confía en la solvencia de quien es titular de una tarjeta de pago pero realmente no se trata del titular). La situación de error que padece le lleva a efectuar un acto de disposición patrimonial (la entrega del bien o la prestación del servicio por parte del receptor del pago), lo cual produce un perjuicio patrimonial para esa misma persona o un tercero (el propio comerciante, la entidad emisora de la tarjeta o el propio titular de la misma, según a quién corresponda hacerse cargo de la cantidad defraudada). Desde el punto de vista subjetivo el autor del hecho debe actuar con ánimo de lucro —y no con otro diverso— buscando la satisfacción de un interés económico como sucede en estos casos de pago ficticio con tarjeta sin abono real del precio.

En los últimos años se ha puesto de manifiesto además la necesidad de que el receptor del pago cumpla con ciertos deberes de diligencia en la aceptación del pago. Tanto desde el ángulo de la exigencia de «engaño bastante» en la descripción del tipo como de acuerdo a los presupuestos generales de la moderna teoría de la imputación objetiva, se hace preciso que se de cumplimiento a ciertos deberes de autoprotección en la correcta realización del pago. En el caso de la presentación de la tarjeta como forma de pago en un comercio, la diligencia mínima exige que el comerciante compruebe la identidad del portador de la tarjeta (coincidente con la identidad del que figura en el mismo instrumento de pago) y de la fecha de caducidad de la tarjeta.

Con la aparición de la posibilidad técnica de efectuar pagos con tarjeta a distancia, sin necesidad de presencia del titular, se introdujeron algunos problemas que trascendieron al tratamiento jurídico-penal de estos supuestos. Los procedimientos electrónicos, especialmente Internet, han facilitado las operaciones comerciales remotas que normalmen-

te se saldan con el pago mediante la aportación también electrónica de los datos de una tarjeta.

Sin embargo se ha entendido que la posibilidad de un aprovechamiento fraudulento de estos nuevos sistemas de pago no podía resolverse de la misma forma que en los pagos presenciales. Estas diferencias han tenido su origen en la concepción mayoritaria del engaño como elemento típico del delito de estafa. Según la doctrina científica y jurisprudencial dominante el engaño en el seno de la estafa tiene necesariamente un carácter personal, sólo puede darse en una relación directa entre dos personas, al igual que el error debe también ser consecuencia de esa previa acción engañosa de tipo psicológico sólo posible en una situación de inmediación personal[4]. Debido a estos presupuestos se hacía imposible la aplicación a estos supuestos de la estafa clásica o convencional. Por ello el legislador de 1995, con la aprobación del nuevo Código Penal, incluyó un supuesto diferenciado de estafa electrónica o informática (art. 248.2). En ella las referencias al engaño y al error no se hacían constar dada su naturaleza personal y se establecía en su lugar el requisito de la manipulación informática. Manipulación llevada a cabo por el autor a la que se añadía de manera confusa la posibilidad sustitutiva de utilización de un «artificio semejante». Mediante la manipulación informática el sujeto debía conseguir la transferencia no consentida de algún activo patrimonial. Los activos patrimoniales, en principio virtuales, se constituyen así en los objetos sobre los que incidirá patrimonialmente la manipulación para producir finalmente un perjuicio en el patrimonio de un tercero. La transferencia supone el paso de activos de naturaleza contable inicialmente al patrimonio de hecho del autor y que se traduce en la causación de un perjuicio efectivo.

Mediante el tipo de la estafa electrónica se pueden captar los supuestos de pagos fraudulentos en la Red, en los que el autor utiliza datos falsos de una tarjeta o unos verdaderos de otro titular evitando hacerse cargo del pago. La aplicación de este supuesto es posible merced al empleo de una noción amplia de manipulación informática que admite su vinculación tanto al sistema informático mismo como a los datos con los que opera el sistema. El concepto amplio de manipulación informática responde básicamente al propuesto por ROMEO[5], en el sentido de la in-

---

[4] Sobre ello extensamente MATA Y MARTÍN, R. M. *Los delitos de estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Aranzadi, 2007. Véase asimismo JAVATO MARTÍN, A.M.ª «Análisis de la jurisprudencia penal en materia de medios electrónicos de pago». *Los Medios electrónicos de pago. Problemas jurídicos,* Ed. Comares, Granada, 2007, pp. 367 y ss.

[5] ROMEO CASABONA, C.M. *Poder informático y seguridad jurídica.* Madrid, 1987, p. 47.

correcta modificación del resultado de un procesamiento automatizado en cualquiera de las fases de procesamiento o tratamiento informático con ánimo de lucro y perjuicio de tercero.

Un enfrentamiento con este concepto extenso de manipulación informática se ha producido con la Sentencia del Juzgado de lo Penal n.º 3 de Málaga de 19 de diciembre de 2005[6] que excluye la introducción de datos no propios en el sistema informático como supuesto de estafa electrónica. El caso hace referencia a hechos en los que los imputados «puestos previamente de común acuerdo en fecha 28 de noviembre del 2000 a través de la página www.tododvd.com de la empresa Red Fénix Sistemas, SL realizaron el pedido de un reproductor de DVD marca Pionner modelo 530/535 con precio de venta 438 € a nombre de Luis Pedro, … y realizando el pago con la tarjeta VISA núm. NUM006, de la que era titular un tercero ajeno a los hechos, quien no había autorizado a los acusados a utilizarla».

Después de unas consideraciones generales sobre el delito[7] el órgano jurisdiccional rechaza la aplicación del delito de estafa informática, pues entiende que —sin demasiadas precisiones— no se da ninguna de las dos situaciones propias del delito. Al parecer tan sólo concibe como objeto de esta modalidad de estafa la actuación sobre los datos existentes (alteración, modificación, supresión, etc.) en el sistema y no la inclusión de nuevos datos, pese a que en ambos casos se produce el resultado de alteración del resultado debido del procesamiento informatizado de los datos. «Huelga decir que ninguna de esta conductas fue llevada, a cabo por los acusados los cuales compran a través de una página web un reproductor de DVD y para el pago del precio designan un número de tarjeta VISA de la que es titular otra persona totalmente ajena a los hechos. Por ello no cabe incluir la conducta de los acusados

---

[6] ARP 2006/43.

[7] «La estafa o fraude informático hace referencia clara, pues, a dos tipos de conductas: a) La alteración, supresión u ocultación de datos existentes en el sistema manipulando o incidiendo en el mismo directamente o empleando artificio semejante, con lo cual aunque el funcionamiento correcto del programa se altera, se llega a un resultado no deseado, bien omitiendo la realización de operaciones procedentes (por ejemplo, no descornando un cargo), bien realizando otras improcedentes (por ejemplo dando por realizada una operación o aumentando o disminuyendo su importe real)… b) Las manipulaciones efectuadas no en los datos sino en la configuración del programa incidiendo en el mismo directamente o empleando artificio semejante, lo que constituye una verdadera manipulación informática que ocasiona que el programa realice operaciones en modo diferente al establecido, aun con datos correctos, ejecutando por ejemplo un cálculo erróneo como puede ser aumentar el importe de la nómina de un empleado, desviar partidas hacia cuentas ficticias, modificar el tratamiento de cuentas corrientes para aumentar los saldos o hacer posible la autorización de pagos, transferencias, etc.»

en el párrafo segundo del art. 248 del Código Penal pues los mismos no manipularon sistema o programa informático alguno sino cuando se les solicita el número de una tarjeta bancaria para cargar en la cuenta asociada a la misma el importe de la compra efectuada designan el número de una tarjeta de la que no es titular ninguno de los acusados y es en la creencia de que todos los datos introducidos en la página web al hacer el pedido del reproductor de DVD son correctos por lo que la empresa Red Fénix SL, procede a hacer la entrega de dicho aparato en el domicilio indicado al hacer el pedido.»

Esta modalidades de uso no autorizado de los datos no deja de suscitar dudas desde el ángulo de las exigencias del principio de legalidad, aunque en general se estima correcta su inclusión en el ámbito de la tipicidad para evitar lagunas. La exclusión de los supuestos de utilización de datos ajenos en el pago parece que pretende distinguir entre las manipulaciones sobre datos ya ingresados en el sistema (típicos) y las que suponen introducir nuevos datos no existentes previamente en el sistema (conducta atípica). En realidad en todos los supuestos anteriores los datos son objeto de tratamiento por el sistema informático y en ambos casos se produce un resultado desviado del mismo. De admitirse tal distinción quedarían excluidas de la estafa informática todas aquellas conductas de introducción de datos ajenos para realizar compras en Internet que hasta la fecha están siendo castigados mediante tal tipo penal, como lo hace el Tribunal Supremo. En este sentido la STS de 20-11-2001[8] señala que la manipulación informática «bien puede consistir en la alteración de los elementos físicos, de aquellos que permiten su programación o por la introducción de datos falsos».

Todavía nos quedaría un ámbito en el que se produce la utilización fraudulenta de las tarjetas. Se trata de los cajeros automáticos de las entidades financieras que facilitan la realización de múltiples operaciones a cualquier hora. Estos sistemas también han propiciado el uso irregular de las tarjetas, habitualmente para obtener cantidades en metálico de los cajeros. La aparición novedosa de estos supuestos sin que el Código Penal contase con ninguna previsión específica para los mismos y el que normalmente los cajeros estuvieran incluidos en un espacio cerrado al que se accedía también mediante la tarjeta llevó a los Tribunales a entender que se trataba de un robo mediante llaves falsas.

Con la aprobación del Código Penal de 1995 el legislador entendió que la solución propuesta por los Tribunales hacía posible considerar llave falsa a la tarjeta en todos los casos y de esta forma incluyó en el

[8] RJ 2002/805.

ámbito de la definición de las llaves falsas un último párrafo por el que se pretendía la equiparación de tarjetas con banda magnética y llaves falsas («A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas y los mandos o instrumentos de apertura a distancia», art. 239 *in fine*).

La consecuencia ha sido que los Tribunales normalmente han apreciado en estos casos un robo con fuerza en las cosas mediante la aplicación de la previsión específica del último párrafo del art. 239 —salvo algún ligero gesto de desacuerdo— sin entrar a considerar algunos aspectos discutibles y que dificultaban la estimación de un auténtico delito de robo[9]. En este sentido cabe señalar que el propio precepto hace referencia a que tal consideración se hace «A los efectos del presente articulo», es decir para el caso de un robo mediante llaves falsas, lo cual hace necesario que se den todas las características propias de las llaves falsa en el delito de robo y las características generales de este, singularmente el que deba emplearse el medio de fuerza «para acceder al lugar donde éstas se encuentran» (art. 237). El propio precepto se refiere a los mandos o instrumentos de «apertura» a distancia retomando el contexto propio del robo con fuerza en las cosas y que sería exigible también para esta modalidad. Además las llaves en el Código Penal español se consideran falsas cuando cumplen la función de apertura de un lugar cerrado mediante su aplicación a un dispositivo de cierre que se abre conforme a su funcionamiento regular. Sin embargo las tarjetas en los cajeros no tienen por qué dar paso previo a un espacio cerrado y además añaden otros aspectos que exceden de la escueta llave falsa construida en el Código como mero instrumento material de apertura.

En realidad este tipo de hechos por su naturaleza se corresponde con una acción defraudatoria, a la que no se puede aplicar la estafa convencional por la ausencia de engaño personal según ha exigido la doctrina y los Tribunales. Pero es que la tarjeta mucho más allá de su posible función como medio de apertura se presenta como un instrumento de legitimación en el ejercicio de un derecho de crédito frente a la entidad financiera —con base en la relación jurídica previa entre titular de la tarjeta y entidad emisora— que comprobando mediante sistemas automatizados a titularidad del instrumento accede al pago.

---

[9] Entorno a este problema de manera más detallada Mata y Martín, R. M. *Los delitos de estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Aranzadi, 2007. También, Javato Martín, A.M.ª «Análisis de la jurisprudencia penal en materia de medios electrónicos de pago». *Los Medios electrónicos de pago. Problemas jurídicos,* Ed. Comares, Granada, 2007, pp. 367 y ss.

2. *El Proyecto de reforma del Código Penal*

El Proyecto de reforma del Código Penal de 15 de diciembre de 2006 pretende añadir en el ámbito de las estafas del art. 248 como supuestos específico la utilización de tarjetas o de los datos correspondientes a las mismas. Con carácter general la Exposición de Motivos del Anteproyecto justifica en buena medida sus propuestas con base en los compromisos y obligaciones que la integración europea supone para la Justicia Penal en sus distintas dimensiones penal, procesal, judicial y policial. Entre los ámbitos que son objeto de armonización comunitaria está el de los medios de pago y que daría lugar a la nueva regulación mencionada.

En el mencionado texto de reforma de la legislación penal al grupo de modalidades típicas de la estafa del art. 248 se ha añadido la defraudación mediante la utilización de tarjetas ajenas o de los datos correspondientes a las mismas. De esta manera el número primero del art. 248 mantendría la figura del tipo básico de la estafa (convencional), pero en el número segundo se incluirían un listado de supuestos que resultarían equiparados, mediante la formula de «También se consideran reos de estafa», a la que se añade cuatro letras en las que se incorporan otros tantos casos particulares de estafa. En la letra a) del segundo número del precepto indicado se consigna la estafa electrónica que anteriormente constituía el único supuesto previsto en esta misma ubicación sistemática. La regulación de la estafa electrónica no varía pero sí su aplicabilidad como efecto de las nuevas modalidades incorporadas. En la letra c) se incrimina de forma expresa la utilización de tarjetas de crédito o débito o de los datos obrante en ellas para realizar operaciones de cualquier clase en perjuicio de otro. Las consecuencias de esta regulación propuesta serían varias. En primer lugar al estar contenida como una modalidad individual más de estafa la de pago fraudulento mediante tarjetas —diversa de la de estafa informática— se diversifica en mayor medida la regulación criminal de los usos fraudulentos de los medios de pago.

En la mencionada modalidad punitiva se incluye expresamente la utilización de los datos identificativos de una tarjeta, de forma diferenciada a los de utilización de la tarjeta misma. Esto implica, por una parte, el refuerzo de la tesis —mantenida ya generalmente por los Tribunales— de que la utilización fraudulenta de los datos de una tarjeta que atribuían falsamente el pago de una operación al titular, resultaba punible como delito de estafa, pese a las dudas suscitadas por alguna resolución judicial. Pero además supone la falta de posesión material de la tarjeta por parte del autor, lo que hace necesario un pago en línea —no presencial— que en principio debería tratarse como estafa informática. Sin embargo la previsión específica de este nuevo supuesto desplaza a

tal modalidad —con base en el principio de especialidad— por lo que sería de aplicación esta particular previsión sobre la base de utilización fraudulenta de tarjetas ajenas. Con ello se vaciaría en buena medida de contenido práctico la estafa electrónica del actual art. 248.2.

El que se trate de una modalidad diferenciada mediante el empleo de la tarjeta o de sus datos no excluye que deba reunir los elementos genéricos de la estafa. Lo contrario sería hacer perder sentido a su ubicación sistemática y la declaración legal por la cual «también se consideran reos de estafa» a los que cometan tal acción punible. De forma paralela a lo previsto en el art. 400 del CP se incluyen también (letra b) las conductas de «los que fabricaren, introdujeren o facilitaren programas informáticos especialmente destinados a la comisión de las estafas previstas en este artículo». Lo cual parece excesivo no sólo por tratarse propiamente de actos meramente preparatorios, sino porque a estos autores en principio deberíamos considerarlos también «reos de estafa». Pero evidentemente no puede ser así pues la acción —como tal acto preparatorio— carece de cualquier correlato o equivalencia con una conducta de estafa.

El tratamiento penal del uso irregular de tarjetas en cajeros automáticos con el Proyecto de Ley de reforma del Código Penal de diciembre de 2006 no ha recibido alteración alguna. Sin embargo una contemplación inicial de la regulación propuesta podría llevar a pensar que puesto que en el 248.2 letra c) se quiere incriminar la utilización fraudulenta de tarjetas en «operaciones de cualquier tipo» debería ser de aplicación esta nueva modalidad. Pero sucede que el autor del Proyecto no ha modificado la previsión del art. 239 respecto a la equiparación de las tarjetas magnéticas con las llaves falsas como instrumento de delito de robo, por lo que es de suponer que seguirá siendo aplicable, pese a que como se ha pretendido poner de manifiesto esta modalidad es la más necesitada de reorientación.

III. **Conductas relativas a la difusión de pornografía**

1. *La preocupación ascendente de la Comunidad Internacional por la protección de la infancia y de la juventud*

Es cada vez más patente la ocupación de los Organismos Internacionales en la defensa de los derechos y libertades de los menores. Entre los distintos ámbitos en los que se quiere actuar está el de la lucha contra la trata de seres humanos, la explotación sexual de los niños y la pornografía infantil. Por ello en las últimas décadas es posible encontrar un buen número de declaraciones y textos de origen supranacional en

los que se manifiestan esta preocupación y se establecen, en algunos casos, medidas dirigidas a la protección de este sector de la población especialmente sensible.

En la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de la ONU en su resolución 44/25, de 20 de noviembre de 1989 se establecen un conjunto de derechos del niño. Se tiene presente que, como se indica en la Declaración de los Derechos del Niño, «el niño, por su falta de madurez física y mental, necesita protección y cuidado especiales, incluso la debida protección legal, tanto antes como después del nacimiento». En su artículo 19 se obliga a los Estados Partes a adoptar «todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual». De forma más directa para nuestro tema el art. 34 establece que «Los Estados Partes se comprometen a proteger al niño contra todas las formas de explotación y abuso sexuales. Con este fin, los Estados Partes tomarán, en particular, todas las medidas de carácter nacional, bilateral y multilateral que sean necesarias para impedir:

a) La incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal;
b) La explotación del niño en la prostitución u otras prácticas sexuales ilegales;
c) La explotación del niño en espectáculos o materiales pornográficos.

Desde 1996 la Unión Europea estableció una serie de programas en materia de lucha contra la trata de seres humanos y la explotación sexual de los niños. Para ello se desarrollaron los programas *STOP* y *DAPHNE* contra la violencia de la que son objeto las mujeres y niños. Implican tanto a las autoridades públicas como a las ONG. En 1997 el Consejo adoptó una Acción Común para favorecer la cooperación judicial. El Consejo Europeo de Tampere y el de Feira invitaron a los países miembros a adoptar medidas concretas en esta materia. Se señalaba que a pesar de las modificaciones introducidas por los Estados miembros en su legislación respectiva, la cooperación judicial es difícil por la falta de definiciones comunes de los elementos constitutivos del delito, la incriminación y las sanciones aplicables.

Con el fin de remediar esta situación la Comisión presentó en diciembre del 2000 dos propuestas de Decisiones Marco. La primera, relativa a la *lucha contra la trata de seres humanos*, que aborda dos distintos aspectos de este tráfico: el tráfico con fines de explotación sexual

y laboral. La segunda, relativa a la *explotación sexual de los niños y a la pornografía infantil*, referida al nuevo fenómeno de la pornografía infantil en Internet. Al elaborar ambas propuestas la Comisión tuvo en cuenta los trabajos realizados en el ámbito internacional y recogidos por el Protocolo de la ONU sobre la trata de seres humanos y por el Proyecto de Convenio del Consejo de Europa relativo a la ciberdelincuencia.

Una primera medida la constituye la Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre la lucha contra la trata de seres humanos y contra la explotación sexual de los niños y la pornografía infantil (COM (2000) 854 final), con la que se quiere reforzar la protección jurídica para las víctimas de estas infracciones y prever medidas para garantizar su reinserción social. Se pretende introducir medidas eficaces contra toda la cadena de la trata de seres humanos, desde el reclutador y el transportista hasta el explotador o cliente. La Comisión se declara consciente de que el fenómeno de la trata de seres humanos ha adquirido una dimensión mundial ya que decenas de miles de personas, sobre todo niños y mujeres, son sus primeras víctimas. Las causas de este tráfico son la pobreza, el desempleo y la ausencia de educación o la vulnerabilidad de algunas categorías como niños y mujeres. Con el fin de encontrar una solución satisfactoria, la Comisión sugiere un enfoque general que pueda abordar los distintos aspectos de un problema tan complejo.

Posteriormente se aprueba una Decisión del Consejo, de 29 de mayo de 2000[10], relativa a la lucha contra la pornografía infantil en Internet, en la que se trata de prevenir y combatir la producción, el tratamiento, la difusión y la posesión de pornografía infantil en Internet. En la Decisión se señala que los Estados miembros tomarán medidas destinadas a animar a los usuarios de Internet a que comuniquen a las autoridades policiales sus sospechas sobre la difusión de material pornográfico infantil en Internet; garantizar que las infracciones en este ámbito sean investigadas y reprimidas, por ejemplo mediante la creación de unidades especializadas dentro del ámbito policial; garantizar una respuesta a tiempo de las autoridades policiales en cuanto reciban información sobre supuestos casos de producción, tratamiento, posesión y difusión de material pornográfico infantil. Por otra parte, los Estados miembros comprobarán regularmente si la evolución tecnológica exige la modificación de sus procedimientos penales en el ámbito de la lucha contra la pornografía infantil en Internet.

Para facilitar la colaboración entre los Estados, se difundirá la lista de los puntos de contacto nacionales que funcionen las 24 horas del

[10] Diario Oficial L 138 de 09-06-2000.

día y de las unidades especializadas. Deberá informarse a Europol de los supuestos casos de pornografía infantil; se organizarán reuniones entre los servicios nacionales especializados. Los Estados miembros estudiarán todas las medidas que permitan la eliminación de la pornografía infantil en Internet e intercambiarán sus mejores prácticas. Se someterán a estudio nuevas obligaciones para los proveedores de servicios de Internet: información a las autoridades competentes en caso de difusión de material de pornografía infantil a través de ellos, retirada de dicho material, conservación del mismo para ponerlo a disposición de las autoridades e incluso la creación de sus propios sistemas de control. En cooperación con la industria, se fomentará la creación de filtros u otras posibilidades técnicas de prevención y detección de este tipo de material.

En el ámbito del Consejo de Europa, pero con trascendencia más amplia, se gestó el Convenio de Cibercrimen (Budapest 2001), en cuyo preámbulo se advierte de los riesgos de la sociedad de la información y de la necesidad de una política penal común para la protección de la sociedad en el ciberespacio, siempre dentro del respeto a los intereses legítimos relativos al desarrollo de la sociedad de la información y a los derechos fundamentales del ser humano. Entre los cuatro grupos de infracciones que el Convenio estipula como aquellas que las legislaciones nacionales deben incriminar, están las infracciones relativas al contenido, que incluyen múltiples conductas realizadas por el autor sobre materiales de pornografía infantil. Se trata de conductas de producción, ofrecimiento, difusión o transmisión o procurar para otro por medio de un sistema informático pornografía infantil. Se extiende la incriminación a la obtención para sí mismo (art. 9.1 letra d) de estos materiales mediante un sistema informático o la mera posesión del material en un sistema informático o de almacenamiento de datos informáticos (art. 9.1 letra e). La Convención se detiene en la determinación del concepto de material de pornografía infantil de manera que establece un concepto claramente amplio del mismo. Así el art. 9.2 considera pornografía infantil todo material pornográfico que represente de manera visual un menor desarrollando un comportamiento sexual explícito, representando una persona que aparezca como un menor desarrollando un comportamiento sexual explícito, o las imágenes realistas representando a un menor desarrollando un comportamiento sexual explícito. Es decir, incluye, tanto el material pornográfico realizado efectivamente con menores, como aquellos otros casos en los que los menores que figuran en el material no son auténticos, pero las imágenes puedan considerarse realistas. La Convención considera como menores a las personas que no hayan alcanzado los 18 años aunque admite que las partes firmantes fijen el límite en los 16 años.

Más recientemente, otra vez en el seno de la Unión Europea, se adopta la Decisión Marco 2004/68/JAI del Consejo de 22 de diciembre de 2003 relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil. Esta Decisión Marco tiene por objeto aproximar las disposiciones legales y reglamentarias de los Estados miembros relativas a la cooperación policial y judicial en materia penal con el fin de luchar contra la trata de seres humanos, la explotación sexual de los niños y la pornografía infantil. La Decisión introduce un marco normativo común a nivel europeo para abordar cuestiones tales como la tipificación penal, las sanciones, las circunstancias agravantes, la competencia y la extradición. Se considera que pese a las distintas iniciativas adoptadas desde hace tiempo, como la adopción por el Consejo en 1997 de una Acción Común en materia de lucha contra la trata de seres humanos y la explotación sexual de los niños, el Plan de Acción de Viena así como en las Conclusiones del Consejo Europeo de Tampere, resulta más adecuado el instrumento de la Decisión Marco, introducido por el Tratado de Amsterdam, para responder mejor a estas prioridades.

En cuanto al contenido, el artículo 1 de la Decisión Marco proporciona la definición de algunos términos fundamentales, como «niño», «pornografía infantil», «sistema informático» y «persona jurídica». De acuerdo con las disposiciones del Convenio de las Naciones Unidas sobre los derechos del niño, la Comisión considera, que el término «niño» es aplicable a cualquier menor de 18 años, aunque haya alcanzado una cierta madurez. El segundo artículo enuncia una serie de comportamientos que deben considerarse ilícitos en cuanto «infracciones relacionadas con la explotación sexual de los niños», tales como coaccionar a un niño para que se prostituya, explotar o lucrarse con ello o facilitarlo por cualquier otro medio; practicar con un niño actividades sexuales recurriendo a alguno de los medios siguientes:

—hacer uso de la fuerza, la coacción o la amenaza,
—ofrecer dinero u otras formas de remuneración a cambio de servicios sexuales,
—abusar de una posición reconocida de confianza, autoridad o influencia sobre el niño.

Los comportamientos punibles incluidos en la Decisión Marco constituyen una «infracción relacionada con la pornografía infantil» se realicen mediante sistemas informáticos o no, son:

—producción de pornografía infantil, o
—distribución, difusión o transmisión de pornografía infantil, o

—ofrecimiento o facilitación por cualquier otro medio de pornografía infantil, o
—adquisición o posesión de pornografía infantil.

De forma que los Estados miembros adoptarán las medidas necesarias para garantizar la punibilidad de la inducción a la comisión de las infracciones mencionadas, así como la tentativa de comisión de las mismas. Las sanciones previstas por cada Estado deberán ser como siempre «efectivas, proporcionadas y disuasorias». La pena privativa de libertad para las infracciones contempladas en los artículo 2, 3 y 4 tendrá una duración de al menos entre uno y tres años. La pena privativa de libertad para determinadas infracciones con circunstancias agravantes prevé una duración de al menos entre cinco y diez años. El artículo 5 proporciona una lista de circunstancias agravantes, sin perjuicio de otras circunstancias establecidas en la legislación nacional cuando:

—la víctima sea un niño que no haya alcanzado la edad del consentimiento sexual según el derecho nacional;
—el autor haya puesto en peligro de forma deliberada o por imprudencia temeraria la vida del niño;
—la infracción se haya cometido empleando violencia grave contra el niño o causándole un daño grave;
—la infracción se haya cometido en el marco de una organización delictiva según la definición de la Acción Común 98/733/JAI.

Cada Estado miembro podrá introducir disposiciones destinadas a inhabilitar a las personas físicas, condenadas por una de las infracciones enunciadas, para el ejercicio de actividades que supongan el cuidado de niños. Además, la Decisión Marco introduce la responsabilidad penal y civil de las personas jurídicas. Esta responsabilidad es complementaria de la de la persona física. La persona jurídica será responsable si la infracción es cometida en su provecho por cualquier persona, actuando a título individual o como parte de un órgano de la persona jurídica, o que ejerza un poder de decisión. Estas sanciones para las personas jurídicas serán «efectivas, proporcionadas y disuasorias», incluirán multas de carácter penal o administrativo, y sanciones específicas como la prohibición temporal o permanente del desempeño de actividades comerciales, una medida judicial de liquidación, o la exclusión del disfrute de ventajas o ayudas públicas.

Desde el punto de vista procesal y con el fin de evitar que el delito quede impune por la existencia de algún conflicto de competencia, la Decisión introduce criterios de atribución. Un Estado tendrá poder de jurisdicción cuando:

—la infracción se cometa en su territorio (principio de territorialidad);
—el autor de la infracción tenga la nacionalidad de dicho Estado miembro (principio de personalidad activa);
—la infracción se cometa en provecho de una persona jurídica establecida en el territorio de dicho Estado miembro.

El segundo criterio es especialmente importante para los Estados que no conceden la extradición de sus nacionales, ya que deberán establecer las medidas necesarias para perseguir judicialmente a sus nacionales por las infracciones cometidas fuera de su territorio.

Para el 20 de diciembre de 2006 los Estados miembros deberían haber adoptado las medidas necesarias con el fin de adaptar su legislación nacional a la Decisión Marco. Las disposiciones adoptadas por los países miembros deberán comunicarse a la Secretaría General del Consejo y a la Comisión. Sobre la base del informe redactado con esta información y del informe escrito de la Comisión, el Consejo comprobará, antes del 20 de enero de 2008, la adecuación de las disposiciones nacionales a la presente Decisión Marco.

2. *Marco general de las conductas punibles relativas a la pornografía*

Entre los delitos contra la libertad e indemnidad sexual aparecen los hechos punibles relativos a la difusión de pornografía. Algunos de los mismos pueden tener una especial vinculación con los medios informáticos. En principio las conductas realizadas con los materiales pornográficos no son en sí mismas consideradas como hechos delictivos. Únicamente por su conexión, de diferentes formas como se verá, con los menores o incapaces, pueden alcanzar la gravedad suficientes como para incluirse en un tipo delictivo. De manera que exclusivamente en los casos de pornografía dirigida a menores, participación de estos en espectáculos pornográficos y de pornografía infantil pueden revestir relevancia penal este tipo de hechos.

Se advierte así un proceso en cierto modo contradictorio pues si por una parte los delitos en el ámbito de la sexualidad y de las conductas relativas a los materiales pornográficos han sido objeto durante las últimas décadas de un continuo proceso de restricción, últimamente se pone de manifiesto un interés por el control de la incidencia de conductas con contenido sexual en los menores, especialmente en lo que a las Nuevas Tecnologías se refiere.

En la regulación actual, sin mencionar expresamente los medios informáticos, se contiene el castigo una multiplicidad de conductas típicas,

como son las de la producción, difusión, exhibición y venta de material pornográfico cometido por cualquier medio siempre que se realice sobre menores o incapaces, éstos participen en espectáculos de esa misma naturaleza o se trate de pornografía infantil.

Como se puede apreciar el ámbito de relevancia de estas conductas tiene como referencia fundamental los materiales pornográficos y de pornografía infantil. Por ello debemos acercarnos a estas nociones y establecer una delimitación suficiente sobre las mismas. En general se suele tomar como referencia las orientaciones que sobre esta materia ha adoptado el Tribunal Supremo Federal de los Estados Unidos. En sentido positivo se vendría a exigir que el contenido global del material estuviera dirigido a excitar el apetito sexual de quienes lo contemplaran y, de forma inversa, que careciera de otros valores suficientemente representado en el material, como los de tipo literario, artístico, pedagógico, científico u otros.

El mencionado Tribunal, según señalan R. Mourullo/Alonso/Lascurain[11] distingue tres posibles estratos en la gravedad de este tipo de contenidos: indecencia, obscenidad y pornografía infantil. La pornografía infantil como supuesto más grave se considera toda imagen (y no los textos) que represente a menores en actitud sexualmente explícita. La obscenidad ha dado paso a una doctrina conocida como «Test Miller» y que comprueba tres aspectos: 1) si el ciudadano medio considera que de acuerdo a los criterios generales de la comunidad la imagen o el texto en su conjunto despierta intereses lascivos, 2) si el contenido representa de manera manifiestamente ofensiva conductas sexuales específicamente definidas por las leyes estatales, y 3) si el texto o la imagen carecen de otra clase de valores como los literarios, artísticos, políticos o científicos. La noción de indecente tiene carácter residual respecto a los anteriores contenidos. El ámbito de lo punible de la pornografía infantil es total desde la distribución hasta la posesión, incluyendo la descarga de estos contenidos de una página *web*. Los contenidos obscenos en cambio podrían ser objeto de posesión en la intimidad del propio hogar en un uso personal. El material meramente indecente resulta amparado por la primera Enmienda pero mediante regulación pueden establecerse determinadas limitaciones como la de prohibir su distribución entre menores.

En lo que hace referencia a la pornografía infantil el Consejo de Europa define la misma como «cualquier material audiovisual que utiliza niños en un contexto sexual» (Recomendación R(91) 11 e informe del Comité Europeo de Problemas Delictivos - 1993)[12]. Se trata de una pri-

---

[11] «Derecho penal e Internet». *Régimen Jurídico de Internet*, La Ley, 2002, p. 301.

[12] Cfr. Morales Prats, F. «Pornografía infantil e Internet». http://www.uoc.edu/in3/dt/20056/index.html, p. 2

mera aproximación pero que resulta excesivamente amplia a los efectos penales pues no discrimina en forma alguna la presencia de los menores en el contexto sexual, lo que puede dar lugar a equívocos. Por ello se suele exigir que el material cualquiera sea su modalidad haya sido elaborado con menores y los mismos alcancen una presencia significativa en el mismo y no meramente ocasional, con inequívocas implicaciones sexuales[13]. Como se ha anticipado la Convención sobre Cibercrimen del Consejo de Europa se ocupa de las conductas relativas a la pornografía infantil llevadas a cabo por y con medios informáticos y de la determinación del concepto. En el art. 9.2 se considera pornografía infantil todo material pornográfico que represente de manera visual un menor desarrollando un comportamiento sexual explícito (a), representando una persona que aparezca como un menor desarrollando un comportamiento sexual explícito (b), o las imágenes realistas representando a un menor desarrollando un comportamiento sexual explícito (c). Con ello se establece una noción amplia de pornografía infantil, siempre referida a comportamientos sexuales explícitos pero que abarca no solamente el material pornográfico realizado efectivamente con menores, sino también aquellos otros casos en los que una persona se hace pasar por un menor y otros en los que los menores que figuran en el material no han participado de forma real en la elaboración del material, pero las imágenes en las que se inserta la figura del algún menor puedan considerarse realistas.

Aun con todos estos perfiles no deja de ser cierto que las nociones de material pornográfico y de material de pornografía infantil no dejan de adolecer de una total certeza, pues las mismas están sujetas a un cierto relativismo cultural y a una determinación subjetiva sobre los valores presentes en el material[14]. Por ello como bien señala Morales[15], es preciso realizar una interpretación material, evitando una mera apreciación formal que pudiera acabar por comprometer las libertades del art. 20 CE. La interpretación restrictiva la entiende posible Muñoz Conde[16] a través de la toma en consideración del contexto (entre otros extremos con la edad y nivel cultural del destinatario), y el que el material de acuerdo a la rúbrica del Capítulo IV sirva como medio de provocación sexual, de manera que

---

[13] Cfr. Orts, E./Roig, M. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, 2001,p. 133.

[14] Cfr. Orts, E./Roig, M. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, 2001, p. 131. También Morales Prats, F. «Pornografía infantil e Internet». http://www.uoc.edu/in3/dt/20056/index.html, p. 2.

[15] «Los ilícitos en la red: pornografía infantil y ciberterrorismo». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona coordinador). Comares, 2006, p. 282.

[16] *Derecho Penal, Parte Especial*. Tirant lo Blanch, 2004, p. 239.

se estime idóneo para producir algún daño en el desarrollo de la personalidad para persona inmaduras o incapaces de un cierto control de sus instintos sexuales.

3. *Materiales pornográficos dirigidos específicamente a menores*

En el caso de la pornografía dirigida a menores lo que se castiga es la intromisión en la indemnidad sexual del menor mediante la facilitación de materiales pornográficos precisamente a sujetos menores de edad (art. 186). Como se sabe estos menores se sitúan en las edades inferiores a los dieciocho años. No se castigan en este supuesto actividades de elaboración o tráfico de material pornográfico, sino exclusivamente de acciones de difusión de los materiales en dirección a menores o incapaces. En definitiva, en el contexto de la incriminación del art. 186 no se trata de un comportamiento realizado con menores, sino una actividad sobre o dirigida a menores, a los que se debe hacer destinatarios del material pornográfico. En consecuencia de todo ello estas mismas conductas realizadas entre adultos carecerían de cualquier significación penal.

Las conductas punibles son las de venta, difusión o exhibición de este tipo de materiales a menores o incapaces. Para evitar algunas aplicaciones inadecuadas, la redacción del tipo exige que el comportamiento se lleve a cabo «por cualquier medio directo». Esta restricción impone una relación directa del autor del hecho con el menor, excluyéndose los casos de venta, difusión o exhibición genérica del material, aun cuando en la práctica pudiera tener algún destinatario menor o incapaz. Para algunos autores este requisito suscita un problema interpretativo al entender que, en definitiva, no puede realizarse informáticamente —singularmente vía Internet— «por cualquier medio directo»[17].

Como se puso de manifiesto en trabajos anteriores en realidad esta exigencia típica no supone ningún obstáculo para admitir conductas pu-

---

[17] Así lo entiende TAMARIT SUMALLA, J.M. *La protección del menor frente al abuso y la explotación sexual*. Aranzadi, 2000, p. 141. Para ANARTE la incriminación contiene dos requisitos que dificultan su aplicación a hechos vinculados con un contexto tecnológico. Por una parte que el medio de venta, difusión o exhibición debe ser directo, es decir, dirigido a víctimas concretas o concretables o que estén físicamente presentes. Además estaría la exigencia de que se realice entre menores o incapaces e incluso el presunto elemento subjetivo de que la acción esté dirigida a involucrar al menor o incapaz en un contexto sexual. «Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal de la sociedad de la información». *Derecho y Conocimiento. Anuario Jurídico sobre la Sociedad de la Información*, volumen 1, 2001, pp. 228-9.

nibles relacionadas con Internet[18]. La Red admite posibilidades de difusión tanto indirecta como directa hacia menores. Medio directo sería claramente el correo electrónico o bien a través de un *chat* en el que se hubiera generado relación específica con un menor. No se puede apreciar en estos casos diferencias justificadas en el tratamiento penal con la entrega personal del material o incluso con el envío por correo postal del material a un determinado menor o incapaz. Medio indirecto y por tanto genérico —no punible— sería la difusión del material a través de una página *web*. Problema distinto, aunque también de relevancia, será el del conocimiento de la edad del sujeto al que se dirige el material pornográfico —tanto mediante actuaciones materiales o a través de Internet—, con la posibilidad real de errores con trascendencia en la responsabilidad penal.

4. *Conductas de intervención del menor o incapaz en espectáculos pornográficos*

En el ámbito de las conductas del Capítulo V («De los delitos relativos a la prostitución y a la corrupción de menores») se castiga la utilización de menores o incapaces en espectáculos exhibicionistas o pornográficos. De los dos grupos de conductas incriminadas en el art. 189, el primero (letra a del número 1 del precepto) incrimina a quien utilice a menores o incapaces en ese tipo de espectáculos. Sería punible por esta vía quien utiliza a los menores en un espectáculo que a través los medios tecnológicos se transmite distintos receptores sin que propiamente se haya elaborado un material pornográfico[19].

Morales Prats/Garcia Albero[20] plantean un aspecto de gran interés para la delimitación del ámbito del la conducta típica. Señalan estos autores que puesto que el tipo del art. 189.1.a no indica nada respecto al tipo de implicación del menor en el espectáculo exhibicionista o pornográfico, deberá entender que la extensión de la incriminación no se limita a aque-

---

[18] Sobre este problema puede verse Mata y Martín, R. M. *Delincuencia informática y Derecho penal*. Edisofer, Madrid, 2001, pp. 107 y ss. También Orts, E./Roig, M. Señalan la posibilidad de aplicar el art. 186 en los supuestos de venta, difusión o exhibición de material pornográfico por la red, a menores o incapaces, siempre que las conductas se realicen de modo directo, esto es, dirigidas a menores concretos o concretables. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, 2001, p. 125.

[19] *Cfr.* Anarte Borrallo, E. «Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal de la sociedad de la información». *Derecho y Conocimiento. Anuario Jurídico sobre la Sociedad de la Información*, volumen 1, 2001, p. 226-7.

[20] *Comentarios a la Parte Especial del Derecho penal* (QUINTERO, Director), Aranzadi, 2005, p. 351.

llos casos en los que el menor es parte activa de conductas o escenas de tipo obsceno, sino que abarca también las conductas en las que el menor se limita a presenciar la conducta obscena protagonizada por mayores de edad pues el menor queda involucrado en un contexto atentatorio a su indemnidad sexual. A este respecto puede señalarse que si bien es cierto que el fundamento general de las conductas punibles es la situación en la que se pone al menor que implica una agresión al libre desarrollo de su persona en el ámbito sexual, no es menos cierto que la configuración de los elementos típicos del art. 189.1.a hacen difícil entender que la conducta de «utilización de menores o incapaces con fines o espectáculos exhibicionistas o pornográficos» lo sean en sentido diverso al de participación activa en el espectáculo. La acción de utilización en relación a su presencia en un espectáculo parece obligar a la existencia de una intervención no puramente pasiva, al margen de que sea deseada o no por el menor y que el espectáculo lo protagonicen mayores u otros menores.

Si los usuarios o los organizadores del espectáculo graban el mismo se está realizando ya un material pornográfico cuya relevancia penal debería ser estudiado conforme a las previsiones de la letra b) del art. 189.1[21] que pasamos a comentar. Esta misma letra a) del precepto se refiere a la elaboración del material de pornografía infantil con la utilización de menores o incapaces que por su coincidencia con la posterior regulación de la letra b debe entenderse incluida en las explicaciones que siguen.

5. *Conductas relativas a materiales de pornografía infantil*

Otro campo diverso es el de la pornografía infantil del art. 189.1.b. En este precepto lo que se castiga son conductas relativas al total ciclo en el que puede estar presente un material pornográfico en el que intervengan menores. En este caso el menor juega el papel ya no de receptor del material sino de elemento constitutivo fundamental del material pornográfico. Se trata de materiales pornográficos en los que el menor es el protagonista del mismo, ahora con independencia del sujeto destinatario de tal material.

En primer lugar resulta punible la creación de este material pornográfico en el cual se empleen menores o incapaces, normalmente como ac-

---

[21] Como señalan Orts, E./Roig, M. *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, 2001, p. 130. También en el mismo sentido Anarte Borrallo, E. «Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal de la sociedad de la información». *Derecho y Conocimiento. Anuario Jurídico sobre la Sociedad de la Información*, volumen 1, 2001, p. 227.

tividades dirigidas a la posterior comercialización del material, aun cuando este último extremo no lo requiere la regulación. En este primer momento del ciclo, se incriminan conductas de elaboración o producción del material (art. 189.1, letra a, segundo inciso y primer inciso de la letra b del art. 189.1). Junto a las conductas propiamente de autoría, la letra b hace referencia también a la facilitación de la producción del material que por su naturaleza podría incluir conductas de mera complicidad y que sin embargo por decisión del legislador se equiparan a la misma elaboración del material y por tanto a la autoría con la misma pena. Las previsiones legales no establecen ningún género de restricción en cuanto al procedimiento de producción del material, por lo que las técnicas informáticas y electrónicas tienen perfecta cabida en los supuestos de hecho.

En la letra b del mismo precepto se incluyen distintas conductas relativas a este tipo de materiales pornográficos especialmente concernientes a momentos posteriores a lo que constituye la producción de los mismos. De esta manera el tipo recoge las actividades de venta, exhibición o difusión o la facilitación de estas misma actividades en relación a materiales pornográficos construidos sobre la base de menores e incapaces. Además de la amplitud del abanico de conductas abarcadas el legislador efectúa dos discutibles equiparaciones. Por una parte a las actividades de venta, distribución o exhibición en sentido estricto iguala las de su facilitación como sucedía con la producción del material y con los mismos efectos. Se impone la misma pena a actividades que por su naturaleza pueden ser muy diversas, asimilando el legislador la mera complicidad a la autoría. Pero además se añade la posesión de material de pornografía infantil, para los mismos fines de venta distribución o exhibición, lo que en sí mismo es menos criticable pero genera indudables problemas de prueba[22]. Estos materiales pueden tener cualquier naturaleza que admita su tratamiento y difusión por la Red, como puede ser imágenes, sonidos, etc. Además la regulación admite la desconexión con los principios generales al posibilitar la persecución de los hechos «aunque el material tuviere su origen en el extranjero o fuere desconocido».

También la posesión misma del material, sin conexión con la realización de alguna de las anteriores conductas resulta incriminada, aunque ahora como tipo atenuado. Con la reforma de 1999 la posesión

[22] Con base en la mencionada equiparación legal no es posible considerar correcto que «la tenencia con fines de difusión a terceros o de tráfico debe entenderse como un principio de ejecución del delito del apartado 1 y penarse como tentativa del mismo» según señala Monterder Ferrer, F. «Especial consideración de los atentados por medios informáticos contra la intimidad y la privacidad». *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad? Cuadernos de Derecho Judicial* III, 2006, p. 234.

constituía un tipo privilegiado y se vinculaba de manera necesaria con la finalidad última de realizar alguna de las actividades ya mencionadas con el material pornográfico. Tras las posterior reforma de 2003 la posesión dirigida a tales fines se sitúa como modalidad básica alternativa, equiparada por tanto a las actividades de venta, difusión o exhibición. Además la mera posesión de material de pornografía infantil constituye a partir de este momento una infracción penal en sí misma considerada («para su propio uso») pero como modalidad atenuada (art. 189.2).

La incriminación de la mera posesión del material de pornografía infantil resulta acorde con la tendencia mostrada por las Instituciones y Convenciones Internacionales en las últimas décadas —como en el caso de los instrumentos de la Unión Europea o el Convenio de Cibercrimen— según hemos señalado ya[23]. Sin embargo, pese a esta coincidencia, no deja de representar problemas político-criminales de envergadura. En este sentido Muñoz Conde[24] estima que con esta criminalización el legislador invade la privacidad de las personas en una medida difícilmente conciliable con el derecho constitucional a la intimidad, sin que se produzca una afectación del bien jurídico tutelado y con infracción del principio de intervención mínima.

El número 7 del art. 198 introduce —con la reforma del año 2003— una nueva precisión sobre el material que puede constituir el objeto material de las conductas punibles de producción, venta, distribución, exhibición o facilitación del mismo. Admite como hecho punible las actividades anteriores sobre una material pornográfico en cuya elaboración no se hubieran empleado menores al menos directamente pero sí su voz o imagen alteradas. Se establece la pena de prisión de tres meses a un año o multa de seis meses a dos años para «el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada».

La incorporación de esta modalidad de material pornográfico infantil supone una ampliación del objeto material del delito y por tanto de su ámbito de aplicación. Para Morales[25] ya la reforma del 1999 permitía

---

[23] Sin embargo como recuerda acertadamente Morales Prats la propia Convención de Cibercrimen admite ciertas modulaciones que no haría necesaria la punición de la posesión en sentido estricto. Por otra parte no sucede lo mismo con la Decisión Marco de 2005 que no deja ese ámbito de decisión.

[24] *Derecho Penal, Parte Especial*. Tirant lo Blanch, 2004, p. 245

[25] Morales Prats, F. «Los ilícitos en la red: pornografía infantil y ciberterrorismo». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona coordinador). Comares, 2006, pp. 283 y 292 y ss.

incluir en la órbita del tipo los supuestos de la denominada pseudopornografía o pornografía simulada en la que se insertan fotogramas o imágenes de menores reales en escenas pornográficas (animadas o no), pues entienden que en tales supuestos se verifica objetivamente una utilización del menor. Sin embargo señala que no resulta incriminada la llamada pornografía técnica en la que adultos aparentan ser menores a los efectos del material en el que se desarrollan comportamientos sexuales explícitos. Y no se incluyen en el ámbito de la tipicidad del nuevo número 7 del art. 189 pues éste exige que en todo caso se empleen la voz o la imagen de un menor, aunque alterada.

La extensión de los supuestos de empleo de voz o imagen real de menores aunque modificadas le parece a MORALES[26] una solución plausible y político-criminalmente al resguardo de las criticas que pudieran efectuarse desde el ángulo de la ausencia de lesividad u ofensividad de la conducta. Todo ello en consideración a la idea de que se está protegiendo la dignidad, el derecho a la propia imagen en el sentido de la *privacy* como derecho a no ser molestado en su esfera privada, pudiendo organizar el sujeto de modo originario el desarrollo de su personalidad. Además también se fundamenta en las dificultades para distinguir la utilización real o virtual de los menores en este tipo de materiales.

Sin embargo para ANARTE[27] la posibilidad de dotar de relevancia a la «pornografía infantil virtual» es nula. Bien es verdad que la opción de este autor se formuló antes de que el legislador incluyera el nuevo supuesto del número 7 del art. 189, pero sin embargo los argumentos parecen perfectamente aplicables a la nueva situación. En primer lugar apunta razones de pura legalidad pues el tipo exige literalmente la utilización de los menores, lo que excluiría tanto el supuesto de inserción de mayores que se hacen pasar por menores como en los casos en lo que se elabora el material mediante la inserción de imágenes manipuladas o digitales, pues en tal caso no se han utilizado propiamente a menores sino tan sólo sus imágenes. También desde el punto de vista del ataque a la libertad sexual, fijado como bien jurídico protegido en

---

[26] MORALES PRATS, F. «Los ilícitos en la red: pornografía infantil y ciberterrorismo». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA coordinador). Comares, 2006, pp. 293-4. Autor que también excluye de la relevancia típica los casos de comics de pornografía infantil en los que no se empleen voces reales de los menores (p. 294).

[27] «Incidencia de las Nuevas Tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información». *Derecho y Conocimiento. Anuario Jurídico sobre la sociedad de la información*, Volumen 1, 2001, p. 227.

este supuesto, carecería de significación la conducta, señalando además el autor que si se toma como referencia la dignidad o la intimidad se corre el riesgo de abarcar conductas cuyo castigo debe plantearse en otro contexto. Igualmente la dificultad para discernir en muchos casos la participación real del menor en el material de la participación puramente virtual se descarta como razón suficiente para su castigo. De forma más contundente MUÑOZ CONDE señala que una interpretación literal puede llevar a la punición de una utilización de imágenes virtuales sin ninguna base real, lo que le lleva a preguntarse si ¿No estamos aquí ante un «Derecho penal de autor» que penalice la tendencia pederasta como tal aun sin que se traduzca en actos que incidan directamente en el menor o incapaz?

6. *El proyecto de reforma del Código Penal*

La Exposición de Motivos del Proyecto de reforma en curso del Código Penal señala que «la formulación de los delitos contra la libertad sexual en nuestro vigente derecho es, en verdad, amplia pero, a pesar de ello, un examen detenido de las diferentes figuras legales ha puesto de manifiesto la existencia de algunos graves vacíos que afectan, además, al grave problema de las agresiones o abusos sexuales de los que son víctimas niños, condición de las víctimas que ha marcado claramente los delitos de tráfico de pornografía —cuya regulación penal se amplía incluyendo más conductas— pero que no había completado su despliegue en todas las infracciones del grupo».

Ello se traduce en que en el artículo 189 se modifican la letra a) del apartado 1 y la letra b) del apartado 3, se añade la letra g) al apartado 3 y se modifica el apartado 8

> «1. Será castigado con la pena de prisión de uno a cuatro años:
>
> a) El que utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.
>
> (…)
>
> 3. Serán castigados con la pena de prisión de cuatro a ocho años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:
>
> (…)
>
> b) Cuando la participación del menor o incapaz en los espectáculos pornográficos o exhibicionistas hubiera sido conseguida mediante

violencia o intimidación, o los hechos revistieran un carácter particularmente degradante o vejatorio.

(…)

g) Cuando se hubiere puesto en peligro la vida o la salud del menor o incapaz.

(…)

8. Cuando los delitos comprendidos en este capítulo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de clausura temporal de sus locales y establecimientos de dos a cinco años.»

En definitiva en el apartado 1.a) del art. 189 se añade junto a las conductas anteriores y la financiación de los espectáculos exhibicionistas o pornográficos en los que intervenga el menor o incapaz la punibilidad de quien se lucre con ello, lo cual generará importantes dificultades a la hora de fijar el alcance de las conductas alcanzadas con penal de manera semejante a como ha sucedido en el ámbito de la prostitución. Además se produce una adaptación más estricta a los supuestos agravados señalados por la Decisión Marco de la Unión Europea en esta materia.

IV. **Ciberterrorismo**

1. *La nueva situación general*

El desarrollo tecnológico logrado por el ser humano en las últimas décadas ha abierto una brecha con el pasado no tan remoto de forma que lo impulsa hacia nuevos estadios históricos. Las actividades sociales de tipo económico, laboral, educativo, de comunicación y otras se apoyan progresivamente en mayor medida en la vinculación a redes de transmisión de datos y procesos automatizados. Pero también la vida cotidiana de los ciudadanos cada vez resulta más asociada a las infraestructuras tecnológicas.

La creciente dependencia de todos los sectores de la vida social de su conexión a procedimientos automatizados e informatizados hace que lo hechos irregulares e ilícitos que puedan ser cometidos a través o sobre este tipo de sistemas alcancen progresivamente una mayor trascendencia. Los servicios públicos (sanidad, regulación del tráfico rodado, aéreo o marítimo), la producción industrial, el comercio, la defensa de un país o la enseñanza, van integrándose inexorablemente en el entramado de las tecnologías de la información y telecomunicaciones.

Todo ello representa sin duda un nuevo mundo y un abanico de posibilidades emergentes para el conjunto social y para las personas singulares. Pero no es menos cierto que asociado a este mismo desarrollo tecnológico aparecen nuevos riesgos y amenazas.

2. *Alianza del terrorismo y el desarrollo tecnológico*

a) La delincuencia en general, y en particular la delincuencia organizada aprovecha los nuevos métodos proporcionados por los avances técnicos en lo que se conoce como la delincuencia de alta tecnología. La enorme difusión social de los medios informáticos, en todos los ámbitos institucional, empresarial, comercial y doméstico, ha provocado un espectacular aumento de su presencia social y el empleo de importantes cantidades monetarias en empresas, materiales e infraestructuras. Con todo ello la emergencia y pujanza de las modernas tecnologías de la información han conducido también hacia una forma diferenciada de «Delincuencia de alta tecnología»[28] y que en ocasiones se conoce como el lado oscuro de la globalización. En realidad se trata de un proceso históricamente más lento pero constante en la vida social en el que la delincuencia reasume los avances tecnológicos dirigiéndolos hacia sus fines.

b) En este contexto el terrorismo, como forma específica de delincuencia organizada percibe las ventajas y posibilidades del uso de los nuevos medios tecnológicos[29]. El conocido como ciberterrorismo constituye una nueva forma, amenazante y específica de terrorismo moderno[30]. Se trata de una nueva dimensión en la estrategia de los grupos armados que su-

---

[28] THIELE, M. *Dimension und Bekamfung.* Marburg, 2001.

[29] Sobre la relación entre terrorismo y delincuencia organizada BOVENKERK, F./CHAKRA, B A. «Terrorismo y delincuencia organizada». *Foro sobre el delito y sociedad* 1,2, 2004, pp. 6 y ss. Autores que establecen los puntos de conexión y las analogías estructurales llegando a convencerse de la convergencia de ambos fenómenos (p. 14). También se analiza en la obra del Conseil de l´Europe. *Criminalité organisée en Europe. La menace de la cybercriminalité*, 2006, pp. 168 y ss. Ya en 1982 se produce en San Sebastián la detención de siete miembros de la banda E.T.A. que, junto con otros tres miembros, integraban un comando de información, transmisiones y electrónico (denominado precisamente comando electrónico). Dicho grupo confeccionaba aparatos electrónicos para ser utilizados posteriormente en la activación de artefactos explosivos. Asimismo, interfería en varias ocasiones emisoras comerciales de radio y de televisión. En los registros practicados se intervinieron armas, explosivos, abundante material para la confección de aparatos electrónicos, así como aparatos para emitir mensajes en frecuencia de TV y Radio.

[30] Conseil de l´Europe. *Criminalité organisée en Euroepe. La menace de la cybercriminalité*, 2006, p. 178.

pone el aprovechamiento para sus fines de las posibilidades que brindan las nuevas tecnologías.

El concepto de ciberterrorismo no deja de resultar problemático y según los límites a los que se someta puede abarcar un número más reducido o más amplio de conductas delictivas. Un concepto sumamente amplio de ciberterrorismo puede ser el de «aquél conjunto de acciones, que son o intentan ser anónimas, orientadas a dañar o dejar fuera de servicio, temporal o definitivamente, sistemas informáticos, pertenecientes a la Administración, Gobiernos, agencias gubernamentales, grandes firmas comerciales o industriales, o su seguridad o su información, disminuyendo o menoscabando su imagen, por razones políticas o ideológicas; o bien contra los recursos estratégicos o datos reservados de redes privadas, por venganza o por razones económicas; o contra los ordenadores personales de particulares para descubrir y capturar palabras de acceso o cuentas e información sobre las mismas»[31]. Nociones tan amplias no proporcionan claridad —incluyendo elementos innecesarios como el anonimato, el posible ánimo de venganza o razones económicas— y admiten un excesivo número de conductas delictivas que no necesariamente se vinculan a actuaciones de grupos terroristas.

En realidad debe tratarse, en definitiva, de la alianza de los grupos terroristas con los nuevos procedimientos destructivos generados por los últimos desarrollos tecnológicos[32]. Para ser estrictos en el ámbito del denominado ciberterrorismo se deben concitar por tanto la presencia de un grupo terrorista y por otra el empleo de los medios propios de las infraestructuras tecnológicas lo que les permite una ampliación de su capacidad operativa. En las publicaciones del Consejo de Europa se ha definido como ciberterrorismo «la utilización o amenaza al recurso intencional —sin autoridad legalmente autorizada— de la violencia contra sistemas cibernéticos o bien la perturbación o la injerencia en estos sistemas, cuando es probable que semejante acción se saldará con una pluralidad de muertos o heridos, graves daños materiales, desordenes civiles o un importante perjuicio económico»[33].

---

[31] Cortijo Fernández, B. «Ciberterrorismo: concepto, armas, ataques y consecuencias». *Actualidad informática Aranzadi*, 40/2001, p. 12.

[32] El Segundo informe sobre el uso de Internet por los terroristas realizado por el *United Status Institute of Peace* recoge la definición de ciberterrorismo de la Profa. Dorothy Denning como la convergencia de ciberespacio y terrorismo. http://www.francispisani.net/2004/05/la_paradoja_del.html.

[33] Conseil de l´Europe. *Criminalité organisée en Europe. La menace de la cybercriminalité,* 2006, p. 178. Define el Ciberterrorismo como «la forma de terrorismo que utiliza las tecnologías de información para intimidar, coaccionar o para causar daños a grupos

Puede señalarse por tanto que debe tratarse del empleo por los grupos terroristas de los medios y procedimientos que proporcionan las Tecnologías de la información y del conocimiento para el logro de los fines ideológicos que sustentan su actividad. Hace referencia a la puesta en práctica de nuevas técnicas basadas en los avances sociales fundamentalmente en los ámbitos de las telecomunicaciones y la informática al servicio de los fines que ya se perseguían tradicionalmente. Medios insidiosos y clandestinos, que favorecen la ejecución a distancia del hecho sin riesgo de ser detenido en el momento, que favorecen el anonimato[34] —al menos con carácter previo—, son de fácil acceso y manejo sin necesidad de cuantiosos gastos y que dificultan las investigaciones para su esclarecimiento, al tiempo que poseen capacidad para producir efectos sobre las personas, sobre los bienes y —en cuanto a su eco social— sobre los medios de comunicación de grandes dimensiones.

Ahora bien esta conexión entre terrorismo y Nuevas Tecnologías se produce simultáneamente en plurales direcciones. Los grupos violentos de carácter terrorista pueden utilizar los procedimientos tecnológicos en el marco de la perpetración de acciones de sabotaje, pero también para sus propias comunicaciones, para transmitir su propaganda, la guerra psicológica, las incitaciones al odio y al crimen, el reclutamiento de miembros, así como para la instrucción de sus componentes y planificación de acciones[35].

3. *Las diversas formas de aprovechamiento de la tecnología para fines terroristas*

Resultan evidentes las posibilidades que abren las Nuevas Tecnologías para quienes desean provocar el pánico en una sociedad. Pero también que estos nuevos medios rápidamente adoptados por las organizaciones terroristas proporcionan no sólo mecanismos dirigidos directamente a causar víctimas y otros efectos materiales, sino que permiten abarcar

---

sociales con fines políticos-religiosos». Orta Martínez, R.«CiberTerrorismo». *Alfa-redi, Revista de Derecho Informático,* n.º 82, mayo de 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=949

[34] A este respecto Cortijo Fernández pone en duda la posibilidad real de anonimato señalando como dificultades reales para identificar al autor la falta de almacenamiento de datos o de colaboración por parte de los proveedores de Internet y el tiempo transcurrido desde el hecho. «Ciberterrorismo: concepto, armas, ataques y consecuencias». *Actualidad informática Aranzadi,* 40/2001, p. 13.

[35] Cfr. Conseil de l´Europe. *Criminalité organisée en Europe. La menace de la cybercriminalité.* 2006, p. 179.

un amplio espectro de las actividades de estos grupos. A los efectos de señalar las consecuencias más destacables en relación a estas conductas y su regulación penal podemos distinguir el empleo de las tecnologías para el uso directo en ataques sobre sistemas informáticos y —por otra parte— la puesta en práctica de los modernos medios tecnológicos en actividades internas o externas pero que no suponen la realización de ataques inmediatos sobre objetivos. En el contexto de ese tipo de acciones los delitos que más comúnmente se entienden puestos en juego por las mismas son el sabotaje informático (daños) o el intrusismo, hecho este mucho más indefinido desde el punto de vista jurídico penal en nuestro país.

a) En primer lugar destacan las Nuevas Tecnologías como instrumento de ataque sobre las infraestructuras básicas. Es posible mediante la interferencia en los sistemas que regulan las grandes infraestructuras producir perturbaciones y daños en las mismas con efectos de grandes dimensiones. Según las noticias proporcionadas por la prensa un ordenador de Al Qaeda capturado contenía los detalles de la estructura arquitectónica y de ingeniería de una presa, detalles que se habían descargado de Internet y habrían permitido a los ingenieros y planificadores de Al Qaeda simular fallos catastróficos[36]. En otros ordenadores capturados, los investigadores estadounidenses hallaron pruebas de que los técnicos de Al Qaeda habrían navegado por sedes que ofrecían programas e instrucciones de programación de los interruptores digitales que hacen funcionar las redes de energía, agua, transporte y comunicaciones.

Para valorar el posible impacto de estas acciones hay que tomar en consideración que el imparable avance técnico ha conducido a una sociedad (al menos en el llamado primer mundo) extremadamente dependiente de los sistemas automatizados, procedimientos informáticos y telecomunicaciones. Pero a su vez este conjunto tecnológico compone unos objetivos particularmente vulnerables a los ataques[37]. Las redes de telecomunicación, el sistema productivo y las grandes infraestructuras se apoyan en buena medida en sistemas de tratamiento de datos. «Los terroristas han aprendido que la seguridad nacional depende de las infraestructuras críticas que se sostienen mediante los sistemas y redes

---

[36] Según indica Salellas el FBI NIPC (*Nacional Infraestructure Protection Center*) informó sobre preparativos de ataques por grupos terroristas al sistema de aprovisionamiento de agua en los EEUU. «Delitos informáticos. Ciberterrorismo». http://www.llustrados.com/publicaciones/EEypVEluF1VYPABJae.php, p. 7.

[37] Cfr. Conseil de l´Europe. *Criminalité organisée en Europe. La menace de la cybercriminalité*. 2006, p.88.

telemáticas»[38]. En realidad ya antes de la implicación de las Nuevas Tecnologías los terroristas habían fijado su atención en el posible impacto de atentados sobre centros pertenecientes a las infraestructuras básicas de un país. «Este fue el caso de las Brigadas Rojas en Italia en los años setenta, que atentaron contra más de 25 centros considerados de interés neurálgico para el Estado»[39]. De forma que, como advierte ORTA MARTÍNEZ[40], la seguridad informática no depende solamente de los aspectos del *software* sino que también depende en gran medida de la seguridad física de los equipos.

De manera que las grandes instalaciones industriales, el control del tráfico automovilístico, marítimo, aéreo y espacial, el sistema energético de un país (con las centrales eléctricas convencionales y nucleares), el aprovisionamiento de agua para la población, las centrales telefónicas, el sistema sanitario y de emergencias, la propia infraestructura de Internet o las comunicaciones sustentan su actividad regular en redes de telecomunicación e información. Los estudios destacan los posibles efectos devastadores de un único ataque sobre alguno de estos centros y la amplificación de los mismos si se combinan con ataques convencionales[41]. Se propone como ejemplo el cambio remoto de la presión de un gaseoducto produciendo una interminable secuencia de explosiones e incendios[42]. Además de los posibles ataques que puedan recibir los centros neurálgicos encargados de administrar los servicios básicos del país también se encuentran los riesgos de ataques a los sistemas destinados a la defensa nacional[43].

Este tipo de hechos conocidos desde una perspectiva criminológica como sabotaje ha sido objeto de atención en instancias internacionales. Su realización puede llevarse a cabo bien mediante la introducción del autor directamente en el sistema ocasionando la destrucción de los elementos lógicos o bien mediante la introducción de programas o rutinas destructoras de los elementos lógicos sin un acceso individualizado como

---

[38] GUDÍN RODRÍGUEZ-MAGARIÑOS, F. *La lucha contra el terrorismo en la sociedad de la información*. Edisofer, 2006, p. 123.

[39] COSIDO GUTIÉRREZ, I. «Los riesgos cibernéticos». *CGC,* 25/2001, p.4.

[40] «CiberTerrorismo». *Alfa-redi, Revista de Derecho Informático*, n.º 82, mayo de 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=949.

[41] Cfr. Conseil de l´Europe. *Criminalité organisée en Europe. La menace de la cybercriminalité*. 2006, pp. 89 y 181. GUDIN indica que un ataque estratégico sobre estos sistemas tendría consecuencias apocalípticas para las naciones y la economía de las mismas. *La lucha contra el terrorismo en la sociedad de la información*. Edisofer 2006, p. 123.

[42] Cfr. SALELLAS, L. «Delitos informáticos. Ciberterrorismo». http://www.llustrados.com/publicaciones/ EEypVEluF1VYPABJae.php, p. 7.

[43] COSIDO GUTIÉRREZ, I. «Los riesgos cibernéticos». *CGC*, 25/2001, p. 7.

en el caso del correo electrónico que aporta virus o gusanos[44]. La Unión Europea presta atención a los fenómenos terrorista y de la delincuencia informática desde hace tiempo, no de forma conjunta pero si desde la común perspectiva de la creación efectiva de un espacio europeo único de justicia, libertad y seguridad[45]. El problema de los actos terroristas ya se mencionó con motivo del Consejo Europeo de Tampere en 1999 y del Consejo Europeo de Feira en junio del 2000. El terrorismo se considera una grave y seria violación de las libertades fundamentales, de los derechos humanos y de los principios de libertad y democracia. Se señala que ante tal amenaza los Estados miembros deben adoptar medidas para garantizar un verdadero espacio de libertad, seguridad y justicia.

Desde los ataques del 11 de septiembre de 2001, la Unión Europea ha intensificado la lucha contra el terrorismo. Así, adoptó una Decisión Marco que invita a los Estados miembros a acercar a sus legislaciones y que establece normas mínimas sobre delitos terroristas (Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo). Según la Decisión Marco los actos a incriminar deben ser cometidos con el fin de amenazar a la población y destruir o afectar seriamente a las estructuras políticas, económicas o sociales del país (asesinato, daños corporales, toma de rehenes, chantaje, fabricación de armas, atentados, amenaza de cometer tales actos, etc). Igualmente la Decisión Marco define a un grupo terrorista como una asociación estructurada de más de dos personas que actúa de manera concertada.

El posteriormente llamado Programa de La Haya, que se adoptó en el Consejo Europeo de 4 y 5 de noviembre de 2004[46], recoge las diez prioridades de la Unión destinadas a reforzar el espacio de libertad, seguridad y justicia durante los siguientes cinco años, entre las que se encuentran la

---

[44] Cfr. González Rus, J.J. «Los ilícitos en la red(I): hackers, crackers cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona, coordinador). Comares, 2006, p. 263. También Morón Lerma. E. *Internet y Derecho penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi, 2002, pp. 66-7. Esta autora distingue entre vandalismo informático (*ciberpunks*) y las acciones de los *hackers*, éstos últimos con un mayor conocimiento del medio.

[45] Inicialmente la Unión Europea estableció una Acción Común 96/610/JAI, de 15 de octubre de 1996, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la creación y mantenimiento de un Directorio de competencias técnicas y conocimientos antiterroristas especializados para facilitar la cooperación antiterrorista entre los Estados miembros de la Unión Europea.

[46] Comunicación de la Comisión al Consejo y al Parlamento Europeo. *Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia* [*COM (2005) 184* final - no publicada en el Diario Oficial].

lucha contra el terrorismo. Para luchar efectivamente contra el terrorismo se propone una respuesta global con un enfoque integrado y coherente. La Comisión hace hincapié en la prevención del terrorismo y el intercambio de información concentrándose en los aspectos relacionados con la captación de terroristas y la financiación del terrorismo, la prevención, el análisis de riesgo, la protección de las infraestructuras de riesgo y la gestión de las consecuencias y una propuesta destinada a evitar la utilización abusiva de organizaciones caritativas para financiar el terrorismo.

La Unión Europea se hizo consciente de la trascendencia de las Nuevas Tecnologías para las nuevas formas de delincuencia y su relación con la criminalidad organizada[47]. Con el fin de mejorar la seguridad de las infraestructuras de la información, la Comisión emitió propuestas dirigidas a prevenir y reprimir los delitos informáticos[48]. La Comisión lanzó la Iniciativa *eEurope* en diciembre de 1999. El plan de acción global sobre esta Iniciativa, aprobado por el Consejo Europeo de Feira en junio de 2000, destaca la importancia de la seguridad de las redes y de la lucha contra los delitos informáticos.

La Unión mediante Decisión Marco pretende reforzar la cooperación judicial relativa a los ataques contra los sistemas de información en el contexto de la creación de un espacio de seguridad, libertad y justicia. Se trata de la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información. Ya en el Consejo Europeo de Tampere, en octubre de 1999, los Estados miembros reconocieron la necesidad de llegar a un acuerdo sobre la definición de una serie de actos delictivos relacionados con las nuevas tecnologías. Estos hechos formaban parte de los actos incluidos en una lista (punto n.º 48 de las Conclusiones). Después la Comisión presentó un plan de acción global *eEurope* desarrollar todas las posibilidades ofrecidas por las nuevas tecnologías y hacer más seguras las redes informáticas.

La Decisión fija a este respecto una serie de nociones como las de sistema de información, datos informáticos, persona jurídica o sin auto-

---

[47] Ya el 19 de marzo de 1998 el Consejo invitó a los Estados miembros a adherirse a la red de información del G8 (accesible día y noche) con el objetivo de tratar cuanto antes y de manera cualificada los distintos tipos de delincuencia vinculada a la alta tecnología. Esta red permitirá a los países adherentes tener una visión global de la delincuencia vinculada a los sistemas informáticos y establecer entre ellos puntos de contacto para la lucha contra la delincuencia en el ámbito de la alta tecnología, puesto que se ejerce a menudo simultáneamente en varios países.

[48] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: *Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos* [*COM (2000) 890* final - no publicada en el Diario Oficial].

rización. De forma que también se indica las infracciones penales perseguibles judicialmente en aplicación de la Decisión Marco, como son el acceso ilícito a un sistema de información, el perjuicio a la integridad de un sistema (el hecho intencionado de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos), la intromisión ilegal en los datos. Se prevé que el elemento de la intencionalidad debe caracterizar en todo caso estos hechos delictivos. Además la inducción, la complicidad o la tentativa de cometer uno o varios de los actos antes mencionados serán también sancionables como infracciones penales.

Los hechos relativos a posibles ataques cibernéticos sobre infraestructuras también están previstos en el Convenio del Cibercrimen de 2001 (Budapest 23.11.01), máxima expresión de la necesidad de cooperación internacional en la lucha contra la criminalidad informática, aunque no previstos específicamente desde la óptica del terrorismo. El Convenio de Cibercrimen propone en esta materia varias infracciones que deberán ser incorporadas a las legislaciones nacionales y que clasifica en cuatro grandes grupos de ilícitos penales.

El primer grupo de infracciones y que es el que resulta de interés para nuestro tema, lo constituyen los hechos contrarios a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Dentro de este grupo se incluyen —en primer lugar— las conductas de acceso ilegal injustificado a todo o parte de un sistema informático (art. 2) y que en no pocas ocasiones se vincula al ciberterrorismo[49]. La legislación penal española actual —a diferencia de lo que sucede en otros países, como Portugal— no conoce una auténtica infracción de mero acceso o mero intrusismo informático[50]. De todas formas el Convenio permite que las partes firmantes modulen la incriminación de este su-

---

[49] Como por ejemplo hace Cortijo Fernández. Alude a las conductas de intrusión como una de las actividades del ciberterrorista, incluyendo en ella los intentos de entrada en un sistema, ataques enmascarados, penetraciones en el sistema de control, fugas o denegaciones de servicio. «Ciberterrorismo: concepto, armas, ataques y consecuencias». *Actualidad informática Aranzadi* 40/2001, p.12.

[50] Sobre la problemática del acceso ilegal en nuestro sistema penal puede verse Mata y Martín, R.M. «La protección penal de datos como tutela de la intimidad de las personas». *Revista Penal*, 18, julio 2006, pp. 234-5. La impunidad de las conductas de mero intrusismo informático la reconoce Morón Lerma, E. *Internet y Derecho penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi, 2002, p. 70. Respecto a la situación en el Derecho suizo y austriaco, Javato Martín, A.M.ª «La tutela penal del Consumidor en el comercio electrónico en el Derecho suizo», *RECPC,* n.º 7, pp. 1 y ss.; del mismo, «La protección penal del consumidor en el comercio electrónico en el Derecho austriaco», *CPC,* n.º 90, pp. 69 y ss.

puesto mediante diferentes formas. Así es posible vincular la punibilidad de este hecho a la violación de medidas de seguridad, la existencia en el autor de determinadas intenciones a la hora de realizar el hecho o la presencia de conexión entre distintos sistemas informáticos.

Aunque como advierte con razón MORON[51] «la exigencia de adicionales tendencias subjetivas en la propia definición típica de la conducta desvirtúa la caracterización del intrusismo y, por tanto, imposibilita conceptualmente su subsunción… Así la tipificación del acceso ilícito con el fin de descubrir la intimidad ajena o un secreto de empresa, o con la intención de causar un daño (entre otras posibilidades delictivas), determina que la conducta, al adentrarse en la órbita típica de otros ilícitos (delitos contra la intimidad, delitos contra los secretos de empresa, delitos de daños, etc.) no pueda ser ya calificada de mero acceso inconsentido. En estos casos, el acceso no autorizado deviene «modus operandi» de esas otras conductas principales, perseguidas y guiadas por ese concreto ánimo del autor». De manera entonces que el conocido como mero acceso informático puede desnaturalizarse por la incorporación de elementos subjetivos o por su vinculación con grupos de delitos de diversa perspectiva, llegando a constituir otra infracción distinta.

Esto es precisamente lo que sucede con la incriminación prevista en el Proyecto de reforma del Código Penal actualmente en tramitación en el que se incluye como punible la del «que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo», (castigado con pena de prisión de seis meses a dos años). En realidad no puede verse aquí la punición del mero intrusismo informático pues —aunque esa fuera la intención del prelegislador— se trata del acceso a los datos o programas y no al sistema informático sin más, vinculándose la conducta con los delitos contra la intimidad (datos) o de daños (programas), pero como actos preparatorios incriminados expresamente por el legislador[52].

---

[51] *Internet y Derecho penal: Hacking y otras conductas ilícitas en la Red*. Aranzadi, 2002, pp. 72-3. Todo ello de acuerdo a la caracterización de la conducta de mero intrusismo informático, pp. 50 y ss.

[52] La Exposición de Motivos del Proyecto señala como justificación que «la tutela penal de la intimidad y de los secretos ha sido tradicionalmente fragmentaria, y condicionada a la realización de conductas de apoderamiento de papeles, cartas o mensajes, o de instalación de aparatos de captación de imagen o sonido, pero a la vez que la importancia fundamental de ese bien jurídico exige cada vez mayor atención y medidas legales, como son esencialmente las recogidas en la legislación sobre protección de datos, crecen los riesgos que lo rodean, a causa de las intrincadas vías tecnológicas que permiten violar la

Eso sí, se prevé una agravante para los casos de comisión se lleva a cabo por organizaciones criminales, pues «la realidad de que los actos de invasión en la privacidad en todas sus manifestaciones no son siempre llevadas a cabo por individuos aislados ha determinado la incorporación de una cualificación punitiva para todas las acciones descritas en el artículo 197 en el caso de que se cometan en el marco de organizaciones criminales».

También se abarcan los supuestos de interceptación ilegal de comunicaciones entre sistemas informáticos o en el interior de un mismo sistema, mediante el empleo de medios técnicos (art. 3). En el art. 4 se sitúan los atentados a la integridad de los datos, consistentes en el daño, borrado, deterioro, alteración o supresión intencional de datos informáticos. Este supuesto se puede condicionar a la producción de daños de carácter grave.

Mayor novedad para el sistema español representa el caso de los atentados a la integridad de los sistemas, consistente en el entorpecimiento grave de un sistema informático mediante las conductas anteriores de introducción, transmisión de daño, borrado, deterioro o supresión de datos informáticos (art. 5). Finalmente en este primer grupo de infracciones se consideran como hechos dignos de castigo por las legislaciones nacionales todo tipo de conductas abusivas relativas a los dispositivos informáticos (desde la producción y venta hasta la obtención para su utilización) que permitan la realización de los hechos delictivos anteriores. También se incriminan las mismas conductas respecto a palabras clave o códigos de acceso de un sistema informático (art.6).

En general estas acciones de sabotaje contra redes de telecomunicación o infraestructuras básicas pueden ser reconducidas en la legislación penal española al delito de daños informáticos del art. 264.2 CP. El mismo reclama una acción de cualquier tipo que incida en los elementos electrónicos («datos, programas o documentos») contenidos en soportes electrónicos («redes, soportes o sistemas informáticos»). En definitiva la conducta debe afectar a los elementos electrónicos y no necesariamente a las redes, soportes o sistemas que los contienen.

---

privacidad o reserva de datos contenidos en sistemas informáticos. Esa preocupante laguna, que pueden aprovechar los llamados *hackers* ha aconsejado, cumpliendo con obligaciones específicas sobre la materia plasmadas en la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, incorporar al artículo 197 del Código Penal un nuevo apartado que castiga a quien por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático.

Señala González Rus[53] que «en sentido genérico, la expresión sabotaje informático alude tanto a la destrucción de sistemas informáticos completos como a la concreta de equipos y datos, programas y documentos electrónicos. En este sentido amplio, pues, el enunciado comprende muy diversas modalidades de ataque al *software* y al *hardware*, tanto si afectan a elementos físicos como lógicos, a sistemas informáticos completos o a componentes particulares de los mismos y tanto si provocan la destrucción, la inutilización o la simple perturbación de su funcionamiento. Dado que lo característico de los medios o procedimientos informáticos es que mediante ellos se llevan a cabo las funciones de almacenamiento, procesamiento o transmisión de la información, resultan más exactas las definiciones de sabotaje informático que comprenden únicamente las conductas que, cualquiera que sea el procedimiento a través del cual se produzcan, tienen por objeto preferente de ataque a los elementos lógicos de un sistema informático… Como consecuencia, en sentido propio debe entenderse por sabotaje informático la destrucción exclusiva de elementos lógicos, tanto si ello se hace mediante la destrucción de sistemas informáticos completos como mediante la específica de equipos y datos, programas y documentos electrónicos».

Algunas de las conductas previstas en la normativa comunitaria como en el Convenio de Cibercrimen pueden plantear dudas sobre su actual inclusión en el precepto mencionado del Código Penal español, singularmente la de obstaculización del funcionamiento de un sistema informático[54]. Los conocidos como ataques de denegación de servicio suponen no una destrucción material del sistema informático, ni necesariamente de sus componentes lógicos, pero sí una imposibilidad funcional de mayor o menor duración. Consiste en «saturar un sistema con peticiones de utilización de sus recursos hasta lograr el desbordamiento del mismo y su bloqueo. Ello impide a los usuarios obtener sus servicios o acceder a los datos que están registrados en el servidor»[55].

---

[53] «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona, coordinador). Comares, 2006, pp. 248-9.

[54] Así lo señala Morales Prats, F. «Los ilícitos en la red: pornografía infantil y ciberterrorismo». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona coordinador). Comares, 2006, p. 277.

[55] González Rus, J.J. «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes». *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (Romeo Casabona, coordinador). Comares, 2006, pp. 267-8. Este autor señala las principales formas de ataques Dds (denegación de servicio). «La más común es solicitar datos o información a un servidor

La posibilidad de castigo de esta conducta puede hacer resurgir la vieja polémica propia del delito de daños entre quienes consideran que el tipo penal requiere la lesión de la sustancia de la cosa y quienes entienden que sin lesión de la sustancia pero afectándose el valor de uso también existe conducta punible. Si se requiere necesariamente la lesión de la sustancia deberán verse alterados sustancialmente los componentes lógicos del sistema informático para poder apreciar una conducta delictiva. En este sentido González Rus reclama «la supresión definitiva de los datos, programas o documentos electrónicos, mediante la afectación de la sustancia de los mismos» para poder aplicar el tipo penal de daños. Para la otra opción alternativa bastaría con que el ataque al sistema informático produjera alteraciones significativas en su funcionamiento sin necesidad de destrucción o alteración grave de sus componentes lógicos.

Pese a las posibles cautelas sin embargo hace ya tiempo que el sistema penal español del delito de daños admitió —incluso para los objetos materiales— los supuestos no sólo de destrucción material del objeto sino de afectación de su valor de uso o funcionalidad y así se reconoce mayoritariamente[56]. La necesaria incidencia de la conducta sobre los elementos electrónicos (datos, programas o documentos) que reclama el tipo no impone una afectación material o sustancial de los mismos sino que resulta posible una incidencia sobre su funcionalidad. En todo caso la reforma propuesta del Código Penal no va dejar a dudas, si es que las hubiera en este momento. En el Proyecto de reforma del Código Penal de 15 de diciembre de 2006 y actualmente en tramitación en las Cortes Generales se incrimina en el nuevo art. 262 y de forma separada los ataques graves a los datos o programas informáticos y los ataques a los sistemas informáticos en el sentido de obstaculizar o interrumpiendo su funcionamiento. La redacción queda como sigue:

> «Se modifica el artículo 264, que queda redactado como sigue:
> 1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos o programas

sin aceptar posteriormente lo demandado, lo que provoca múltiples intentos de envío y acaba saturando las posibilidades del equipo. El efecto se multiplica cuando las peticiones se hacen desde muchos equipos y sesiones, para lo cual se hacen frecuentemente convocatorias masivas a través de *Chat* o grupos de noticias. Otro procedimiento también utilizado consiste en dirigir correos electrónicos con direcciones IP falsas a un servidor, que al intentar establecer la conexión y no conseguirlo, va bloqueándose. El bloqueo definitivo se produce cuando alcanza el límite de posibles conexiones que puede tener abiertas el sistema».

[56] Véase respecto a las acciones de sabotaje informático Mata y Martín, R.M. *Delincuencia informática y Derecho penal.* Edisofer, 2001, pp. 70 y ss.

> informáticos ajenos, será castigado, en consideración a la gravedad del hecho, con la pena de prisión de seis meses a dos años.
>
> 2. El que sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema de información ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, será castigado, atendiendo a la gravedad del hecho, con la pena de prisión de seis meses a tres años.
>
> 3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:
>
> 1.º Se hubiese cometido en el marco de una organización criminal.
>
> 2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.
>
> (…)
>
> 4. Cuando los delitos comprendidos en este artículo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en los apartados 1 y 2, y del tanto al décuplo en el supuesto del apartado 3.»

La exposición de motivos del Proyecto de reforma del Código Penal justifica la nueva redacción en una simplificación de la regulación y en el cumplimiento de las obligaciones dimanantes de la normativa comunitaria. «Valga decir que la reforma no ha hecho otra cosa que unir los actuales artículo 263 y 264, para facilitar la comprensión del sentido de unas normas que no tenían que estar separadas al tratarse siempre de la misma conducta variando en función de medios y de finalidades. En cambio, resultaba inadecuada la presencia de la destrucción de documentos, datos o programas contenidos en redes, soportes o sistemas informáticos, que reciben su propia regulación en el siguiente artículo 264, que se destina en exclusiva a las diferentes modalidades de ataques a los sistemas informáticos entre las cuales los antedichos daños son solo una posibilidad. Con esa especialización de los daños se completa el cumplimiento de la ya mencionada DM 2005/222/JAI sobre ataques contra los sistemas de información».

De momento los análisis más serios indican que la alarma creada frente a este posible tipo de ataques resulta desmesurada pues en realidad todavía no se tiene constancia de algún hecho de este tipo exitoso para una organización terrorista. Pero al mismo tiempo se advierte sobre

el riesgo de subestimar la amenaza que mediante el empleo del ciberespacio representan las organizaciones terroristas, de manera que resulta obligado integrar este tipo de riesgos en las estrategias de seguridad[57], pues se tiene la seguridad de que tarde o temprano se tratarán de utilizar también estos medios[58].

b) Un aspecto fundamental que aporta la existencia de Internet a los grupos terroristas es una herramienta básica para la transmisión de información. En este nuevo contexto tecnológico la transmisión de información por estos medios permite una gran rapidez y dificultades considerables para ser detectada. La complejidad para advertir este tipo de comunicaciones por parte de los grupos terroristas puede ir en aumento cuando se utilizan técnicas de encriptación o mediante mensajes asociados a fotografía[59] otros elementos neutrales[60], teniendo en cuenta que los sistemas de cifrado anteriormente de difícil acceso en la actualidad pueden ser accesible en Internet[61]. La versatilidad de las Nuevas Tecnologías abre grandes posibilidades pues puede ser enviada todo tipo de informaciones, como órdenes de ejecución, documentación preparatoria como planos, fotografías, videos, textos etc.[62].

---

[57] Cfr. Conseil de l´Europe. *Criminalité organisée en Europe. La menace de la cybercriminalité.* 2006, p. 182. También en el mismo sentido el Segundo informe sobre el uso de Internet por los terroristas realizado por el *United Status Institute of Peace*. http://www.francispisani.net/2004/05/la_paradoja_del.html.

[58] Cfr. la información sobre el Segundo informe sobre el uso de Internet por los terroristas realizado por el *United States Institute of Peace*. http://www.francispisani.net/2004/05/la_paradoja_del.html

Según el informe Weimann tres serían las razones por las cuales todavía no se han producido este tipo de ataques terroristas. En primer lugar porque las instalaciones estratégicas no son accesibles mediante Internet. En segundo lugar porque hacen falta conocimientos muy especializados para poder provocar efectos a gran escala que se calcula tan solo un 1% de los *hackers* contaría con ellos. En tercer lugar porque se necesita invertir mucho tiempo y dinero en el intento. Se estima necesario cinco años de preparación y 200 millones de dólares en cifras del año 2001. Después de los atentados del 11 de septiembre la CIA en un informe enviado al Comité de Inteligencia del Senado de los EEUU advertía de las dificultades para llevar a cabo ataques de «ciberguerra» por los grupos terroristas pero al tiempo que estos «tienen el deseo y la intención de desarrollar la destreza necesaria para llevar a cabo un ciberataque efectivo».

[59] Señala Orta Martínez que existe una hipótesis de que los ataques a las torres gemelas del 11 de septiembre de 2001, fueron posibles al envío y recepción de mensajes embebido en imágenes digitales, a través del método de cifrado u ocultamiento conocidos como esteganografía digital. «CiberTerrorismo», *Alfa-redi, Revista de Derecho Informático* n.º 82, mayo de 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=949.

[60] Conseil de l´Europe. *Criminalité organisée en Euroepe. La menace de la cybercriminalité*. 2006, p. 186.

[61] Cfr. Cosido Gutiérrez, l. «Los riesgos cibernéticos». *CGC* 25/2001, p. 4.

[62] Cfr. Cosido Gutiérrez, l. «Los riesgos cibernéticos». *CGC* 25/2001, p. 4.

Además cabe señalar que la actual evolución organizativa de los grupos terroristas incrementa también la importancia de este tipo de comunicaciones. Como es sabido desde hace un tiempo este tipo de organizaciones han pasado de organigramas generales de gran magnitud en las que el descubrimiento de una parte podría poner en riesgo al conjunto a redes y estructuras celulares con un mayor aislamiento que evita que el resto de la organización pueda verse afectada por la detección de una parte de la organización[63]. Por eso las comunicaciones electrónicas no vinculables a un determinado espacio físico permiten una mayor seguridad y un mayor aislamiento de las partes de la organización. Estos canales sin definición física resultan de más difícil aprehensión y más adecuados al nuevo tipo de organización celular.

También permiten las tecnologías del conocimiento y la información una enorme publicitación y expansión de su ideología. En Internet la creación de sitios *web* se muestra como un instrumento sencillo, poco costoso y muy adecuado para difundir su propaganda, teniendo en cuenta que siempre se ha considerado la guerra psicológica como uno de los principales elementos del terrorismo. Se estima que los cómplices de Bin Laden han dispuesto de al menos cincuenta sitios *web* que pueden ser instrumentalizados con rapidez para expandir sus motivaciones, justificar sus acciones y aplaudir sus atentados, cambiando con frecuencia la ubicación y dirección de la página *web* lo que complica la localización e interrupción —en su caso— de las mismas[64]. Hecha la difusión de sus grupos y acciones en un ambiente de romanticismo y victimismo es posible alentar a la incorporación de quienes se sienten atraídos. De manera que también se produce el empleo de estos medios como canal de reclutamiento de nuevos miembros de las organizaciones armadas.

Una de las preocupaciones fundamentales de las autoridades nacionales e internacionales en materia de terrorismo es la de detectar y

---

[63] Cfr. Bovenkerk, F./Chakra, B.A. «Terrorismo y delincuencia organizada». *Foro sobre el delito y sociedad* 1,2, 2004, p. 7.

[64] Conseil de l´Europe. C*riminalité organisée en Europe. La menace de la cybercriminalité*. 2006, pp. 183-4. Orta Martínez indica que la propaganda de los grupos catalogados como terroristas se ha hecho común en Internet. El Ejercito de Liberación Nacional colombiano (ELN), las FARC, Sendero luminoso, ETA, el Hezbollah, el Ejercito Zapatista de Liberación Nacional de México y hasta el Ku Klux Klan tienen presencia en la *Web* lo cual hace evidente la utilización de tecnología por parte de estos grupos. «CiberTerrorismo». *Alfa-redi, Revista de Derecho Informático,* n.º 82, mayo de 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=949. Luciano Salellas muestra algunos ejemplos de los sitios *web* correspondientes a las organizaciones terroristas como medio de difusión y enaltecimiento de sus propios grupos. «Delitos informáticos. Ciberterrorismo». http://www.Ilustrados.com/publicaciones/EEypVEluF1VYPABJae.php, p. 7.

cegar las fuentes de financiación de las organizaciones criminales pues de este modo se puede estrangular sus actuaciones. Precisamente el desarrollo tecnológico permite también a estas organizaciones la búsqueda de nuevos métodos de financiación que les permite continuar su espiral criminal e incluso abrir nuevos campos o incrementar su actividad[65]. Por una parte permiten abrir la solicitud de colaboración económica a un número muy superior de personas y asociaciones mediante donaciones directas o a través de fundaciones o asociaciones dependientes de la organización.

Pero ahora también se pueden valer de los medios tecnológicos para realizar operaciones transnacionales mediante complejas transacciones internacionales. Estas permiten tanto facilitar el pago por la adquisición de materiales y equipos utilizados en su actividad criminal y también como medio de blanqueo de cantidades de dinero que proceden de actividades ilegales y que luego pueden ser aplicados a las actividades terroristas[66]. En definitiva las Nuevas Tecnologías dotan de nuevos recursos y mecanismos mediante los cuales lograr una adecuada acumulación de capital que permita el funcionamiento del grupo armado.

---

[65] Una nueva fórmula de financiación aprovechando precisamente las Nuevas Tecnología es la extorsión informática, pues los Ciberterroristas están realizando extorsión a grupos financieros para recaudar fondos a cambio de no ser ciber atacados, por lo que aquellos que realizan estos pagos bajo amenazas están cancelando vacunas, para no ser atacadas informáticamente o bien para no revelar datos de clientes. Orta Martínez, R. «CiberTerrorismo». *Alfa-redi, Revista de Derecho Informático,* n.º 82, mayo de 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=949.

[66] Cfr. Cosido Gutiérrez, I. «Los riesgos cibernéticos». *CGC,* 25/2001, p. 5. También Campón Domínguez, J.A. «El blanqueo de capitales y la financiación del terrorismo como amenazas de seguridad». *CGC,* 30/2004, pp. 128-9.

Algunas cuestiones acerca de la estafa informática y uso de tarjetas (Incidencia del Anteproyecto de 2006 de reforma del Código penal)

Jaime Moreno Verdejo
Fiscal del Tribunal Supremo

In Memoriam

Me habría gustado no tener que empezar así, no tener que escribir estas líneas, pero mis primeras palabras han de ser en recuerdo de José María Lidón. La tristeza hace difícil comenzar pronunciando su nombre. Sus profundos conocimientos jurídicos que le convirtieron en un excelente Magistrado, sus enormes valores e integridad que hicieron de él un hombre de bien, en fin, toda su persona inspira y dota de sentido a estas Jornadas.

El asesinato de José María nos impone un ineludible deber de firmeza en la defensa de los valores constitucionales por los que dio la vida. A recordarle, a tributarle un periódico y merecido homenaje, se orientan estas IV Jornadas.

Por ello, cuando recibí la amable invitación de Carmen Adán sentí un profundo orgullo ante lo que entendí como una magnífica ocasión. Son muy pocas las veces que he tenido una sensación tan intensa sobre la oportunidad y el honor de acudir a una cita.

Gracias a los dos codirectores, Carmen Adán y Norberto de la Mata, y mi agradecimiento también a cuantas personas desde la Dirección de Relaciones con la Administración de Justicia, la Fiscalía y la Judicatura, han hecho posible estas Jornadas.

I. Introducción

El Código Penal aprobado en 1995 llevó a cabo un importante esfuerzo por contener previsiones que dieran respuesta a las múltiples y variadas manifestaciones que se engloban bajo la denominación de *delincuencia informática*. Los arts. 197 sobre descubrimiento de secretos,

248.2 que regula la estafa informática, 264 sobre daños, 270 sobre protección de propiedad intelectual, entre otros, son buena muestra de la preocupación del Código por atajar diversas fórmulas delictivas de esta naturaleza.

En todo caso, al reparar en el tratamiento jurídico de determinadas manifestaciones delictivas relacionadas con la informática, se deja sentir la presencia de dos mundos que caminan a muy distinta velocidad. Un año sería un plazo muy corto para la elaboración, modificación o valoración de una norma jurídica. En ese espacio de tiempo, por el contrario, la evolución tecnológica deja obsoletos los más modernos sistemas. Las formas de comisión delictiva y los vericuetos que recorren las manifestaciones fraudulentas, yendo siempre por delante de cualquier inicial previsión, pueden mutar varias veces en ese período.

El objeto del presente trabajo es incidir en algunos problemas que de ordinario se presentan en la práctica judicial al aplicar el tipo penal de la estafa informática[1]. Ya avanzo que no pretendo abordar un estudio sistemático y completo del tipo penal[2] —para lo que tampoco me siento capacitado, dicho sea de paso— sino analizar algunas cuestiones puntuales y prácticas sobre determinados aspectos que se suscitan generalmente a la hora de su aplicación. Las importantes novedades que se presentan en el Anteproyecto de 2006 de reforma del CP justifican asimismo las referencias al mismo.

Junto a la definición tradicional de estafa (art. 248.1), el legislador incluyó en 1995 como esencial novedad la modalidad de estafa informática (art. 248.2). Dispone el art. 248 CP:

> «1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
>
> 2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero».

Por LO 15/2003 se adicionó un apartado 3 al art. 248 que dispone:

---

[1] Este trabajo actualiza y amplia el publicado conjuntamente con Teresa Ruano Mochales bajo el título «Uso fraudulento de tarjeta de crédito: dimensión jurídico penal y la cuestión de la responsabilidad civil». *Revista Jurídica Sepin Penal*, n.º 2, marzo-abril 2003.

[2] Un completo estudio de esta modalidad de estafa puede verse en Galán Muñoz, A., *El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 CP.* Ed. Tirant lo blanch, Valencia, 2005.

> «3. La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo».

Pese a los casi diez años transcurridos desde la vigencia de la estafa informática siguen siendo muchas las dudas interpretativas que los elementos del tipo presentan y no pocas por ello las divergencias doctrinales.

Sin embargo, su aplicación en la praxis no se ha producido, en mi opinión, en la enorme medida en que se preveía al momento de su nacimiento. En estos años de vigencia del art. 248.2, pese a la creciente utilización del dinero de plástico y el aumento del uso de la informática, el número de sentencias dictadas por este delito y la complejidad de los supuestos de hecho sometidos a la Administración de Justicia han quedado muy por debajo de las iniciales expectativas. Se ha visto fundamentalmente limitada a supuestos de empleo de tarjetas de crédito y a operaciones bancarias *on-line*.

II. **La tipificación de la estafa informática: una necesidad sentida en la práctica (STS de 19 de abril de 1991)**

El caso que enjuició el Tribunal Supremo en esta sentencia[3] (Ponente: Soto Nieto) se basaba en los siguientes hechos probados: J.V. apoderado de una sucursal del Banco Hispano Americano, en varias ocasiones anteriores a julio de 1985, manipulando las cuentas corrientes de diversos clientes, haciendo apuntes contables por vía de ordenador, consiguió incorporar a su peculio una suma cercana a los 4 millones de ptas., procedentes de diferentes clientes.

La AP le condenó como autor de un delito continuado de estafa y otro de falsedad en documento mercantil a penas de 1 año y 5 meses de prisión y multa.

La Defensa de J.V. recurrió alegando que era improcedente la calificación de estafa.

El TS estimó el recurso, partiendo para ello de que el engaño, como elemento nuclear de la estafa, ha de ser bastante y producir un error esencial en el sujeto pasivo que le mueva a la realización del acto de disposición. Tomando en consideración el elemento engaño señala la

---

[3] Un estudio de esta sentencia se lleva a cabo por Moner Muñoz, E., «Las defraudaciones». *Jornadas sobre las novedades del CP en materia de delitos contra la propiedad, Estudios Jurídicos del Ministerio Fiscal,* Madrid, 1997, pp. 433 y ss.

sentencia que «mal puede concluirse la perpetración de un delito de estafa por parte del procesado, al impedirlo la concepción legal y jurisprudencial del engaño, ardid que se produce e incide por y sobre personas (…) la inducción a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina (…) a las máquinas no se les puede engañar, a los ordenadores tampoco, por lo que los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce el engaño ni el error necesarios para el delito de estafa».

El TS absolvió consecuentemente de estafa, pero como quiera que la tesis de la Defensa en la instancia había sido la de la absolución y alternativamente la de apropiación indebida, condenó por éste delito —manteniendo igual la pena— al entender que «existió auténtica disposición por parte del acusado, quien ostentaba la condición de apoderado de los fondos que le fueron entregados para su administración (…) el inculpado se apropió de dinero que tenía a su alcance por razón de su condición de apoderado de la entidad bancaria y en cuya administración tenía intervención directa».

La salida incriminatoria dada en esta sentencia por el TS suscita de inmediato un interrogante. ¿Y si la conducta hubiera sido llevada a cabo por un tercero ajeno al Banco que, en definitiva, no tuviera la previa posesión o disponibilidad de los bienes? Rechazada también en esta hipótesis la apropiación indebida, la conducta habría de incriminarse por hurto o considerarse atípica.

La calificación como hurto a la entidad bancaria, solución por la que, en último extremo, nos decantamos, suscitaría sin embargo bastantes dificultades: no se «toman» bienes sino que se provoca un «acto de disposición» del Banco en favor del sujeto activo o incluso de un tercero, lo cual queda reflejado en la contabilidad de la entidad bancaria. ¿No se está forzando el tipo del hurto cuando es el propio sujeto pasivo quien entrega la cosa, por ejemplo, a la cuenta de un tercero que al recibir la transferencia puede quedar confiado en haber recibido un pago o una donación del sujeto activo, y constando en contabilidad la operación?

De otra parte, en la calificación de estafa y apropiación indebida las dos citadas sentencias estimaron perjudicado al Banco. Pero las dudas en caso de reputar hurto aún pueden extenderse más: el hurtado ha sido el Banco —como entendemos[4]— o cada uno de los clientes afectados.

[4] Pese a la inexistencia de un precepto similar al art. 156 de la Ley Cambiaria y del Cheque de 16 de julio de 1985.

Este supuesto es paradigmático de la necesidad sentida por el legislador y llevada a cabo en el Código Penal de 1995 de ampliar el concepto de estafa a aquellos supuestos en los que fraudulentamente se logra de un sistema informático la realización de un acto de disposición patrimonial a favor propio o de tercero[5].

III. **Cuestiones de jurisdicción y competencia**

El carácter transnacional de estos comportamientos delictivos se deduce de la facilidad que para el autor supone operar vía Internet. El ciberespacio provoca una relativización de los parámetros espaciotemporales característicos del mundo físico. Las fronteras penales se resienten ante la facilidad de su traspaso mediante la Red. En materia de estafa informática desde el territorio de un primer país el sujeto activo de este delito puede incidir en activos situados en un segundo país y colocarlos, a su vez, en un tercer sitio, dando lugar no sólo a problemas de identificación del autor sino de jurisdicción de los Tribunales nacionales.

Tales problemas de jurisdicción internacional pasarán a ser meramente de competencia territorial cuando la actividad y el resultado se produzcan en diferentes lugares de un mismo país.

De acuerdo con el principio de universalidad (art. 23.4 LOPJ) España podría perseguir conductas ilícitas sin tener en cuenta la nacionalidad del autor ni el lugar de comisión del hecho delictivo cuando se trate

---

[5] La sentencia que hemos tratado guarda estrecha relación con el supuesto abordado por la STS 661/2005, de 23 de mayo. Dicha sentencia analiza el caso del asesor contable que con la confianza de los socios instala el servicio integral de banca telefónica que ofrecía Banesto. Conocidas por él las claves del programa citado, que le fueron entregadas por los socios, así como las de otros servicios bancarios de la misma entidad, denominada «Bknet» y Bktel», que tenía la empresa contratados, empezó a realizar transferencias bancarias desde las citadas cuentas de Fino y Gómez S.L. a otras que tenía abiertas a su nombre por total de 69.093.636 pesetas por medio de 230 transferencias durante varios años hasta que fue descubierto.

La sentencia casa la recurrida por falta de motivación y absuelve al penado. Señala en concreto que «la sentencia recurrida expone una serie de consideraciones jurídicas genéricas sin fundamentar la subsunción del caso concreto y, sobre todo, *sin razonar en qué consiste, en este supuesto de hecho, la manipulación informática o el artificio semejante utilizado por el recurrente. Es preciso tener en cuenta que la realización de disposiciones de dinero no autorizadas no configura por sí misma todavía el delito del art. 248.2 CP. En efecto, en todo caso, parece que, sin especificar el artificio informático —del que nada dice el Tribunal a quo— la responsabilidad del acusado sólo podría haberse fundamentado en el art. 252 CP., que no fue alegado ni por el Fiscal ni por la Acusación Particular*…».

de genocidio, terrorismo, piratería y apoderamiento de aeronaves, falsificación de moneda, prostitución y corrupción de menores y tráfico de drogas. El catálogo de delitos acogibles al principio de universalidad para su persecución extraterritorial, está integrado por una relación de delitos definidos como tales para la protección de bienes jurídicos de primerísimo orden.

El problema, como ha señalado Marchena[6], se plantea por cuanto referirse a delitos que utilizan la Red como instrumento ejecutivo, supone poner el acento en el formato, más que en el bien jurídico cuya defensa se trata de garantizar. La ordenación de delitos sometidos al principio de universalidad presupone un catálogo de bienes jurídicos cuya propia naturaleza impone esa persecución reforzada. Desde este punto de vista, parece claro que no toda ofensa a cualquier bien jurídico, ejecutada aquélla mediante tecnología telemática, podría justificar el acogimiento de un criterio de justicia universal. De ahí que la reformulación del principio de universalidad a partir de un criterio puramente instrumental, supondría un verdadero peligro para la coherencia del sistema de delimitación jurisdiccional. La fijación de los límites jurisdiccionales de un Estado no puede inspirarse en pautas puramente formales, ligadas al *modus operandi* del autor del delito, sino que exige una atención ponderativa centrada en el bien jurídico afectable por el delito.

Ahora bien, es claro que, sin recurrir al principio de universalidad en su persecución, son muchas las causas que suponen un claro interés supranacional en dificultar la utilización de la red con fines puramente delictivos.

1. *El principio de ubicuidad como solución facilitadora*

El delito de estafa[7] no se comprende entre los delitos recogidos en los apartados 3 y 4 del art. 23 de la LOPJ. Por ello, para su persecución por los Tribunales españoles será preciso que el delito 1) se haya cometido en territorio español o a bordo de buques o aeronaves españolas por cualquiera o 2) en el extranjero por españoles o extranjeros que tras el delito hayan adquirido la nacionalidad española y concurran los tres requisitos del apartado 2 del art. 23 citado (a saber, que el hecho sea punible en el lugar de ejecución; que el agraviado o Fiscal accionen ante

[6] Marchena Gómez, M., «Algunos aspectos procesales de Internet». Ponencia presentada a los Cursos de Formación del CGPJ.

[7] Sí lo está la falsificación de moneda y su expedición, lo que abarcará los casos de clonado y falsificación de tarjetas de crédito.

la justicia española; y que el autor no haya sido absuelto, indultado o penado en el extranjero y cumplida por entero la condena).

El primero de los requisitos —que el hecho sea punible en el lugar de la ejecución— suscita, como señala Galán Muñoz[8], el problema de la inexistencia de una uniformidad o proximidad en la delimitación nacional de cada una de las conductas típicas de los delitos informáticos, lo que se ha venido en denominar *paraísos para los delitos informáticos*, es decir, territorios desde los cuáles se podrían ejecutar algunas de tales conductas sin temor a recibir sanción penal alguna puesto que los ordenamientos penales vigentes de tales lugares, al no haber sido adaptados, no las preverían como típicas.

Por tanto, interesa determinar cuándo estos delitos se entienden cometidos en territorio nacional.

El art. 7 CP acude para determinar la *ley penal en el tiempo*, es decir, para fijar el momento en el que se ha de entender cometido el delito, al criterio de la actividad, que viene representado por el momento en que se despliega la acción u omisión delictiva con independencia del ulterior de su resultado. Ahora bien, este criterio no es extrapolable al problema que nos ocupa. El TS, en sentencias 143/1999, 21 de diciembre —*caso Roldán*—, 933/1998, 16 de octubre y 1030/1998, 22 de septiembre, ya se ha pronunciado a favor de una interpretación restrictiva del mandato del art. 7 del Código Penal, limitado a la determinación de la ley penal aplicable desde el punto de vista de la aplicación temporal de la norma penal.

Nada dice el CP acerca de la determinación de la ley penal en el espacio. En estos casos, cuando los actos de ejecución y el resultado se cometen en diferentes países es posible acudir a las tres clásicas teorías: actividad, resultado y ubicuidad.

La teoría del resultado (en lo que se refiere a la estafa los fondos de los que se ha dispuesto se hallan en España y el sujeto ha operado desde el extranjero) suscita el problema de la necesidad de extradición del sujeto.

La teoría de la actividad (el sujeto actúa desde España respecto de fondos situados en otro país) suscita el problema de que el conocimiento del perjuicio y la investigación se inician en otro lugar.

La evolución jurisprudencial en esta materia puede resumirse de la manera siguiente: el TS desde la aceptación inicial de la teoría del resultado se ha inclinado de forma progresiva y clara en favor de la teoría de la ubicuidad.

---

[8] *Op. cit.*, p. 42.

El TS adoptó como criterio de aplicación general la teoría del resultado en las sentencias 18 de septiembre de 1925, 7 de abril de 1926 y 5 de mayo de 1975.

Sin embargo, se produce un cambio de orientación a favor de la teoría de la ubicuidad en las siguientes resoluciones:

Quizá la primera muestra de la aplicación de ese criterio sea el ATS de 12-3-1996 (rec. núm. 3240/1995), en el que se trataba de discernir el lugar de comisión en un delito continuado de estafa mediante el uso abusivo de una tarjeta de crédito a sabiendas de que estaba anulada. El TS admitió la competencia de los Tribunales españoles para conocer de todas las utilizaciones de la tarjeta falsa en peajes de autopista a cargo de una cuenta radicada en un banco en España, admitiendo que cabía conocer no sólo del uso de la tarjeta en peajes españoles sino también del uso en peajes sitos en el sur de Francia. Razona el TS que «…conforme a la teoría de la ubicuidad tanto debe aceptarse el lugar de la manifestación de la voluntad como aquel en el que se produce el resultado. En el presente caso el perjuicio acaece en España…».

El ATS de 3-2-1997 (rec. núm. 960/1996), en el que puede leerse:

> «… La cuestión del lugar de comisión del delito se debe resolver, según lo vienen reiterando diversos precedentes de esta Sala, de acuerdo con la llamada teoría de la ubicuidad, ampliamente mayoritaria en los derechos vigentes de los Estados miembros de la Unión Europea y postulada también por la teoría entre nosotros. Según ésta, los hechos se deben tener por cometidos en todos los lugares en los que se ha desarrollado la acción, así como en los que ha tenido lugar el resultado. Cuando se trata de omisiones el lugar de comisión debe ser aquel en el que debió haber ejecutado la acción omitida».

La relación de conexidad vuelve a ser determinante para la afirmación jurisdiccional en el ATS de 20-2-1992 (rec. núm. 990/1991), con arreglo al cual la circunstancia de que el delito falsario se hubiera cometido en Luxemburgo, concebido aquél como medio para la comisión de una estafa que despliega sus efectos en España, permite sostener que en nuestro territorio fue ejecutado el propósito delictivo y en él puede ser enjuiciado. Insisten en la idea expuesta, los ATS de 20-3-1992 y de 15-11-1990.

Al margen de los distintos autos recaídos en la resolución de cuestiones de competencia, el TS ha tenido ocasión de consagrar el renovado criterio a favor de la ubicuidad en las sentencias 187/1993, 20 de julio, 10 y 25 de noviembre de 1992 (ésta última recaída en el rec. núm. 2168/1990), autorizando una conclusión con arreglo a la cual la tesis de la ubicuidad como criterio de delimitación jurisdiccional puede entenderse como de aceptación jurisprudencial pacífica.

En dicha evolución jurisprudencial se ha producido un hecho de enorme importancia: en fecha 3 de febrero de 2005 el Pleno no jurisdiccional del Tribunal Supremo ha facilitado enormemente la resolución de las cuestiones de competencia territorial al establecer como Acuerdo que «El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa».

Se sienta así definitivamente el *principio de ubicuidad* como criterio enormemente facilitador de la resolución de estos problemas[9].

Cualquier órgano jurisdiccional en cuyo partido se haya llevado a cabo alguno de los actos de ejecución del delito será competente y, entre todos ellos, se atenderá a aquél que primero comenzare la instrucción de la causa. No obstante, esta última regla se ve muy modulada en la praxis. Es decir, sentado que cualquiera será competente en la medida en que en su partido se hayan desplegado actos de ejecución, el Tribunal Supremo no sólo ha manejado criterios cronológicos para resolver entre todos los posibles el órgano competente, sino que ha acudido a otros criterios que, en definitiva, vienen inspirados por la facilidad para la instrucción del delito.

El principio de ubicuidad es válido tanto para determinar el lugar de comisión delictiva tanto a efectos de decidir entre jurisdiccionales nacionales cuanto entre juzgados nacionales de diferentes territorios.

2. *Los llamados «lugares de tránsito»*

Como ha señalado Marchena[10], no debe olvidarse que entre el lugar de la acción y el lugar del resultado pueden existir idas y venidas que afecten a los límites jurisdiccionales de otros Estados. La ubicación de los

---

[9] En ejemplo que señala Marchena, *op. cit*., la teoría de la ubicuidad permitirá entender que la inoculación de un potente virus destructivo mediante el correo electrónico, llevada a cabo desde fuera de España por un no nacional, pero que expande sus nocivos efectos en sistemas informáticos radicados en territorio español, puede ser perseguida en nuestro país, en la medida en que el delito, atendiendo al resultado, también puede reputarse cometido en España. Esa conclusión estaría vedada si entendiéramos aplicable la teoría de la actividad, pues el delito, en la medida en que la acción se habría desarrollado por un extranjero, fuera de nuestro territorio y el delito de daños no se halla en el catálogo de figuras delictivas del art. 23 de la LOPJ, no se entendería cometido en los límites jurisdiccionales españoles.

[10] Marchena Gómez, M., «Algunos aspectos procesales de Internet». Ponencia presentada a los Cursos de Formación del CGPJ.

nodos conlleva como efecto ciertos *saltos territoriales* que podrían plantear la duda acerca de si en cualquiera de los Estados en que se sitúa uno de aquellos, podría también estimarse cometido el delito. No cabe duda de que en esos terceros lugares radica una prueba del delito.

No parece, sin embargo —sigue señalando este autor— que la respuesta positiva encuentre fundado apoyo. El recorrido telemático a través del cual discurre el sofisticado medio ejecutivo, no puede aspirar a definir una pretensión de jurisdiccionalidad. Sólo el lugar en el que se despliega la acción y el lugar en el que se ejecuta el resultado pueden aportar los elementos necesarios para su ponderación. La irrelevancia jurídica de esa ruta telemática a los efectos de afirmar o negar la propia jurisdicción, parece consecuencia obligada de la ausencia de bien jurídico ofendido en los llamados «lugares de tránsito».

Nuestro sistema jurídico ofrece algún ejemplo concreto en el que esa irrelevancia tiene acogida normativa. Es el caso de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuyo art. 4.1.c), al definir el ámbito aplicativo de los respectivos instrumentos jurídicos nacionales, excluye aquellos casos en que los medios automatizados se hallen situados en territorio de algún Estado miembro a los exclusivos fines de tránsito[11]. Este criterio, como no podía ser de otra manera, ha sido incorporado a la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (art.2.1.c)[12].

En el ámbito de la Unión Europea, la Posición Común adoptada por el Consejo de la Unión con fecha 27 de mayo de 1999, relativa las negociaciones del proyecto de Convenio sobre delincuencia en el ciberespacio, celebradas en el Consejo de Europa expresó el compromiso de los Estados miembros de apoyar la inclusión en el Convenio de «…disposiciones que faciliten una investigación y persecución eficaces de los delitos penales relacionados con sistemas y datos informáticos (…)». La Comisión concluye destacando el compromiso de garantizar que se establezca una jurisdicción pertinente para los delitos previstos en el citado Convenio, reformando las disposiciones relativas a la cooperación y asistencia judicial, estudiando la posibilidad de «… una búsqueda informática transfronteriza, a efectos de un delito penal grave»[13].

---

[11] *Diario Oficial* núm. L 281, 23 de noviembre 1995, pp. 31-50.

[12] BOE núm. 298/1999, 14 de diciembre.

[13] *Diario Oficial* L-142, 5 junio 1999, pp. 1 y 2. CELEX http://europa.eu.int/celex/celex_es.htm.

El Convenio sobre Cibercriminalidad de fecha 23 de noviembre de 2001[14] se adopta por los Estados miembros del Consejo de Europa preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer infracciones penales. Merecen destacarse ahora las siguientes previsiones del Convenio:

> Artículo 22.—Competencia
>
> 1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículo 2 a 11 del presente Convenio, cuando la infracción se haya cometido:
>
> a) en su territorio;
>
> b) a bordo de una nave que ondee pabellón de ese Estado;
>
> c) a bordo de una aeronave inmatriculada en ese Estado;
>
> d) por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.
>
> 2. (…)
>
> 3. Las Partes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.
>
> 4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.
>
> 5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.
>
> Artículo 23.—Principios generales relativos a la cooperación internacional
>
> Las Partes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar

[14] En vigor desde el 1 de julio de 2004, si bien ratificado sólo por 11 Estados, entre los cuales no se encuentra España. Un análisis de algunas de las cuestiones procesales que suscita puede verse en González López, J. J., «La respuesta procesal a la delincuencia informática: especial atención al Convenio sobre el Cibercrimen». www.noticiasjurídicas.com.

los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

Artículo 25.—Principios generales relativos a la colaboración

1. Las Partes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. (…).

3. Las Partes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

3. *Determinación competencial en casos de transferencias bancarias entre diferentes puntos geográficos*

La estafa informática puede suponer la transferencia de activos desde una cuenta a otra radicada en diferente territorio. Se suscita entonces una cuestión de competencia que no es diferente de la que puede darse en la estafa común cuando el perjudicado transfiere por sí desde su cuenta dinero a la cuenta del estafador radicada en otro lugar. En la estafa común o en la informática la actuación del sujeto activo (manipulando el sistema o convenciendo al perjudicado para que efectúe la transmisión) han podido tener lugar en un sitio distinto del de cualquiera de ambas cuentas.

La jurisprudencia viene ofreciendo soluciones diferentes.

Así, no faltan pronunciamientos (AATS 27 de junio de 1991, 26 de mayo y 23 de junio de 2000 y 20 de noviembre de 2001; también Auto del TSJ de Andalucía de fecha 30 de julio de 2002) que permiten sostener que los hechos se han cometido en el lugar donde radica el banco del estafado, lugar en el que se realiza el acto de disposición patrimonial consistente en la transferencia patrimonial con destino a la cuenta corriente indicada por el imputado.

Y tampoco faltan pronunciamientos jurisprudenciales que apoyan la tesis contraria según la cual el delito se consuma (AATS de 4 de febrero de 1981, 18 de julio de 1987, 26 de octubre de 1987, 15 de abril de 1988, 6 de febrero de 1991 y, especialmente importante, el de 28 de

abril de 2003) en el lugar en el que el sujeto activo tiene la disponibilidad de los efectos del delito, lo que implica señalar como competente al Juzgado del lugar donde habían sido transferidos o de destino final de los fondos.

Recientemente, tras la adopción del Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo antes citado de 3 de febrero de 2005, las discrepancias siguen presentes.

El ATS de 10-12-2004 se inclina por estimar competente el Juzgado en el que se halla la cuenta corriente del sujeto activo del delito en la que se recibe dicho dinero, solución que no obstante —advierte— se puede ver modulada en cada caso, en aras de facilitar la instrucción delictiva, en atención al antes citado principio de ubicuidad.

Por el contrario, el ATS de 31-3-2006 (rec. núm. 177/2005) resolvió en sentido contrario la cuestión suscitada entre Madrid, donde desde una terminal informática se llevaron a cabo las operaciones bancarias fraudulentas, y Valladolid, lugar donde radicaba la cuenta corriente de la denunciante en la que se cargaron los actos de disposición patrimonial ordenados desde Madrid (no menciona siquiera la resolución cuál es el lugar de destino de los fondos transferidos desde Valladolid). El TS estimó en base al principio de ubicuidad que procede resolver la presente cuestión de competencia a favor del Juzgado de Instrucción de Valladolid que comenzó en primer lugar la investigación de los hechos, y donde radicaba la cuenta corriente de la denunciante a cuyo cargo se hicieron, desde Madrid, los fraudulentos actos de disposición patrimonial.

IV. **Un problema enquistado. Uso indebido de tarjeta en cajeros automáticos: ¿robo con fuerza o estafa informática?**

1. *Planteamiento de la cuestión*

La extracción de dinero de cajeros automáticos mediante la utilización de tarjetas ajenas, obtenidas mediante sustracción y uso indebido del número PIN o clonadas (caso este en que se añadiría la falsificación de moneda *ex* art. 386), suscita de antiguo la polémica acerca de su tipificación.

Las dificultades para su encaje en una y otra figura han llevado a algún autor[15] a sostener la conveniencia de un tipo penal específico para

[15] Mata y Martín, R.M., «Los nuevos sistemas de seguridad desde la perspectiva del robo con fuerza en las cosas. Tratamiento en el proyecto de CP de 1994», en *Estudios jurídicos en memoria del profesor Dr. D. José Casabó Ruíz*. Vol. II, Valencia, 1997.

estas conductas. El Anteproyecto de reforma del CP de 2006 —al que se aludirá en un apartado específico— ha optado por la inclusión de ese tipo especial en sede de estafas.

Ya adelanto que a mi juicio la conducta debe ser reputada estafa informática y no robo con fuerza. Pero, en cualquier caso, desde un punto de vista práctico, y con carácter previo a las consideraciones sobre los argumentos a favor de una u otra tesis, debo señalar lo siguiente:

—cuando las AAPP condenan ya por robo, ya por estafa, el penado suele combatir en casación esa calificación con los argumentos de quienes sostienen que se trata del otro delito;
—los recurrentes sostienen que se condenó por estafa y no por robo, o viceversa, y que al ser delitos no homogéneos, y al no haberse acusado por el tipo correcto procede la absolución, que dicen impuesta por el principio acusatorio;
—algunos recurrentes van en su argumentación más lejos cuando la condena fue por el tipo básico de estafa. Señalan que el tipo básico de robo con fuerza es hoy —tras la reforma operada por LO 15/2003— más grave que la estafa. Aquel tiene pena de 1 a 3 años (art. 240) y la estafa de 6 meses a 3 años (art. 249), por lo que siendo su «suelo» de menor gravedad y siendo el «techo» punitivo idéntico ha de reputarse más grave el robo. Por ello, sostienen que aunque se estimasen homogéneos no cabe variar el título de condena a un delito más grave sin que se haya abierto la puerta mediante la tesis y se haya acogido por alguna acusación.

Al menos ya me he encontrado en dos ocasiones con este tipo de planteamiento por el recurrente ante la condena por estafa de la AP (caso de uso de tarjeta ajena en cajero). En el primer caso (STS 185/2006, de 24 de febrero) la Sala apreció el recurso por otro motivo: presunción de inocencia. En el segundo (recurso n.º 2/11142/2006) está pendiente de ser dictada la sentencia.

Lo expuesto pone de relieve la conveniencia de que los Fiscales califiquemos estas conductas de forma alternativa para evitar situaciones como la descrita. No obstante, es discutible que proceda la consecuencia de absolver por estafa al no haberse acusado de robo, como pretenden los recurrentes, y no que proceda —aun cuando se estime que es robo la correcta calificación— mantener la condena por estafa al tratarse de un delito de menor gravedad: si ha cometido un delito más grave —robo— y se le ha condenado por uno más leve —estafa— carece de razón su queja. En los casos contrarios no habría obstáculo para condenar por estafa a quien vino condenado por robo. Todo ello partiendo de que estafa y robo pueden ser consideradas —en el caso concreto— homo-

géneas, en el sentido de que todos los elementos fácticos aparecen en uno y otro tipo. Ningún hecho nuevo se introduciría en la sentencia: tan solo se otorgaría una distinta valoración jurídica. Además, el hecho de que la «nueva tipificación» jurídica sea apuntada por la propia defensa disiparía toda posibilidad de alegación de indefensión.

Pero, por encima de todo ello, parece llegado el momento en que el TS resuelva la cuestión en un Acuerdo de Pleno, evitando, como sucede hoy, que las sentencias de las AAPP condenen bien por robo o por estafa (parece que se inclinan más por esta última solución).

2. *Criterio jurisprudencial*

Ya antes de la vigencia de este Código se cuestionó la tipificación de estas conductas como hurto, robo con fuerza o estafa. La Consulta 2/1988 de la FGE sostuvo —ante la imposibilidad de aplicar la estafa clásica— la procedencia de la calificación como robo con fuerza por entender comprendida en el concepto legal de llave falsa la tarjeta y desestimó la calificación como estafa ante la dificultad de apreciar los elementos engaño y error (solo posibles de persona a persona). Posteriormente las SSTS 6-3-89, 21-9-90, 8-5-92 y 21-4-93 mantuvieron dicho criterio.

Con la promulgación del CP de 1995, parte de la doctrina ha señalado que tales supuestos de uso de tarjetas encajan con mayor claridad que antes en el robo con fuerza a la luz de los arts. 238 y 239, que consideran la tarjeta magnética como llave y, además, reputan como fuerza en las cosas el descubrimiento de las claves de los objetos muebles cerrados para sustraer su contenido —art. 238.3.º—.

Esa tesis se ha visto respaldada por el criterio mantenido por el TS en las SS 427/99, de 16 de marzo, y 666/99, de 29 de abril. Han estimado, frente a la postura de las AAPP que condenaron por estafa informática, que los hechos encajan en el delito de robo con fuerza en las cosas y no en la estafa por la inexistencia de «manipulación informática o artificio semejante» —conducta exigida por el art. 248.2, definidor de la estafa informática—.

La primera sentencia señala: «Con relación al nuevo art. 248.2 hay que entender que dicho fraude informático no contempla la sustracción de dinero a través de la utilización no autorizada de tarjetas magnéticas sobre los denominados "cajeros automáticos", porque la dinámica comisiva no aparece alejada de la clásica de apoderamiento, aunque presenta la peculiaridad de la exigencia del uso de la tarjeta magnética para poder acceder al objeto material del delito *(…) no supone por ello el uso*

de la tarjeta por el no titular la "manipulación informática" o artificio semejante que requiere el precepto». En la misma línea la segunda de las sentencias citadas absuelve de estafa y reputa robo con fuerza: «… para reservar la regulación específica que contempla el art. 248.2 a la sanción de comportamientos en los que concurra la manipulación, sin ampliarla a supuestos en los *que dicha maniobra informática o artificio contable no existe al tratarse de la utilización de una tarjeta legítima encontrada o sustraída a su titular*».

Sin embargo, otras sentencias posteriores del TS, como se verá, han variado esa postura y acogen el criterio de la estafa. En cierto modo la jurisprudencia ha venido progresivamente apartándose de la línea jurisprudencial que se viene comentando. Tres sentencias apoyarían esa afirmación: SSTS 2175/2001, 1476/2004 y 185/2006, que se comentan.

En la sentencia 2175/2001, de 20 de noviembre (Ponente Excmo. Sr. Martínez Arrieta), se ha estimado que la identificación como titular de una tarjeta por quien no lo es ante un aparato informático constituye la conducta del art. 248.2 CP. Se trataba de un caso en el que el sustractor de la tarjeta en connivencia con el empleado de un establecimiento comercial introducen ésta en el lector para obtener una mercancía con cargo a dicha tarjeta. La sentencia señala:

> «Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del CP. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que éste signifique artimaña, doblez, enredo o truco. La conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado».

En la sentencia 1476/2004, de 21 de diciembre[16], se contempla un parecido supuesto y se concluye que utilizar un sistema informático ajeno

[16] En igual sentido la reciente STS 692/2006, 26 de junio, que castiga como estafa informática la utilización de tarjetas desde un terminal de punto de venta (TPV) para el uso de tarjetas de pago. Insiste en que «*La conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente, está empleando un artificio para aparecer como su titular ante el terminal bancario a*

encaja en el verbo nuclear del tipo. La sentencia enjuiciaba los siguientes hechos: los dos acusados desde la tienda de la madre del acusado manipularon el Terminal Punto de Venta (TPV) que se encontraba en el interior del referido comercio, terminal propiedad de la entidad Banco Bilbao Vizcaya Argentaria, S.A., vinculado a la cuenta corriente de la que era titular la citada madre, y utilizando la tarjeta VISA ELECTRÓN titularidad de la acusada efectuaron 12 operaciones de compras por 100 ptas. cada una y otras tantas de «Abono por devolución de compra» por un importe total de 52 millones de pesetas que lograron así se ingresaran en la cuenta de la acusada. Posteriormente con la tarjeta extrajeron dinero en un cajero y obtuvieron servicios en establecimientos. La STS lo califica de estafa informática, señalando que sí existió manipulación informática ya que «es equivalente, a los efectos del contenido de la ilicitud, que el autor modifique materialmente el programa informático indebidamente o que lo utilice sin la debida autorización o en forma contraria al deber. En el presente caso, por lo tanto, el recurrente carecía de autorización para utilizar el medio informático y, además, produjo efectos semejantes a la misma, sobre el patrimonio del Banco».

De hecho, ese giro jurisprudencial puede verse completado claramente en la STS 185/2006, de 24 de febrero (Ponente Excmo. Sr. Bacigalupo) en la que en un caso de uso de tarjeta en cajero (en el que la Sala terminó casando la recurrida, además, por vulneración de la presunción de inocencia) afirmó:

> «Es claro que el delito de estafa (tipo básico o común del apartado 1 del art. 248), único por el que el recurrente ha sido acusado, no concurre en estos casos, dado que sólo puede ser engañada una persona que, a su vez, pueda incurrir en error. Por lo tanto, ni las máquinas pueden ser engañadas —es obvio que no es "otro", como reclama el texto legal—, ni el cajero automático ha incurrido en error, puesto que ha funcionado tal como estaba programado que lo hiciera, es decir, entregando el dinero al que introdujera la tarjeta y marcara el número clave. Sin embargo cabría pensar, sólo hipotéticamente, que *el uso abusivo de tarjetas que permiten operar en un cajero automático puede ser actualmente subsumido bajo el tipo del art. 248.2 CP, dado que tal uso abusivo constituye un "artificio semejante" a una manipulación informática*, pues permite lograr un funcionamiento del aparato informático contrario al fin de sus programadores. Pero este tipo, no puede ser considerado homogéneo con el del art. 248.1 CP y, en todo caso, no ha sido objeto de acusación».

---

quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado. Y, en consecuencia, se encuentra incurso en la conducta definida en el art. 248.2 del Código penal».

3. *Encaje típico de la conducta: identificarse ante el sistema es manipulación informática*

Deben examinarse dos cuestiones diferentes: 1) ¿existe fuerza en las cosas al introducir la tarjeta en un cajero? y ¿existe apoderamiento?, y 2) se produce o no manipulación informática por el hecho de usar una tarjeta y teclear un *password* conocido previamente.

1) Que las tarjetas constituyen llave no ofrece cuestión.

a) El problema es otro: no basta con que la tarjeta sea llave sino que ésta ha de haber sido *empleada para acceder al lugar en el que las cosas se guardan*[17]. La fuerza en las cosas que requiere el robo es aquella precisa para «acceder al lugar donde éstas se encuentren», tal y como lo define legalmente el art. 237 CP. Y el dinero en los cajeros se halla en un cajetín en el interior del mismo al que en ningún momento se accede.

Al operar en un cajero con una tarjeta, lo esencial es que se introducen datos en el ordenador y que el sistema efectúa una disposición patrimonial no consentida por el titular que se llega a registrar contablemente. Es accesorio que se acceda con la tarjeta (lo que no siempre es así) al recinto donde se halla el cajero y no cabe afirmar que se acceda al lugar donde el dinero se guarda. Los arts. 238 y 239 no son aplicables a estos supuestos. El empleo de la tarjeta como llave permite calificar de robo cuando con la misma se accede al lugar donde están las cosas (v. gr.: la tarjeta es la llave de la habitación del hotel a la que se consigue entrar para robar algún objeto).

Igualmente el descubrimiento de las claves a que se refiere el art. 238.3 ha de ser para acceder al interior de los objetos muebles cerrados (v. gr.: se descubre la clave y se accede al interior de la caja fuerte).

En nuestro supuesto no se accede al interior del cajero, es decir, al depósito donde se conserva el total del dinero de la máquina, sino que *el aparato entrega por sí una cantidad seleccionada de tal depósito de dinero y como acto de disposición deja incluso constancia contable de la operación*.

Por tanto, *lo esencial es que se produce una operación informática —introducir la tarjeta, teclear el número clave y seleccionar cuenta e importe—, que lleva al aparato a efectuar una «transferencia no consentida de un activo patrimonial»*.

---

[17] En esta línea Almela Vich, C., «El Delito de estafa y el de apropiación indebida». *Actualidad penal* n.º 35, 1998; y González Rus, J.J., «Protección penal de sistemas, elementos, datos, documentos y programas informáticos». *RECPC* 01-14, 1999.

b) Se ha negado que se trate de estafa ante la consideración[18] de que no se da una verdadera transferencia no consentida de un activo patrimonial, como exige el tipo, sino que se entrega una cosa mueble como es el dinero. Se parte de la necesidad de un asiento contable. La tesis no es convincente ya que el asiento contable se produce, no de una cuenta a otra sino de una cuenta a «ventanilla». La operación se carga en la cuenta del titular de la tarjeta y se anota como destino la retirada en efectivo por cajero. No comprendo por qué sólo ha de admitirse en la estafa los casos en que el activo patrimonial se anota contablemente en otra cuenta y no las operaciones de retirada de efectivo ante una máquina. Aun en aquellos casos en que se transfiriera contablemente a otra cuenta el sujeto activo puede —y será lo más normal— retirar materialmente después el activo transferido a su cuenta, sin que por ello sea entonces cuando cometa la estafa, que ya estaría consumada en tanto se tuvo la disponibilidad del dinero una vez que éste ingresó en la cuenta propia.

De otra parte, Galán Muñoz[19] niega la calificación de estafa al señalar que se obtiene un lucro «no como consecuencia directa de la consecución de una verdadera transferencia electrónica de activos patrimoniales, sino a resultas de la posterior ejecución por su parte, o por parte de un tercero, de un *acto de apoderamiento* de dinero ajeno».

A mi modo de ver la tesis no es admisible pues no existe acto de apoderamiento alguno sino mera recepción por el usuario del cajero de lo que el sistema informático ha transferido o dispuesto voluntariamente en su favor. Al igual que no se habla de apoderamiento —propio del robo— cuando el estafador recibe materialmente dinero del estafado en virtud del acto de disposición en la estafa común (incluso aunque se lo dejara en un sobre en un determinado lugar de donde tuviera que retirarlo). Recibir físicamente dinero es diferente de apoderarse. Apoderarse implica la ausencia de voluntad del *tradens*, y en la estafa el *tradens* (persona o cajero) entrega el dinero, ya sea por el engaño en la estafa común o por la manipulación del sistema en la informática.

La disposición de la maquina es voluntaria y por ello no es dable afirmar que existe el «apoderamiento» propio del robo que exige que se produzca contra la voluntad —o al menos sin la voluntad— del dueño. Sobre el carácter voluntario de la entrega hago míos los razonamientos

---

[18] Herrera Moreno, M., «El fraude informático en el Derecho penal español». *Actualidad penal* n.º 39, 2001.

[19] *Op. cit.*, pp. 756 y 903.

contenidos en el Voto particular emitido a la STS 1025/1992, de 8 de mayo, por el Magistrado Bacigalupo Zapater[20].

Por el contrario, el ejemplo me parece muy ilustrativo, sí sería «apoderarse» la conducta de quien consiguiendo manipular el sistema informático de apertura de una caja fuerte accede a su interior y toma el dinero allí existente; en tal caso no hay transferencia voluntaria ni se efectúa asiento contable de salida alguno.

2) Lo que habrá que determinar es si esa operación informática puede ser calificada de «manipulación informática o artificio semejante».

La no inclusión en el concepto de «manipulación informática» de aquella conducta consistente en introducir en el cajero la tarjeta y teclear el número secreto, tesis que ha manejado la jurisprudencia en las primeras sentencias citadas y que llevó a negar la posible calificación como estafa, es más que discutible.

Dicha tesis parte de la idea inicial de que no toda operación en un sistema informático debe ser considerada «manipulación informática». Y en esta línea se confiere a la expresión manipulación un sentido pe-

---

[20] Transcribo parte del referido Voto particular: «… En particular no cabe afirmar como lo hace la mayoría de la Sala, que "ese apoderamiento a través de manipulación normal sobre el cajero sito en la fachada de la entidad bancaria (…) constituye por lo menos un delito de hurto (…) porque siempre se estaría tomando una cosa sin la voluntad de su dueño". Precisamente el último elemento, la contrariedad a la voluntad de su dueño, no se puede afirmar aquí sin violentar el concepto de "voluntad" que esta Sala utiliza a diario. La programación del cajero electrónico para que entregue el dinero a cualquier persona que disponga de la tarjeta y conozca el número clave, implica que el titular del dinero, es decir el banco o la institución de crédito, quieren que el dinero sea entregado al que introduzca la tarjeta y señale el número clave secreto, cualquiera sea su identidad, pero también cualquiera sea su legitimación para hacerlo. Contra esta afirmación se afirma, sin embargo, que es evidente que la institución de crédito no quería entregar el dinero a una persona no legitimada, es decir, a una persona que carezca de autorización del titular de la tarjeta. Pero, este punto de vista se apoya en una confusión de la voluntad con el deseo. Por lo tanto, se expone a todas las críticas que se han formulado desde antiguo a tal identificación: un resultado indeseable no es por ello involuntario. De otra manera no sería posible admitir que el dolo eventual es una forma de los actos voluntarios. En este sentido no parece discutible que esta Sala no hubiera dudado en considerar como voluntaria la conducta del que predispone un arma de fuego para que se dispare cuando alguien pretenda abrir la puerta de la habitación, con el objeto de dar un escarmiento al que intente robar en su ausencia, aunque el que resulte muerto por el disparo no haya querido entrar a robar, p. ej. porque era su propio hijo ignorante del mecanismo de defensa predispuesto (…). Si se considera, por el contrario, que toda persona que obtiene dinero del cajero automático sin estar legitimado para ello realiza una conducta típica, habrá que sancionar como autor de hurto o de robo del dinero obtenido al titular legítimo de la tarjeta que extrae más dinero que el que tiene contractualmente autorizado. También en este caso habría que admitir que el banco "no quería" entregar la cantidad que supera el límite establecido en el contrato…».

yorativo. Es decir, la conducta del art. 248.2 al exigir una «manipulación informática» está precisando que la operación llevada a cabo deba contener un elemento de mendacidad. Ahora bien, la expresión manipulación no implica mendacidad o conlleva carga peyorativa desde una interpretación literal. Además, ese elemento peyorativo se cubre en la medida que el autor a través del manejo informático burla el sistema y obtiene una transferencia inconsentida.

En cualquier caso, donde radica el desacuerdo es en la restricción de la manipulación, propugnada por alguna doctrina y seguida por la jurisprudencia, a los casos siguientes: 1) manipulación del programa: al introducir los datos correctos, el programa, indebida y previamente manipulado, efectúa una operación que se salda con un resultado distinto, y 2) manipulación de datos: lo que implica suprimir, ocultar o alterar los datos reales por lo que el resultado final que ofrece el programa es distinto. Y en esta segunda modalidad de manipulación no incluye esa línea jurisprudencial los casos en que el programa es puesto a funcionar de modo no autorizado, mediante la identificación ante el sistema con un número PIN indebidamente obtenido.

Ahora bien, por el contrario, a mi juicio, sí que *en tales casos se están ocultando datos reales e introduciendo datos falsos en el sistema: se oculta la identidad real del operador y se suplanta la del verdadero titular. Tal identificación, a través de la introducción del número secreto obtenido indebidamente, tiene una relevancia o eficacia jurídica que constituye el dato clave para estimar que sí estamos ante una manipulación informática. Dicha relevancia se pone de manifiesto a través de la consideración de que teclear el* password *ante el sistema es tanto como identificarse.*

La Decisión Marco del Consejo de la Unión Europea de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, dispone en su art. 3:

> «Cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario (…) mediante:
>
> —la *introducción*, alteración, borrado o supresión indebidos *de datos informáticos, especialmente datos de identidad*, o
> —la interferencia indebida en el funcionamiento de un programa o sistema informáticos».

De ahí se desprende que la identificación a través del número secreto o PIN es una de las conductas que enuncia la Decisión Marco entre las que caracterizan la manipulación informática.

Debe repararse en que *en un supuesto de estafa ordinaria la ocultación de la verdadera identidad o la suplantación de la identidad de un tercero no generarían dudas acerca de su posible consideración como engaño bastante*, en definitiva como manipulación.

La identificación a través del número secreto genera una presunción de uso del sistema por parte de su titular, y de ello se extraen importantes efectos jurídicos, fundamentalmente en el plano de la responsabilidad civil: así, entre otras, la sentencia 6/1999, de 20 de enero, de la AP de Navarra, sección 1.ª, estimó que el hecho de haber sido tecleado el *password* suponía tanto como identificarse, lo que excluyó la carga de la prueba para la entidad bancaria de que la tarjeta fue usada por el cliente, imputando el perjuicio al cliente de la alegada utilización en un cajero de la tarjeta por una tercera persona, ya que, además, el robo de la misma no fue comunicado. En idéntico sentido de estimar relevante el teclado del número PIN a efectos de servir de pleno acto de identificación cabe señalar la STS, Sala 1.ª, de 21 de diciembre de 2001.

En consecuencia, debe incluirse como una modalidad de manipulación informática, a los efectos de aplicar el art. 248.2, el mero hecho de utilizar el número secreto de otro para identificarse ante el sistema, aunque incluso dicho número hubiese sido obtenido al margen de cualquier actividad delictiva[21] (*v. gr.:* se llega a conocer el número porque el titular lo deja apuntado o lo comunica imprudentemente o porque el sujeto activo lo deduce de la fecha de nacimiento o de otro dato del titular que le lleva a descubrirlo por pura casualidad).

Los supuestos que se reservaban por la inicial línea jurisprudencial citada para la inclusión en el concepto de manipulación informática constituyen supuestos que exceden de una mera manipulación y entran en concurso delictivo con otras infracciones. Así:

—En los casos en que se obtenga el *password* mediante un artificio informático (por ejemplo, el *hacker* que se introduce en el sistema para apoderarse de dichas claves de acceso) estaremos ante un doble delito: el apoderamiento constituiría un delito de descubrimiento de secretos del art. 197; la utilización posterior de dicho *password* como medio de identificación ante el sistema cubriría la figura de la estafa informática.

—En los casos de manipulación del programa para obtener una transferencia estaríamos ante dos hechos penalmente valorables en concurso: la alteración y consiguiente causación de daños, des-

[21] En esta línea de conceptuación de la manipulación informática se sitúa Galán Muñoz, A., *op. cit*., pp. 754 y ss.

perfectos o alteraciones en el programa constituiría el delito de daños recogido en el art. 264.2; la obtención de una transferencia implicaría la estafa informática.

En definitiva, identificarse ante el sistema informático mendazmente, introducir datos en el sistema que no se corresponden con la realidad, ha de ser considerado bajo la conducta de manipulación informática a que se refiere el tipo del art. 248.2.

4. *La calificación de robo en oposición a la determinación del perjudicado por tales conductas*

Un penúltimo argumento sirve para defender la tesis de estafa frente a la de robo. Si se considera robo el hecho, habría de entenderse perjudicado por el robo siempre a la entidad bancaria: el dinero ha sido robado, es decir, tomado o apoderado del cajetín o depósito de dinero del cajero automático, y no cabe sostener entonces que se haya robado el dinero de un concreto titular.

Ello pugna con la consideración efectuada en algunas sentencias (como la anteriormente citada de la AP de Navarra, entre muchas otras, que dilucidan la cuestión del perjudicado tanto en vía civil como penal) que entran a valorar si el perjudicado ha de ser el titular de la cuenta o el Banco, habida cuenta precisamente de que se usó el *password* en la operación.

Tal consideración sobre la persona perjudicada a raíz del acto de disposición (la transferencia no consentida del activo patrimonial que realiza automáticamente el aparato) es propia de la figura de la estafa y no del delito de robo, que no contiene acto de disposición alguno.

Un último argumento —ciertamente muy práctico si se quiere y poco dogmático— en aras de la calificación como estafa. Es muy frecuente el descubrimiento de grupos de personas en cuyo poder se hallan tarjetas falsificadas así como utensilios para su falsificación. De hecho clonan las tarjetas para realizar compras en establecimientos comerciales y también para extraer dinero en cajeros de entidades de crédito. Pues bien, resulta artificial desdoblar la calificación jurídica del uso de la tarjeta, de modo que su uso en local comercial sea constitutivo de estafa y su uso en cajero sea merecedor de la calificación de robo. De hacerlo así nos hallaríamos ante dos delitos distintos en concurso (no parece que puedan incluirse en un único delito continuado). Resulta absurda, y más grave para el penado, esa separación en dos delitos de lo que no es sino una única intención de los autores de obtener metálico o efectos mediante las tarjetas, que merece una única respuesta punitiva.

5. *La solución del Anteproyecto de 2006 de reforma del CP en materia de estafa*

El Anteproyecto modifica el artículo 248, alterando en buena medida la definición legal de estafa, que quedaría redactado como sigue:

> «1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
>
> 2. También se consideran reos de estafa:
>
> a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
> b) Los que fabricaren, introdujeren o facilitaren programas informáticos especialmente destinados a la comisión de las estafas previstas en este artículo.
> c) *Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en ellos, realicen operaciones de cualquier clase en perjuicio de su titular*.
> d) Los que, en un procedimiento judicial de cualquier clase, faltaren a la verdad en sus alegaciones o manipularen las pruebas en que pretendieran fundarlas, provocando error en el Juez o Tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero».

Las novedades del Anteproyecto al definir la estafa son muchas.

1) El uso de tarjetas en cajeros, que es el tema que nos ocupa, se recogería ahora en un tipo especial en el apartado c) del nº 2 del art. 248 que regularía la estafa mediante utilización de tarjetas de débito, crédito o cheques de viaje. La utilidad de recoger entre el concepto de estafa y de modo especial tales conductas deriva precisamente de las dudas suscitadas acerca de su calificación. En todo caso se echa de menos una referencia más concreta en la Exposición de Motivos al porqué de la nueva tipificación, pero es indudable que la reforma evidencia la voluntad del legislador de calificar como estafa los empleos fraudulentos de tarjetas en todo caso (operaciones de «cualquier clase» indica la Exposición de Motivos), ya en establecimientos comerciales y por ello ante personas o directamente ante terminales informáticos, aun cuando en ellas se utilizare una clave o número PIN.
   Es de señalar que la mención que el proyectado art. 248. 2. c) efectúa a «en perjuicio de su titular» no es del todo correcta. En

el empleo fraudulento de tarjetas de crédito no siempre es fácil determinar quién soporta finalmente el perjuicio derivado, lo que aconseja no cerrar la definición legal circunscribiendo el perjuicio al «titular» de la tarjeta. Parece preferible que la definición legal se refiera a en perjuicio de su titular «o de tercero».

2) En el art. 248.2.b) se suprime la «posesión» de programas informáticos especialmente destinados a la comisión de las estafas. Este apartado, recientemente introducido por la LO 15/2003, de 25 de noviembre, castiga a los que «fabricaren, introdujeren, poseyeren o facilitaren» dichos programas. La proyectada supresión de la posesión dificultará en la práctica la persecución de estos hechos. De otra parte, no se vulnera el principio de intervención mínima en tanto se castiga la posesión únicamente cuando se acredite que está destinada a la comisión de estafas, de acuerdo con la línea interpretativa ya señalada en su día por la STC 105/1988 en relación con el delito de tenencia de útiles para el robo del art. 509 del CP derogado. Por ello, se estima preferible el mantenimiento de la redacción actual. Además, la vigente redacción es paralela a la del art. 400 que castiga la tenencia de programas de ordenador específicamente destinados a la comisión de falsificaciones o falsedades, sin que el Anteproyecto haya venido a suprimir de este precepto la posesión de tales programas[22].
3) La regulación en el Anteproyecto de la denominada estafa procesal en el apartado d) del n.º 2 del art. 248 merece una crítica muy desfavorable, que no me resisto —aunque excede del ámbito de esta ponencia— a dejar aquí apuntada[23].

---

[22] En este sentido se expresa el Informe del Consejo Fiscal al citado Anteproyecto.

[23] En el apartado d) del n.º 2 del art. 248 se recoge la definición de la estafa procesal y al tiempo se excluye la misma de los subtipos agravados del art. 250.

No es necesario que el art. 248 defina todas las posibles modalidades de estafa siempre que éstas tengan encaje en el concepto genérico de la misma. Así, no se define la estafa de seguro o la estafa a través de un cheque al descubierto, por poner ejemplos, y entendemos que tampoco debe definirse la estafa procesal en tanto es una modalidad que, aun singular, se halla dentro de la definición genérica de estafa del apartado 1 del precepto, por mucho que efectivamente el acto de disposición lo realice un juez o un tribunal en perjuicio de un tercero. El concepto, además, es pacífico en la jurisprudencia, que suele definir con precisión esta modalidad de estafa cuando la enjuicia.

Al tiempo, la definición dada no está exenta de problemas: en la definición, al recoger la conducta engañosa, el proyectado precepto se refiere a una doble modalidad «faltar a la verdad en las alegaciones y manipular las pruebas». No parecen conductas equiparables en gravedad.

Y no está claro que faltar a la verdad (como mera falsedad ideológica) en las alegaciones de un proceso sea —siempre y en todo caso como podría hacer pensar erróneamente

V. **Manipulación de máquinas para obtención de productos**

Se suscita la cuestión de la dificultosa aplicación del art. 248.2 a la conducta consistente en abusar de aparatos expendedores para que entreguen, sin el correspondiente pago, las mercancías que albergan o permitan el acceso a servicios.

El Anteproyecto 2006 de reforma del CP no efectúa previsión específica alguna para estas conductas.

La jurisprudencia menor ha venido pronunciándose en modo desigual: mientras la AP de Lugo en sentencia de 9 de julio 1998 aplicaba este tipo a quienes mediante monedas cogidas con un hilo conseguían en sucesivas operaciones tanto el producto como la devolución (obteniendo más de 400 €) del supuesto precio al estimar que concurría un

---

la definición legal— un engaño que revista el carácter de bastante y sobrepase la frontera penal. Es decir, no todo incumplimiento de la probidad procesal encaja en el engaño bastante de la estafa procesal. Ello ha sido reconocido así por el TS en múltiples sentencias (así, se ha señalado, por ejemplo, que no basta la falsedad ideológica y que no es estafa si el acusado niega su firma o no reconoce la deuda; más recientemente, después de que no se alcanzara acuerdo alguno en el Pleno no jurisdiccional del Tribunal Supremo de 27 de abril de 2005 acerca de la relevancia que penalmente ha de otorgarse a la conducta consistente en oponer —mendazmente— la excepción de falsedad en un juicio ejecutivo, se dejó libertad a la Sección para resolver haciéndolo en la STS 624/2005, de 27 de abril, que estima que la conducta de haber opuesto en un pleito civil la excepción de falsedad de las firmas ciertamente estampadas por el acusado en las letras de cambio en que se fundaba la acción ejecutiva en ejercicio no ha de tener encaje penal en el delito de estafa pese a que es un modo de operar moral y socialmente reprobable, pero que no merece un juicio de reproche en el ámbito jurídico penal) y parece que la amplia definición legal apunta a otra cosa, al castigo de toda falsedad ideológica, lo que sólo podría dar lugar a confusas interpretaciones.

De seguirse la definición proyectada se estaría ampliando la estafa procesal para incluir las alegaciones falsas de las partes en un proceso. Ello conllevaría consecuencias no deseables: la limitación excesiva e indebida del derecho de defensa y la apertura de una enorme puerta a todo tipo de posibles prejudicialidades penales en tanto que alguna de las partes de un proceso no penal estimara que la contraparte «falta a la verdad en las alegaciones».

Por ello, se estima innecesaria e incorrecta la definición legal.

De otra parte, con la definición legal y supresión del art. 250.2 se otorga el carácter de estafa no agravada a la estafa procesal, que se ve sometida al régimen punitivo común o tipo básico de la estafa. Parece preferible mantener su carácter de subtipo agravado en el art. 250 en atención a la incidencia que origina en la Administración de justicia, la mayor energía criminal para su logro, las mayores complicaciones procesales para desmontar sus efectos y la implicación en la conducta delictiva de autoridades judiciales que se ven involuntariamente envueltas en la trama de terceros. Es más la Exposición de Motivos se refiere a que se ha apreciado una «preocupante repetición de intentos, a veces consumados, de engañar a los Jueces» lo que, precisamente, abonaría su mantenimiento como subtipo agravado.

artificio semejante a la manipulación informática, la SAP de Madrid de 21 de abril de 1999 negaba estafa ante quien utilizando el abono de tercero hacía que el torniquete de un servicio de transporte le franqueara el paso, absolviendo de estafa pues no se daba transferencia de activos patrimoniales.

Son muchos los problemas que la calificación de estafa informática sugiere.

En primer lugar es discutible la concurrencia de la conducta. Afirmarla requerirá adoptar un concepto amplio de manipulación informática o de artificio semejante, como cualquier acción tendente a lograr el «engaño» de una máquina, a hacer accionar la misma en nuestro favor. Lo que sucede es que en muchos casos (el de la sentencia de Lugo es un claro ejemplo) no estaremos ante una manipulación o artificio informáticos sino meramente mecánicos. No en todas las máquinas cabe calificar de informático el mecanismo que la hace actuar en nuestro favor. Por ello, para cobijar algunas de estas conductas en la estafa será preciso admitir que el CP al referirse a «artificios semejantes» admite que sean simplemente mecánicos, no informáticos. A mi juicio con ello no se vulneraría el principio de legalidad: la estafa informática surge para incluir aquellos supuestos en los que se «engaña» a una máquina y ésta, sin apoderamiento del sujeto activo, entrega «voluntariamente» algo a cambio. En el art. 248.2 se recogería así la estafa comprendiendo en ella cualquier engaño —informático o mecánico— a una máquina.

En segundo lugar, es discutible que en todos estos casos pueda hablarse de la «transferencia de un activo patrimonial». Algunos autores[24] anudan ese resultado al hecho de que la operación se anote contablemente como una transferencia contable de una partida a otra —en el caso del torniquete en ocasiones existe algún registro contable de la operación para impedir que con el mismo abono accedan dos personas a un mismo espectáculo, no en el de la máquina expendedora— y que ello suponga la afectación de un elemento contable como son los activos —lo que no sucedería en estos casos—. Pero la exigencia de dicha anotación o la restricción del concepto «activo» sólo a valores representados mediante anotaciones no se perfila en el texto del art. 248.2. El concepto de «transferencia no consentida de un activo patrimonial» se cumple, a mi juicio, tanto si un valor mediante anotación contable pasa de una cuenta a otra, cuanto si se entrega materialmente por la máqui-

[24] Herrera Moreno, M., «El fraude informático en el Derecho penal español». *Actualidad penal* n.º 39, 2001.

na un activo entendiendo por tal el producto que la maquina dispensa o el servicio al que permite el acceso.

En todo caso, las dudas que la cuestión suscita y las dificultades de orden práctico para que estas conductas (normalmente se quedará en falta lo descubierto) lleguen al TS, parecen aconsejar que en el Anteproyecto de 2006 citado se establezca alguna aclaración sobre su tipicidad (como ha sucedido, como hemos visto, con los cajeros automáticos y también, como veremos, con la falsificación de tarjetas).

VI. **Falsificación de tarjetas**

Aunque no se trata de un supuesto de estafa informática —sino en muchas ocasiones el delito previo para su posterior comisión—, he considerado de interés una referencia a esta materia, tan absolutamente frecuente en la práctica de nuestros tribunales.

1. *Su consideración como falsificación de moneda*

La STS 948/2002, de 8 de julio, planteó la cuestión de que la falsificación de las tarjetas de crédito o débito dada la técnica de «asimilación» a la moneda aplicada por el Código en su artículo 387, suscitaba el problema de la determinación de si la manipulación de una tarjeta auténtica, en cuya banda magnética se introducen datos obtenidos fraudulentamente de otra perteneciente a un tercero, ha de considerarse «fabricación» de moneda falsa, a los efectos del artículo 386.1.º CP —en cuyo caso competencia de la AN— o si es procedente la alternativa, caso de no considerarse falsificación/fabricación de moneda, de considerar que nos hallamos ante una falsedad de documento mercantil (arts. 390 y 392 CP), en su caso en concurso instrumental con el delito de estafa (art. 248 CP), o, incluso, la subsunción de toda la conducta defraudatoria, incluida la falsedad, en el tipo especial del artículo 248.2 del Código Penal, en cuyo caso compete a las AAPP.

Sometida la cuestión, por la indudable trascendencia que entrañaba, al Pleno no jurisdiccional del Tribunal Supremo, en sesión celebrada el día 28 de junio de 2002, se acordó que la correcta calificación de tales hechos, en criterio de dicho Pleno, habría de ser como delito de falsificación de moneda del artículo 386 del Código Penal, toda vez que la generación de un documento nuevo, sin existencia previa ha de considerarse «fabricación» y no simple «alteración», pues precisamente el elemento esencial en la tarjeta es la banda magnética y la voluntad del

legislador no parece otra que la de la severa represión de estas acciones, atendiendo a la importancia económica actual de las tarjetas como instrumentos de pago.

Literalmente el Acuerdo de la Sala, adoptado en el referido Pleno, dice así:

> «Las tarjetas de crédito o débito son medios de pago que tienen la consideración de "dinero de plástico", que el artículo 387 del Código Penal equipara a la moneda, por lo que la incorporación a la "banda magnética" de uno de estos instrumentos de pago, de unos datos obtenidos fraudulentamente, constituye un proceso de fabricación o elaboración que debe ser incardinado en el artículo 386 del Código Penal. En tales supuestos, dada la imposibilidad de determinación del "valor aparente" de lo falsificado, no procede la imposición de la pena de multa, también prevista en el referido precepto. Asimismo se pronuncia el Pleno favorablemente a la procedencia de que por el Tribunal competente para la resolución del Recurso de Casación se acuda, a tenor de lo dispuesto en el artículo 4.3 del Código Penal, al Gobierno de la Nación exponiendo la conveniencia de la inclusión, en el Código Penal, de un precepto específico que contemple los actos de falsificación de tarjetas, con establecimiento de las penas adecuadas para cada supuesto, en consonancia con lo previsto para esta materia por la Decisión Marco del Consejo de Ministros de la Unión Europea sobre "la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo", de fecha 28 de mayo de 2001».

Posteriormente, el Pleno no jurisdiccional de esta Sala, celebrado en fecha 5 de abril de 2005, aunque consideró la cuestión, no adoptó una resolución ni criterio distinto del transcrito, sin perjuicio de su estudio en una nueva reunión. El Acuerdo ha sido recogido en posteriores sentencias del TS y ha sido ratificado en otro Pleno celebrado el 27 de abril de 2005.

2. *Diferencia y posible concurso con la estafa informática*

La ya citada STS 948/2002, de 8 de julio, diferencia entre el delito de falsificación de tarjeta de crédito del art. 386 CP y la estafa informática del art. 248.2, señalando:

> «la conducta consistente en la alteración de la banda magnética, que supone la generación de una tarjeta "ex novo", integra, por sí misma, el delito de falsificación de moneda, independiente del uso posterior fraudulento a que ese instrumento de pago mendaz pueda ser destinado, produciéndose, en tal caso, una relación concursal entre ambos

> ilícitos. Una cosa es, por tanto, que se manipulen sistemas informáticos para defraudar, y otra, completamente distinta, que se confeccione una tarjeta mediante la incorporación falsaria de datos de origen o producción informática para, con ella, posteriormente llevar a cabo actos fraudulentos. Diferencia que claramente ha de distinguir entre el contenido de la Estafa denominada informática y la cometida mediante el empleo de una tarjeta con banda magnética previamente falsificada».

3. *Cuestión de competencia objetiva*

Partiendo de la doctrina sentada han sido, sin embargo, muchas las cuestiones, prácticamente siempre negativas, suscitadas entre Juzgados de Instrucción y Juzgados Centrales acerca de la no competencia para conocer de las falsificaciones de tarjetas de crédito.

La cuestión desde el plano teórico se halla resuelta según lo expresado: si los hechos encajan en la falsificación de moneda (a la que se equiparan tarjetas y cheques de viaje) conocerá la AN. Si se trata de uso de lo ya antes falsificado por otros la calificación procedente será de estafa y falsedad documental y conocerá la AP.

Sin embargo, las cuestiones se han originado fundamentalmente por la discrepancia en torno a la indiciaria calificación de los hechos. De ese modo la calificación posible e indiciaria de los hechos en atención a la prueba de que se disponga determinará la competencia objetiva. El ATS 12-9-2005 poniendo de relieve esta cuestión señala:

> «… no quiere decir que todos los hechos delictivos en los que aparezcan tarjetas de crédito o similares falsificadas hayan de ser competencia de la Audiencia Nacional. Es relativamente frecuente que lo descubierto sea sólo el uso de una o varias tarjetas de crédito para sacar dinero de algún cajero o entidad bancaria o para comprar en un establecimiento comercial, en cuyo caso no cabe prever imputación alguna de esos delitos de los arts. 386, 387 ó 400, sino únicamente de estafa, uso de documento mercantil falso u otra figura delictiva siempre ajena a tales falsedades de moneda o tipos asimilados. Cuando así sucede no hay base para atribuir la competencia a los órganos penales de la Audiencia Nacional, sin perjuicio de que, si realmente, por los datos existentes en el procedimiento, es previsible que se acuse por delito de falsedad de moneda de esos arts. 386, 387 ó 400 CP o esa acusación por falsedad de moneda llega a formularse, sea entonces cuando tengan que remitirse las actuaciones a estos últimos órganos».

Debe señalarse que la mera posesión de la tarjeta de crédito falsificada para su utilización como medio de pago, o, en general, como instrumen-

to mercantil, no se encuentra incardinada en el delito de falsificación de moneda, de suerte que el uso de la misma podrá generar un delito de estafa y de falsedad en documento mercantil, cuya competencia instructora recaerá en el órgano jurisdiccional del lugar según las reglas del art. 17 de la Ley de Enjuiciamiento Criminal. En tanto que la conducta imputada no conste que consista en algo distinto de la simple utilización de una tarjeta de crédito falsa para abonar mercancías o servicios, la competencia ha de recaer en el Juzgado de Instrucción correspondiente.

Normalmente habrá de atenderse a determinados datos probatorios para estimar el delito del art. 386. Fundamentalmente al hecho de que la tarjeta contenga los datos de identidad del inculpado, en cuyo caso es procedente la consideración de la participación a modo de cooperador necesario del inculpado en la alteración de la banda magnética de la tarjeta, arts. 386 y 387 CP, por cuanto que suministró para la falsificación de la tarjeta de crédito sus datos de identidad, lo que reclama la competencia de la Audiencia Nacional al amparo del art. 65 LOPJ. También el hecho de que en los registros se hayan intervenido gran cantidad de tarjetas, lectores-grabadores de bandas magnéticas, ordenadores en cuyo disco duro aparecen programas para la creación de tarjetas, tarjetas con la banda magnética borrada u otros útiles para la falsificación.

Son varias las resoluciones del TS en los últimos tiempos acogiendo estos criterios. Así AATS de 24 de enero, 7 de julio, 18 de noviembre y 10 y 22 de diciembre de 2003 y de 16, 19, 26, 28 y 30 de enero y 18 de febrero de 2004 y de 10 de marzo, 14 junio, 12 y 15 septiembre, 6 octubre y 29 noviembre de 2005.

4. *La solución del Anteproyecto de 2006 de reforma del CP en materia de falsificación de tarjetas de crédito*

El Anteproyecto incide de modo esencial sobre la calificación de la conducta y sobre la competencia objetiva al modificar los arts. 387 y 399 bis CP y el art. 65 LOPJ.

El proyectado artículo 387 quedaría redactado como sigue:

> «A los efectos del artículo anterior, se entiende por moneda la metálica y el papel moneda de curso legal. Se equipararán a la moneda nacional las de otros países de la Unión Europea y las extranjeras».

Se suprime así la actual referencia equiparativa a las «tarjetas de crédito, las de débito y las demás tarjetas que puedan utilizarse como medio de pago, así como los cheques de viaje».

El Anteproyecto, en su Disposición final primera, también contempla la modificación del art. 65 LOPJ para atribuir a los órganos de la Audiencia Nacional, el conocimiento entre otros de los delitos de «b) Falsificación de moneda y fabricación de tarjetas de crédito y débito falsas y cheques de viajero falsos, siempre que sean cometidos por organizaciones o grupos criminales». De este modo el cambio proyectado alcanzaría a la competencia objetiva para conocer de estas causas que quedará extramuros de la Audiencia Nacional —incluso tratándose de falsificación de moneda— salvo que concurra una organización o grupo criminal. No cabe dejar de reconocer que la atribución de todas las falsificaciones de tarjetas de crédito a dicho órgano, sin la exigencia de la concurrencia de alguna otra nota, evidenciaba una carga de trabajo no fácilmente justificable y poco operativa.

También alcanza la reforma proyectada a la calificación de la conducta. Las conductas falsarias sobre las tarjetas se tipifican —entre las falsedades documentales— en el art. 399 bis del Anteproyecto, que dispone:

> «1. Será castigado con la pena de prisión de cuatro años a ocho años el que falsificare, copiándolos o reproduciéndolos, tarjetas de crédito o débito o cheques de viaje. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o los hechos fueran cometidos en el marco de una organización criminal dedicada a estas actividades.
>
> Los Jueces y Tribunales impondrán a la organización, bien como penas si procediere la declaración de su responsabilidad penal de acuerdo con lo dispuesto en el artículo 31 bis de este Código, bien como medida en los casos previstos en el artículo 129, la disolución y clausura definitiva de sus locales y establecimientos.
>
> 2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados en cantidad que permita suponer están destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación.
>
> 3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de dos a cinco años.»

Sobre toda esta materia el Informe del Consejo Fiscal al Anteproyecto, de fecha 27 de noviembre de 2006, efectúa unas muy interesantes aportaciones[25].

---

[25] Puede verse en www.intranet.fiscal.es. Señala el referido Informe sobre esta materia:

«Como complemento a esta reforma se tipifica separadamente la falsificación, la tenencia y el uso de tarjetas de crédito o débito y cheques de viaje, creando a dicho fin una nueva Sección, 3.º bis, en el Capítulo II del Título XVIII del Libro II, integrada

por un único artículo el 399 bis, en el que se describen dichos comportamientos de falsificación a los que posteriormente nos referiremos.

La actual equiparación a la moneda metálica y/o al papel moneda, de las tarjetas de crédito, de débito y cheques de viaje, se llevó a efecto por la L.O. 10/1995 de 23 de Noviembre, frente a la concepción más estricta que al respecto había mantenido el Código Penal TR 1973, en el artículo 284. La inicial redacción de este precepto en el Código Penal de 1995, fue modificada posteriormente por la L.O. 15/2003 de 25 de noviembre, que amplió el concepto de moneda, haciendo extensiva dicha equiparación a las demás tarjetas que puedan utilizarse como medio de pago y cuya vigencia se produjo el 1 de octubre del 2004.

La preocupación por las conductas falsarias relacionadas con medios de pago distintos del efectivo, cristalizó en la Decisión Marco del Consejo de la Unión Europea de 28 de mayo del 2001 en la que se puso de manifiesto la necesidad de que estas conductas fueran objeto de tipificación en los estados miembros, previéndose sanciones efectivas, proporcionadas y disuasorias para las personas físicas y jurídicas que cometan o sean responsables de tales delitos. Esta Decisión, orientada a favorecer la lucha, a nivel internacional, contra el fraude y la falsificación de medios de pago, había sido precedida de otros instrumentos jurídicos como la Decisión de 29 de abril de 1999 por la que se amplia el mandato de Europol a la persecución de esta actividad criminal.

Esta línea de actuación supranacional es coincidente con el planteamiento del legislador español al equiparar los comportamientos falsarios realizados respecto de la moneda metálica o papel moneda y de otros instrumentos de pago, siendo la última modificación operada en el artículo 387 C. Penal por la L.O. 15 /2003 el resultado de la voluntad del legislador de implementar en el ordenamiento jurídico interno la Decisión Marco de 28 de mayo del 2001. Sin embargo la mencionada Decisión no propugna una equiparación, absoluta a efectos penales entre las conductas falsarias que tienen por objeto la moneda y las que se refieren a otros instrumentos de pago, sino únicamente promueve la adopción, en los distintos ordenamientos jurídicos, de las medidas necesarias para garantizar la protección de dichos instrumentos de pago, mediante la tipificación de determinados comportamientos en relación con los mismos entre los que se incluye su falsificación o manipulación, la transmisión a otros a sabiendas de su falsedad, su uso fraudulento y el establecimiento de sanciones efectivas, proporcionadas y disuasorias, que al menos en los casos graves deben ser privativas de libertad, de tal duración, que permitan la extradición.

En nuestro país, la tipificación específica de la falsificación, tenencia y/o uso a sabiendas de su falsedad de tarjetas de crédito, débito y cheques de viaje, de forma independiente de los comportamientos de similar naturaleza respecto de la moneda en sentido estricto, había sido reclamada desde amplios sectores de la doctrina penal y de la jurisprudencia, como específicamente se reseña en el Acuerdo de Pleno del Tribunal Supremo de 28 de junio del 2002 en el que la Sala Segunda sugería del órgano competente la utilización del artículo 4.3 del Código Penal para proponer al Gobierno de la Nación la conveniencia de tipificar en el Código Penal, de forma separada a la falsificación de moneda, los actos de falsarios relativos a tarjetas de crédito y débito y cheques de viaje y el establecimiento de penas adecuadas para cada supuesto.

De otro lado la definición y sanción de unos y otros comportamientos en preceptos diferentes se hacía también necesaria para solucionar definitivamente las discrepancias generadas en los últimos años en orden a la delimitación de las competencias para la instrucción y el enjuiciamiento de los procedimientos tramitados por delitos de falsificación de moneda, entendida esta, de acuerdo con la actual redacción del art. 387,

en un sentido amplio es decir asimilando a la moneda metálica y al papel moneda, las tarjetas de crédito, las de débito y las demás tarjetas que puedan utilizarse como medio de pago, así como los cheques de viaje.

Efectivamente a tenor de los artículo 65.1 b) y 89 bis párrafo 3.º de la LOPJ la competencia para la instrucción y enjuiciamiento de los delitos de falsificación de moneda se encuentra atribuida a los Juzgados Centrales y a la Sala de lo Penal de la Audiencia Nacional y si bien, en un principio el Tribunal Supremo, en Auto de fecha 23-XI-1998 estimó que la equiparación entre la moneda en sentido estricto y lo que se ha venido a llamar "dinero de plástico" lo era solo a efectos penales pero no procesales, posteriormente el criterio se modificó, tras el Acuerdo de Pleno de 28 de Junio del 2002 (en el que considera que la alteración de la banda magnética de las tarjetas de crédito y débito constituye un delito del art. 386 C.P), en virtud de Auto, entre otros de 24 de enero del 2003 que considera que dicha calificación delictiva produce necesariamente la competencia de la Audiencia Nacional ya que, según se razona, el "dinero de plástico" constituye un medio de pago cuya incidencia traspasa las barreras de las fronteras y ha exigido un tratamiento uniforme a nivel internacional a través de la Decisión Marco del Consejo de Ministros de la Unión de 28 de mayo del 2001.

Dicho criterio competencial fue asumido por otras resoluciones posteriores de la Sala Segunda del Tribunal Supremo tales como los ATS de 18-XI-2003 y 22-XII-2003 y 19-I-2004, si bien el Alto Tribunal se pronunció de forma discrepante en alguna otra resolución como el Auto de 19-IX-2003 en el que se mantiene el criterio tradicional de asignación del conocimiento de estos comportamientos a los Juzgados y Audiencias competentes territorialmente argumentando que es de todo punto evidente la existencia de una importante diferencia entre las tarjetas de crédito y la moneda metálica o papel moneda especialmente en lo que se refiere a su origen y al deber de protección respecto de los mismos. Este estudio comparativo se completa con la referencia al ATS de 24-IV-2004 que en orden a la delimitación de competencia entre los órganos territoriales y los correspondientes a la Audiencia Nacional distingue en atención a la imputación concreta de hecho delictivo, diferenciando si la imputación lo es por delito de fabricación o introducción de moneda falsa o si se trata de simple tenencia de efectos falsificados y con la cita del Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo, de fecha 5-V-2005 con el que se pretenden clarificar las discrepancias en esta materia.

En cualquier caso, la decisión del legislador de tipificar independientemente de la falsificación de moneda, los comportamientos delictivos relacionados con el llamado "dinero de plástico" y la propuesta de modificación, a través de la Disposición final primera del Anteproyecto, del artículo 65 de la L.O.P.J. según la cual corresponderá a los órganos de la Audiencia Nacional, el conocimiento entre otros de los delitos de "b) Falsificación de moneda y fabricación de tarjetas de crédito y débito falsas y cheques de viajero falsos, siempre que sean cometidos por organizaciones o grupos criminales" van a permitir dar por zanjada toda esta discusión doctrinal sobre competencia para la instrucción y enjuiciamiento de dichos procedimientos, al asignarse específicamente a dichos órganos centrales el conocimiento de las conductas falsarias consistentes en la fabricación (y no otros comportamientos típicos) de dichos efectos cuando concurra la circunstancia de que el delito se haya cometido por organizaciones o grupos criminales, correspondiendo en los demás casos la competencia a los órganos procedentes de acuerdo con los criterios ordinarios del artículo 14 y ss de la LECrim.

Además la tipificación independiente de las conductas ilícitas cuando tienen por objeto tarjetas y cheques de viaje, permitirá solucionar las cuestiones interpretativas que se han ido planteando en estos últimos años como consecuencia de la dudosa aplicación

de determinados comportamientos típicos definidos en el art. 386 C. Penal, a las actuaciones relacionadas con tarjetas de crédito, debito o cheques de viaje, tales como los consistentes en "expendición", "distribución", "tenencia para expendición", etc., conductas estás, previstas en relación con la moneda metálica o papel moneda pero difícilmente aplicables en los supuestos relacionados con el llamado "dinero de plástico".

Falsificación de tarjetas de crédito y débito y cheques de viaje (art. 399 bis)

Los comportamientos falsarios relacionados con las tarjetas de crédito, débito o cheques de viaje se tipifican en el art. 399 bis del Anteproyecto, antes mencionado, cuyo tenor literal es el siguiente:

1. Será castigado con la pena de prisión de cuatro años a ocho años el que falsificare, copiándolos o reproduciéndolos, tarjetas de crédito o débito o cheques de viaje. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o los hechos fueran cometidos en el marco de una organización criminal dedicada a estas actividades.

Los Jueces y Tribunales impondrán a la organización, bien como penas si procediere la declaración de su responsabilidad penal de acuerdo con lo dispuesto en el artículo 31 bis de este Código, bien como medida en los casos previstos en el artículo 129, la disolución y clausura definitiva de sus locales y establecimientos.

2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados en cantidad que permita suponer están destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación.

3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de dos a cinco años.

La primera cuestión que llama la atención al examinar este precepto es que el Anteproyecto se refiere exclusivamente a las tarjetas de crédito, debito o cheques de viaje, omitiendo cualquier referencia a "las demás tarjetas que puedan utilizarse como medio de pago", que como ya indicamos habían sido incorporadas al texto actual del art. 387 por la L.O. 15/2003 equiparándolas a las primeramente indicadas, sin que dicha omisión haya sido justificada en forma alguna por el legislador en la Exposición de Motivos del anteproyecto y sin que acertemos a explicar esta circunstancia.

Al describir el comportamiento típico, sorprende la técnica que el prelegislador utiliza para describir la conducta típica en el apartado primero, ya que parece referir la falsificación a los supuestos de copia o reproducción, sin incluir referencia alguna a otros supuestos, como por ejemplo, los de alteración del documento original en alguno de sus elementos esenciales pese a que una de las conductas que con mayor frecuencia es objeto de valoración por los órganos judiciales en relación con la falsificación de estas tarjetas, es precisamente la modificación u alteración de su banda magnética, manteniendo el soporte inicial. Ciertamente una interpretación amplia del concepto de falsificación acorde con la dicción del art. 390, permite fácilmente despejar estas dudas pero es evidente que la redacción del precepto puede inducir a error sobre los comportamientos típicos, por lo que sugerimos una previsión más amplia y clara en la descripción de conductas en el tipo básico.

Por otra parte, el Anteproyecto opta por una penalidad para estos delitos sensiblemente más leve que para el tipo penal en el que en el momento presente se incardinan estos comportamientos, delito de falsificación de moneda, que en sus modalidades de fabricación, alteración, introducción o exportación de moneda falsa, transporte, expendición o distribución en connivencia con el falsificador, introductor o exportador,

está actualmente castigado con pena de prisión de 8 a 12 años y multa del tanto al cuádruplo del valor aparente de las monedas. Este criterio penológico que se promueve en el anteproyecto se considera adecuado dado que como amplios sectores doctrinales han tenido ocasión de manifestar, estos documentos, dada su naturaleza y origen, no se hacen merecedores de un nivel de protección idéntico al establecido para la moneda de curso legal, especialmente en los supuestos menos trascendentes, sin perjuicio de lo cual y precisamente para sancionar con mayor rigor los supuestos más graves, se contempla en el inciso segundo del párrafo primero la imposición de la pena en su mitad superior, cuando resulten afectados por el delito una generalidad de personas o el mismo se cometa en el seno de una organización criminal dedicada a estas actividades.

Esta decisión, por otra parte, es acorde con la Decisión Marco citada anteriormente, que recordemos no propugnaba ni aconsejaba la equiparación de sanciones sino únicamente que estas fueran efectivas, proporcionadas y disuasorias, apuntando únicamente la procedencia que algunas de ellas, las más graves, estuvieran sancionadas con pena privativa de libertad que pueda dar lugar a la extradición

También es loable la previsión del apartado segundo del mismo párrafo de acordar, respecto de la organización bien como penas, si se la considera responsable penal por ostentar personalidad jurídica, o bien como medida al amparo del artículo 129, su disolución o la clausura definitiva de sus locales o establecimientos.

En los párrafos segundo y tercero se sancionan respectivamente, la tenencia de tarjetas y cheques de viaje falsificados si estuvieran destinados a la distribución y el mero uso de estos efectos sin haber tomado parte en la falsificación.

El primero de los supuestos resulta impreciso en la definición del comportamiento típico. Si lo que se pretende sancionar es la mera tenencia de estos efectos con la finalidad de distribuirlos o traficar con ellos, al igual que ocurre con similar conducta en el artículo 386 Código Penal en referencia al papel moneda o moneda metálica, resulta perturbadora la referencia a la cantidad de tarjetas o cheques de viaje falsos poseídos, pues puede darse la circunstancia de que aun no ocupándose un número importante de estos efectos, concurran otras circunstancias que por si mismas acrediten dicha tenencia preordenada al tráfico o distribución. Es por ello que estimamos más aconsejable la tipificación de este comportamiento exigiendo exclusivamente que su destino sea la distribución o el tráfico de los efectos falsificados, con idéntica técnica a la empleada en el artículo 386 sin perjuicio de establecer, si así se estima oportuno, que dicha finalidad puede deducirse de la cantidad de efectos falsos incautados en poder del imputado.

La comparación con el artículo 386 del Código Penal nos obliga a efectuar una última reflexión a propósito de este nuevo precepto ya que a diferencia de lo previsto a propósito de la falsificación de moneda, en relación con la cual la tenencia preordenada a su expedición o distribución se sanciona con pena inferior en uno o dos grados a la correspondiente a los falsificadores, en este nuevo precepto se equiparan a efectos punitivos ambos comportamientos. Esta circunstancia supone que en los supuestos de tenencia, la pena prevista por el legislador resulte desproporcionada a la gravedad del hecho, si la comparamos con la establecida para los autores de la falsificación y con la previsión punitiva del artículo 386 para los detentadores de moneda falsa.

En cuanto a los comportamientos de mero uso, el legislador exige como elementos del tipo, el conocimiento de la falsedad y la actuación en perjuicio de tercero, equiparando a estos efectos la utilización de las tarjetas de crédito, debito o cheques de viaje al uso de documentos públicos, oficiales o mercantiles falsos, por parte de quien no haya tomado parte en la falsificación».

VII. **La compleja determinación de la responsabilidad civil**

Aun cuando este epígrafe no contempla supuestos que en su totalidad pueden ser considerados como estafa informática (sí lo serían el uso de tarjeta en cajero o en terminales en establecimientos comerciales creados a tal efecto o en connivencia con el titular o el empleado de un establecimiento; no lo sería el uso de tarjetas falsas en establecimientos comerciales que ha de reputarse estafa común) he considerado que las dificultades que en la práctica suscita la formulación de la petición de responsabilidad civil en todos estos casos merecía su tratamiento en un epígrafe separado.

La responsabilidad civil que se deriva del uso indebido de tarjetas de crédito por terceros es una cuestión poco pacífica en sede de Audiencias Provinciales, tanto en el orden jurisdiccional penal como en el civil.

Las relaciones jurídicas que soportan la emisión y uso de la tarjeta de crédito son sumamente complejas. Por ello, se plantean múltiples interrogantes respecto de quién sea el sujeto perjudicado por una acción delictiva en la que medió el uso de una tarjeta de crédito. Concurre un evidente interés entre las personas que intervienen en la relación contractual y comercial que genera la emisión y utilización de la tarjeta en no ser considerado perjudicado por la posible utilización delictiva por un tercero. En otras palabras, se da una lucha de intereses, generalmente entre el banco y el cliente, por evitar ser, en definitiva, quien haya de soportar el perjuicio patrimonial derivado de la posible insolvencia del sujeto activo del delito.

Los criterios para reputar perjudicado a uno u otro de los intervinientes en sede de responsabilidad civil derivada de delito, y si esos criterios pueden verse alterados posteriormente en reclamación interna en sede civil, constituyen interrogantes de enorme enjundia práctica.

Del análisis de la jurisprudencia menor dictada al efecto, cabe indicar que la respuesta es sumamente casuística, resolviéndose según las circunstancias concurrentes, los sujetos parte en el procedimiento y la prueba que, en su caso, dichos sujetos puedan aportar en defensa de sus posturas.

Desde una perspectiva económica, como pone de manifiesto la sentencia civil de la Audiencia Provincial de Castellón, Sección 2.ª, de 12 de Febrero de 2000:

> «en el uso de las tarjetas de crédito se parte de una constatación innegable: existe un riesgo derivado de la emisión de tarjetas y su utilización. Riesgo de que la tarjeta se extravíe o sea robada, o duplicada, utilizada fraudulentamente, en suma, y con ello, se obtenga un beneficio

económico —bien la extracción de dinero en cajero automático, bien la adquisición de bienes en comercios—. Y de ello, indudablemente, deriva un perjuicio, que puede afectar al titular, al emisor, y al mismo propietario de la marca; puede ocurrir, también, que algún elemento de la relación contractual, ciertamente compleja, a tres, cuatro bandas, valga la expresión, ya sea personal, ya sea mecánico del sistema, no actúe o lo haga defectuosamente…».

1. *Dos planos diferentes en la determinación del sujeto perjudicado*

La consideración como delito de las conductas que analizamos conlleva que la responsabilidad civil que se examina sea la responsabilidad *ex delicto.*

Por ello, conviene, en primer lugar, reparar en dos cuestiones esenciales que se corresponden con dos planos distintos que inciden en el tratamiento de dicha responsabilidad.

Primero, desde el plano jurisdiccional penal interesa, primeramente, establecer quién sea el propietario del dinero o de los efectos obtenidos con la acción delictiva. En definitiva: a quién se ha estafado, robado o hurtado *su dinero.* Ese será el sujeto pasivo y primer perjudicado por el delito.

Segundo, en ese plano jurisdiccional penal, relativo a la fijación del sujeto pasivo, como titular del bien jurídico atacado, sin embargo, pueden incidir las complejas relaciones contractuales entre las diferentes personas que intervienen como partes en la emisión y funcionamiento de una tarjeta. Del incumplimiento de sus obligaciones puede resultar que la pérdida del dinero por su propietario haya de ser soportada finalmente por otra persona, en una especie de traspaso del perjuicio desde el sujeto pasivo al finalmente perjudicado. Y esa determinación, propia de las relaciones internas entre las partes contratantes y ajenas al delito y al delincuente, se dilucidará en ocasiones en vía penal, aunque no necesariamente siempre.

Es posible que en vía penal se considere perjudicado al propietario del dinero, sin entrar en otras consideraciones, y que éste, generalmente ante la insolvencia del autor del delito, se dirija, en vía civil y por relaciones contractuales internas, a solicitar indemnización contractual a alguna otra de las partes intervinientes en las relaciones mercantiles derivadas de la emisión y uso de una tarjeta. En tales casos, se siguen consecutivamente dos procedimientos: penal y civil, por ese orden (art. 114 LECrim), con ámbitos de decisión diferentes: en vía penal se señala quién es el estafado o robado, quién es el dueño del dinero defraudado o sustraído;

en vía civil se ventila la acción de repetición de dicha persona frente a otra por el posible incumplimiento de sus obligaciones en los contratos que rodean la emisión o uso de la tarjeta.

No obstante, también es posible —de hecho resulta frecuente— que en la vía jurisdiccional penal se resuelvan ambas cuestiones conjuntamente. Es decir, que el juez penal entre a conocer de los dos planos señalados —no sólo del primero— y decida atribuir la condición de perjudicado no al propietario del dinero sino a otro de los intervinientes (titular de la tarjeta, establecimiento comercial, emisor de la tarjeta). En ese caso, la cuestión le viene resuelta al juez civil en una eventual futura reclamación. Esto es lo que sucedió en el caso que resuelve la sentencia civil de la AP de Zaragoza, sección 4.ª, 239/1999, de 13 de abril. Los hechos que dieron lugar al mismo son los siguientes: en sentencia penal firme se condena a dos personas por la utilización de una tarjeta ajena en establecimientos comerciales originando un saldo deudor de 327.000 ptas. a las penas correspondientes por los delitos de estafa y falsedad, y a indemnizar en tal cantidad a la titular de la tarjeta, a quien se consideró por la sentencia penal como perjudicada. El Banco, ante el hecho de que la titular cerró la cuenta sin saldar dicho descubierto, demandó en vía civil a la titular el reintegro de aquella cantidad. La sentencia señala: «… en el referido procedimiento penal se ejercitó juntamente con la acción penal, la civil derivada de delito, que no fue renunciada ni reservada expresamente para ejercitarla después, con lo que quedaron definitivamente resueltas las responsabilidades civiles nacidas de la infracción penal, para cuyo conocimiento tienen competencia los tribunales penales», y, con invocación de la STS 24 de octubre de 1988, dispone que la sentencia penal ya ha resuelto sobre la condición de perjudicada por la acción delictiva de la titular y, en consecuencia, la condena a reintegrar a la entidad bancaria la cantidad que a ella le fue defraudada por el hecho delictivo.

A raíz de los dos planos expuestos se hace necesario analizar, de una parte, quien es el propietario del dinero defraudado; de otra, cómo inciden las relaciones contractuales subyacentes en la emisión y empleo de una tarjeta. A ello se dedican los apartados siguientes. En todo caso, debe dejarse señalado, como ya se apuntó, que las soluciones dadas en la práctica judicial han sido muy dispares[26].

[26] Encontramos pronunciamientos dispares en sede de nuestras Audiencias, respecto de quién asume esta condición. En unos casos abogan por la condición de perjudicado del titular y en otros, por la condición de perjudicado de la entidad bancaria o de VISA. Prueba de estas posturas divergentes, son los pronunciamientos que se relacionan a continuación.

2. *Determinación del propietario de los efectos defraudados*

El sujeto pasivo del delito, en cuanto titular del bien jurídico protegido, será el propietario del patrimonio defraudado. Su determinación conlleva importantes consecuencias, entre las cuales cabe señalar, por ejemplo, la de la aplicabilidad o no de la excusa absolutoria entre determinados parientes del art. 268 CP. En este sentido, si el sujeto pasivo es la entidad bancaria y no el titular de la cuenta corriente, será indiferente, a los efectos del art. 268, la posible existencia de parentesco entre el autor del delito y el titular de la tarjeta, ya que el delito se habrá producido respecto de un sujeto pasivo distinto, ajeno a la relación parental. Una interesante STS sobre la cuestión es la STS 1476/2004, de 21 de diciembre, ya antes comentada[27].

La sentencia de la Audiencia Provincial de Tarragona, de 8 de junio de 1998, condenó por estafa y por robo con fuerza en las cosas, declarándose probado que el dinero cargado en la tarjeta Visa fue reintegrado por VISA ESPAÑA a su titular. Ambos acusados debían responder civilmente de la cantidad defraudada frente a VISA.

La sentencia de la Audiencia Provincial de Santa Cruz de Tenerife, de 7 de abril de 2000, condena a los responsables de los delitos cometidos de estafa y falsedad documental con tarjeta de crédito a indemnizar a terceros perjudicados por las infracciones, debiendo abonar, solidariamente, entre ellos a las entidades Sistema 4B, S.A. y Central de Medios de Pago Visa, las cantidades defraudadas y los intereses generados.

La Audiencia Provincial de Barcelona, con fecha 5 de abril de 1998, dictó sentencia por la que declaraba como hechos probados que el condenado coge un bolso con la tarjeta a la que acompañaba una cuartilla de papel en el que figuraba el número secreto de a misma, con la cual se hicieron reintegros en un cajero automático y adquisiciones en establecimientos. La entidad bancaria no había reintegrado a la titular de la tarjeta el importe de las extracciones. La sentencia condena al acusado a entregar la cantidad extraída, recuperada en las actuaciones, a la perjudicada, titular de la tarjeta, como restitución de la suma sustraída.

La sentencia de la Audiencia Provincial de Granada, de 22 de diciembre de 2001, estimó que perjudicados por los pagos efectuados mediante tarjeta de crédito son los vendedores o comerciantes que resultaron engañados si la Caja no les abonó el importe de las facturas, o la propia Caja si les hizo el abono inmediatamente.

[27] En la citada sentencia, que recordemos enjuiciaba el caso de dos jóvenes que desde la tienda de la madre de uno de ellos utilizan el terminal de venta para efectuar devoluciones de supuestas compras por 52 millones de ptas. que se abonan en la cuenta de uno de los acusados, señala la sentencia no aplicable la excusa absolutoria del art. 268 pretendida por el acusado hijo de la dueña del comercio ya que «el perjudicado ha sido el Banco y por lo tanto es el sujeto pasivo del delito. Consecuentemente, queda excluida la posible aplicación del art. 268 CP. Las discusiones que puedan haber existido entre el Banco y los usuarios de la terminal electrónica empleada por los acusados sobre si la madre del acusado debía asumir el daño civil producido por el delito, no afecta en absoluto el hecho de que el delito haya tenido por lo menos dos sujetos pasivos y que el Banco haya sido uno de ellos, ya que, en todo caso, el carácter litigioso de una suma importante que pudo haber pesado sobre el patrimonio del Banco es ya constitutivo de un daño patrimonial.

El contrato por el que se obtiene la tarjeta no funciona de forma autónoma sino que se vincula o necesita de una cuenta a través de la cual se produce una apertura de crédito. Esta cuenta funciona como una cuenta bancaria, en la que el emisor lleva la cuenta corriente del titular, refleja un saldo y remite un extracto periódico comunicando dicho saldo.

De ese modo, la tarjeta de crédito se vincula a un contrato de cuenta corriente bancario, contrato que tiene carácter autónomo respecto de los contratos a los que sirve de soporte; de modo que los ingresos realizados por el titular en metálico conservan las peculiaridades propias de un contrato de depósito irregular, por el cual, al quedar el dinero depositado confundido con el patrimonio del depositario, éste, es decir, la entidad bancaria, ha de soportar los riesgos derivados de su deber de conservar la cosa depositada.

Conforme al contrato de cuenta corriente, el Banco presta un servicio de caja, que supone el cumplimiento por su parte de las órdenes que el cliente puede darle de acuerdo a los usos bancarios. El depósito de numerario en cuenta corriente hecho por un cliente es para el banco una operación pasiva, de modo que éste recibe en concepto de depósito irregular un dinero ajeno obligándose a retribuir al cliente depositario con un interés determinado y a realizar en su beneficio, si la cuenta es corriente y a la vista, un servicio de caja y gestión de los fondos.

Como ha venido señalando la Sala de lo Civil del Tribunal Supremo (entre otras, sentencias 4 de diciembre de 1975 y 11 de marzo de 1992), entre los variados tipos de depósitos bancarios, está aquél que comporta para el banco la obligación de devolver la suma depositada a petición del depositante y en el momento mismo en que éste lo exija, operación ésta que ha venido a denominarse en la técnica mercantil y bancaria, depósito en cuenta corriente, dándose la circunstancia de que, cuando ese depósito es de cosas fungibles, se le autoriza para disponer del objeto del depósito, con obligación de devolver otro tanto de la misma especie y calidad, generando entonces la figura del depósito irregular caracterizado por el hecho de que el depositario adquiere, desde el momento de la constitución de aquél, la propiedad de las cosas depositadas.

El hecho de que el depósito del dinero en la cuenta corriente por el titular de la tarjeta sea un depósito irregular es sumamente relevante, ya

---

De aquí se deduce que, aunque hayan sido los padres del acusado quienes hayan debido soportar en última instancia las consecuencias patrimoniales del delito, el hecho punible, como tal, se cometió contra el patrimonio del Banco. Es claro que la propiedad del dinero, que los cuentacorrentistas ingresan en sus cuentas y que, por lo tanto, se encuentra en poder del Banco, forma parte del patrimonio de éste y no del de los titulares de las cuentas (arts. 1753 y 1768 Código Civil)».

que, conlleva que, desde el momento mismo de la entrega del dinero, éste pasa a ser propiedad de la entidad bancaria, la cual se obliga a devolver el *tantundem* y, por tanto, en el supuesto de que entregue dicho dinero a una persona no idónea, a la cual no tenía obligación de realizar el pago, por no existir orden expresa del titular de la cuenta, correrá con los riesgos y daños derivados de dicha entrega[28].

En el mismo sentido y conforme a lo establecido en los artículo 1156 y siguientes del Código Civil, se ha de entender que, desde la perspectiva del pago como modo de extinción de las obligaciones, el hecho de que se entregue una cantidad de dinero a una persona no idónea para recibirlo, no produce dicho efecto extintivo. Concretamente, los artículo 1162, 1163 y 1164 del Código Civil determinan que para que el pago sea válido, se ha de hacer a persona en cuyo favor estuviese constituida la obligación, o a otra autorizada, a un tercero (en cuanto fuese de utilidad para el acreedor), o al que estuviese en posesión del crédito (siempre que se realice de buena fe).

De modo que, si el pago se realiza a una persona diferente a las relacionadas en los artículo mencionados, no se considerará un pago válido ni, por ende, conllevará la extinción de obligación alguna.

En síntesis, la obligación del depositario de devolver al depositante la cosa depositada (artículo 1766 Código Civil y 306 del Código de Comercio) se extingue por el pago, requiriéndose para que éste sea eficaz que se haga a la persona en cuyo favor estuviese constituida la obligación o a otra autorizada para recibirla en su nombre, como señala el artículo 1162 del Código Civil, ya que, de no ser así, no se producirá dicho efecto extintivo. En el depósito irregular ni siquiera existe en el depositario, convertido en propietario, obligación de devolver la «cosa depositada», sino que ésta es de su propiedad y existe un derecho de crédito de un tercero sobre su valor.

Por ello, en el supuesto de que la entidad bancaria, en su calidad de depositario, entregue el dinero depositado en la cuenta corriente en cuestión (dinero que es de su propiedad) asume el riesgo de que dicha cantidad se entregue a persona no idónea o de que se le esté dando un

[28] Dichas consecuencias derivan de lo dispuesto en los artículo 306 y 307 del Código de Comercio, relativos al depósito mercantil. Conforme al artículo 306 del Código de Comercio, en la conservación del depósito responderá el depositario de los menoscabos, daños y perjuicios que las cosas depositadas sufrieren por su malicia o negligencia. Respecto a los riesgos derivados de los depósitos de numerario, establece el artículo 307 del Código de Comercio, que correrán a cargo del depositario, siendo de cuenta del mismo los daños que sufrieren, a no probar que ocurrieron por fuerza mayor o caso fortuito insuperable.

uso indebido y fraudulento, de modo que, de producirse dichas circunstancias, debe reintegrar el importe que se ha extraído de la cuenta del titular depositante de forma automática, asumiendo las consecuencias de los pagos realizados[29].

3. *Incidencia de las relaciones contractuales en la consideración última del sujeto perjudicado.*

A) Breve referencia al concepto de tarjeta de crédito. Sujetos implicados en su emisión y posterior uso

La tarjeta de crédito en sí misma, es un documento emitido por una entidad mercantil como instrumento de pago en sustitución del dinero, cuya concesión por la entidad bancaria deriva de relaciones contractuales plurales en cuanto están implicados, además del titular-usuario y del banco distribuidor, la entidad emisora (da denominación a la tarjeta) y el establecimiento donde se utiliza para la adquisición de bienes o servicios.

Como punto de partida, se ha de señalar que la tarjeta de crédito, en palabras de la sentencia del Tribunal Supremo de fecha 22 de diciembre de 1998 tiene una «escasa o nula regulación legal, pese a los años que ya lleva funcionando, se rige por las normas establecidas por las entidades que las emiten como un caso más y con las limitaciones propias de las condiciones generales en los contratos de adhesión, cuyo titular puede utilizarla con distintas finalidades».

Existen concretas referencias en nuestra legislación a la tarjeta de crédito como las previstas en los artículo 2 y 15 de la Ley 7/1995, de 23 marzo, sobre Crédito al Consumo, y el artículo 46 de la Ley 7/1996, de 15 enero, de Ordenación del Crédito Minorista; sin perjuicio de su sometimiento a la normativa bancaria, a los pronunciamientos dictados por el Servicio de Reclamaciones del Banco de España, a la Ley 7/1998, de 13 abril, sobre Condiciones Generales de la Contratación, así como a la normativa comunitaria.

---

[29] En relación con la estafa cometida a través de cheque, la consideración del depósito irregular sustenta esta misma postura: es el banco el perjudicado por el pago del cheque mendaz, en tanto propietario del dinero, y no el titular de la cuenta corriente salvo que le sea derivable el daño al mismo por incumplimiento de alguna obligación contractual. En dicho sentido se expresa el art. 156 de la Ley Cambiaria y del Cheque, de 16 de julio de 1985: «El daño que resulte del pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido negligente en la custodia del talonario de cheques o hubiera procedido con culpa». Vid. SSTS, Sala 2.ª, de 15 de febrero de 1986 y 23 de septiembre de 1986, entre otras, reputando perjudicado al banco librado.

En la normativa comunitaria existen diversas Recomendaciones en cuanto a buenas prácticas acerca de la utilización de las mismas, entre las que destacamos la Recomendación 88/590/CEE de la Comisión, de 17 de noviembre de 1988, relativa a los sistemas de pago y, en particular, a las relaciones entre los titulares de las tarjetas y los expedidores de las mismas[30], y la Recomendación de la Comisión, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos, así como un Código de Buena Práctica de la Banca Europea sobre sistemas de pago mediante tarjeta aprobado por la Federación Bancaria de la Comunidad Económica Europea, de 14 de noviembre de 1990.

A efectos de analizar el presente apartado, se hace necesario, primeramente, determinar los múltiples sujetos implicados en la emisión y uso de una tarjeta de crédito; sujetos que se encuentran unidos por diversos contratos, dando lugar una relación jurídica compleja.

—*El emisor,* será aquel empresario que libre la tarjeta de crédito a cambio de una comisión económica fija y directa o bien variable en función del beneficio obtenido por la misma. La Recomendación 88/590 UE, de 17 de noviembre de 1988, relativa a los sistemas de pago, define al emisor como la persona que, en el marco de su actividad profesional, pone a disposición de un cliente un instrumento de pago, en virtud de un contrato suscrito con él.

—*El titular de la tarjeta,* será aquélla persona física o jurídica que contrata la emisión y uso de la tarjeta de crédito y los servicios complementarios que el emisor ofrece a cambio de una comisión. A este respecto, destacamos la posibilidad de que exista un titular contratante, pero los beneficiarios sean diversos, como es el caso de las tarjetas de empresa.

—*El establecimiento comercial*, aceptante de la tarjeta, será aquella persona física o jurídica que contrata o con el emisor o con un tercero que le presta el servicio de pago y que, en virtud de dicho contrato, acepta la tarjeta como instrumento de pago.

[30] La Recomendación contempla la adopción de normas comunes por lo que se refiere a la responsabilidad del expedidor: (i) por el incumplimiento o el mal cumplimiento de las órdenes de pago o de las operaciones conexas de un titular contratante; (ii) por las operaciones que no hayan sido autorizadas por el titular contratante bajo reserva de que este último cumpla las obligaciones que le incumben en caso de pérdida, robo o reproducción de su medio de pago. (iii) El contrato entre el emisor y el titular debe precisar también qué consecuencias tendrá para este último la pérdida, el robo o la falsificación de su medio de pago.

—*La entidad bancaria* que, normalmente, negocia con los establecimientos comerciales la admisión del sistema de tarjeta, asume la deuda y la obligación de liquidarles las operaciones y, en definitiva, se instituye como representante del sistema de tarjeta. Normalmente, existe una entidad de crédito con la que el titular o el aceptante han suscrito un contrato de cuenta corriente, por el cual, el primero tiene domiciliados los pagos de las comisiones, obtención de dinero a través de cajeros automáticos y pagos a establecimientos comerciales y el segundo tiene domiciliados el importe de las operaciones comerciales que se realizan en su establecimiento.

Tras esta breve definición de los sujetos que intervienen en el uso de la tarjeta de crédito, simplemente hacemos mención a la necesidad de atenerse en sus actuaciones a la Recomendación 87/598/CEE de la Comisión, de 8 de diciembre de 1987, por la que se aprueba el código europeo de conducta referente a los pagos electrónicos, cuyos objetivos son dar seguridad y comodidad a los consumidores y mayor seguridad y productividad a los prestadores de servicios y emisores.

B) Obligaciones de las partes derivadas del contrato de tarjeta. Importancia de su observancia a efectos de determinar la responsabilidad civil

En virtud del contrato de tarjeta de crédito, las partes contraen unas obligaciones mínimas que han de observar, cuyo incumplimiento puede derivar en su perjuicio la correspondiente responsabilidad civil.

a) Obligaciones del emisor[31]

Destacan, genéricamente, la de limitar el riesgo en el uso de la tarjeta de crédito, tanto de los titulares como de los establecimientos comerciales afiliados a dicho sistema de pago; la de adoptar medidas para

[31] La Recomendación de la Comisión, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos mencionada anteriormente, establece que el emisor queda sujeto a ciertas obligaciones, entre las que cabe destacar las siguientes: (i) abstenerse de revelar el número de identificación personal del titular a cualquier otra persona; (ii) abstenerse de enviar al titular un instrumento electrónico de pago no solicitado; (iii) conservar un registro interno de las transacciones a que se refiere la Recomendación; (iv) asegurarse de que el titular dispone de medios adecuados para realizar la notificación prevista en la Recomendación en caso de robo, extravío o error; (v) en caso de litigio con el titular, demostrar que la transacción ha sido correctamente registrada y contabilizada y no se ha visto afectada por un incidente técnico o de otro tipo.

prever y evitar el uso fraudulento de la tarjeta y la de actuar con rapidez tras el aviso de extravío o sustracción.

Más concretamente, en primer lugar, la entidad bancaria ha de cuidar, no sólo de que llegue la tarjeta a su titular, sino también de que reciba el número clave para su utilización, evitando que, por cualquier circunstancia, la tarjeta no llegue al receptor. Evidentemente, se entenderá que la entidad bancaria es responsable[32] de aquellas disposiciones que se realicen a través de tarjetas que no han llegado a sus titulares. Será perjudicado el banco emisor en aquellos supuestos de actuaciones de empleados de oficinas bancarias que se han apoderado de tarjetas de crédito a las que acompañaban el número de clave secreto, o en supuestos de hurtos de las tarjetas y sus claves por terceros en las propias oficinas bancarias.[33]

Se plantean en este punto ciertas dificultades ante casos en que el titular alega que no ha recibido la tarjeta y que se le están cargando en cuenta diversos importes de cargos que no ha efectuado el mismo. La entidad bancaria se encuentra entonces ante la tesitura de probar que la tarjeta llegó a su titular y fue utilizada por éste. Para evitar dar cabida a estas conductas, es una garantía de entrega la remisión de la tarjeta por correo certificado, de forma separada al PIN. En todo caso, existe una presunción de uso por el titular que deriva de la recepción por éste de la tarjeta, de la identificación a través del número secreto y de la ausencia de comunicación de robo o extravío. En este sentido, la sentencia civil de la sección 1.ª de la AP Navarra, 6/1999, de 20 de enero, resuelve un caso de esta naturaleza: el cliente pretendía de la entidad que le fuera

---

[32] La Recomendación de la Comisión, de 30 de julio de 1997 establece que el emisor de un instrumento electrónico de pago es responsable: (i) de la no ejecución o la ejecución incorrecta de las transacciones contempladas en la Recomendación; (ii) de las transacciones efectuadas sin la autorización del titular y de cualquier error o anomalía en la gestión de su cuenta atribuible al emisor. El emisor responderá en tal caso por: (i) el importe de la transacción no ejecutada o ejecutada incorrectamente; (ii) el importe necesario para colocar al titular en la situación en que se encontraba antes de la transacción no autorizada.

El emisor de un instrumento de dinero electrónico se considerará responsable de la pérdida del valor contenido en el mismo o de las operaciones incorrectas efectuadas por el titular, cuando la pérdida o la ejecución incorrecta se deban a una disfunción del instrumento, del dispositivo, del terminal o de cualquier otro equipo homologado, siempre que dicha disfunción no haya sido provocada deliberadamente por el titular.

[33] La sentencia civil de la Audiencia Provincial de Málaga, sección 4.ª, de 9 de septiembre de 1994, resolvió que el Banco era responsable por negligencia y ello, por aplicación de lo dispuesto en los artículo 1103 y 1104 del Código Civil, en la medida que puso a un tercero en poder de la clave de identificación, así como de la tarjeta renovada, sin que conste probado que llegara al titular.

reintegrado el importe del cargo en su cuenta por utilización de la tarjeta en cajeros, argumentando que la tarjeta no llegó a su poder al haber incurrido en negligencia el banco al remitírsela. La sentencia desestima la pretensión sosteniendo que:

> «no considera la Sala que, a los efectos de excluir un actuar negligente en la entrega de las tarjetas, deba la entidad bancaria demostrar físicamente el uso de la tarjeta por el titular de la misma, pues precisamente la tarjeta de crédito a través del código en ella incorporado, facilita un medio de operación bancario en que la identidad física queda relativizada, sustituyéndose el control de autenticidad del usuario, por la tenencia (remitida personalmente) de la tarjeta y el número secreto, que permite su utilización con garantía».

De otra parte, de acuerdo con los modelos de condiciones generalmente establecidos, una vez recibida la tarjeta por el titular, se excluirá la responsabilidad del emisor cuando el titular de la tarjeta haya actuado con dolo o negligencia en el cumplimiento de sus obligaciones (entre otras, custodia de la tarjeta o de la clave o número secreto que permite la utilización de la misma); si bien, recayendo la carga de la prueba en la entidad emisora y no en el perjudicado. Es decir, es el emisor quien habría de probar, en su caso, que el titular ha actuado con negligencia o dolo en el cumplimiento de sus obligaciones.

Finalmente, la entidad emisora ha de tener un sistema en el que queden constancia de las operaciones (registro interno de las transacciones llevadas a cabo con cargo a las tarjetas) y probar que las operaciones registradas son reales, es decir, que no se ha producido un fallo en el sistema informático. En este sentido, la sentencia del Tribunal Supremo de fecha 21 de diciembre de 2001, ante un caso en que la titular de la tarjeta afirmó no haber conocido los suministros cuyo pago se reclamaba, considera que corresponde a la entidad bancaria probar la realidad de las operaciones concertadas tanto con el establecimiento adherido como con el emisor, efectuadas con las tarjetas de crédito emitidas por los mismos.

Por medio del número PIN se podrá identificar las órdenes de entrega de mercaderías y servicios y se confirmará su recepción, ocurriendo lo mismo con los datos registrados a través de la cinta magnética de la tarjeta, respecto del producto o servicio adquirido. Así, al quedar constancia de las operaciones concertadas, tanto en el establecimiento adherido como en el emisor es, a través de la aportación de los datos contenidos en estos registros, como se podrá reclamar de los pagos que no se han satisfecho voluntariamente por los beneficiarios de los mismos. Si surge una controversia entre el titular y emisor, este último ha de demostrar

que la operación discutida había sido correctamente registrada y contabilizada, no resultando afectada por una avería técnica o de otro tipo. Por tanto, la entidad emisora habrá de aportar los soportes magnéticos o justificantes de uso de tarjetas (datos facilitados por establecimientos adheridos con las respectivas facturas).

b) Obligaciones del titular

1.º *Firma de la tarjeta*

La primera obligación exigible al titular, es que, de forma inmediata a la recepción de la tarjeta, proceda a estampar su firma en la misma. Respecto de esta obligación, se plantea la cuestión de qué ocurre en los supuestos en los que una tarjeta que no ha sido firmada es usada de forma fraudulenta. Entendemos que si la misma ha sido utilizada indebidamente, tras la recepción del titular que no la firmó, podrá achacarse la responsabilidad al mismo por su negligencia al incumplir esta obligación.

2.º *Custodia de la tarjeta y del número secreto*

En todos los contratos de tarjeta de crédito, se exige al titular que custodie con diligencia la tarjeta y el PIN.

El PIN, como señala la sentencia del Tribunal Supremo de fecha 21 de Diciembre de 2001, constituye el número de identificación personal, número secreto o número clave, elemento que suple a la exhibición del DNI y a la firma autógrafa del titular de la tarjeta, y permite (eventualmente, incluso a quien no sea su titular, si cuenta con la pertinente autorización habiéndosele facilitado el documento y el dato numérico) la obtención de servicios, bienes o dinero a través de máquinas.

Los contratos suelen incluir una cláusula por la cual se obliga el cliente a conservar diligentemente la tarjeta y a evitar que su Número de Identificación Personal (PIN) sea conocido por nadie. Actualmente, se puede observar la introducción de cláusulas más elaboradas a este respecto en las que se exige que los titulares no anoten el PIN en la tarjeta ni en ningún documento que acompañe a la misma, así como a no utilizar como tal, datos o fechas obrantes en documentos de uso habitual.

También se prevé que, en caso de utilización de la tarjeta conjuntamente con el PIN, no será de aplicación la cláusula de exención de responsabilidad, salvo que el cliente demuestre que cedió él mismo bajo coacción.

Indudablemente, la disposición de dinero mediante la introducción del número PIN correcto, conllevará una presunción de que se ha utili-

zado la misma por su titular legítimo. Sin embargo, no podemos ignorar que hoy en día, dados los avances tecnológicos e incluso los métodos sofisticados que se van utilizando, es posible averiguar el número de identificación y utilizarlo correctamente. Por tal motivo, en ningún caso, el uso del PIN correctamente acredita de forma automática la intervención del titular, ni cabe que se invierta la carga de la prueba en el titular.

Igualmente, resulta complicado enfrentarse al análisis de hasta qué punto ha de llegar la conservación del PIN «diligentemente». Así, se han dado innumerables casos en los que los tribunales se han tenido que enfrentar con la valoración de conductas de sujetos que habían apuntado el número del PIN en algún lugar y, por tal motivo, la tarjeta había sido utilizada con conocimiento del número secreto.

Así, sin perjuicio de las dificultades de prueba que pueden surgir a este respecto y a título de ejemplo, se analiza si es diligente la conducta de un sujeto que se la deja en el vehículo con el número (sentencia de la Audiencia Provincial de Bilbao de fecha 19 de diciembre de 1986 y sentencia de la Audiencia Provincial de Castellón de 12 de febrero de 2000[34]). En definitiva, la conclusión a la que se ha de llegar es que al sujeto no se le puede exigir que memorice el número o que lo lleve siempre encima, por lo cual, puede anotarlo, teniendo cuidado de que dicha anotación se realice de forma separada a la tarjeta.

El equivalente al PIN o firma de contrato, en el ámbito de la Banca telefónica sería el denominado CAP (Código de Acceso Personal), respecto al cual, el titular tiene, igualmente, una obligación de conservarlo. En el supuesto de robo, hurto, extravío o falsificación del soporte que lo contenga, se ha de comunicar al servicio de Banca Telefónica. En los contratos de tarjeta se suele estipular, que en el caso de que no se comunique el hecho, el Banco quedará relevado de cualquier responsabilidad que pueda surgir como consecuencia de las operaciones que se efectúen con el mismo.

3.º *Comunicación de la pérdida o sustracción de la tarjeta*

Una de las más importantes obligaciones que pesan sobre el titular es la de notificar, de inmediato, las incidencias ocurridas en relación con la tarjeta de crédito, tales como la pérdida, sustracción o copia de

[34] Afirma la sentencia de la Audiencia Provincial de Bilbao citada que no puede considerarse que dejar la tarjeta en el interior del vehículo suponga falta de diligencia en la custodia de la misma, pues es obvio, que no puede adquirir el compromiso de llevarla siempre encima. Por su parte, la referida sentencia de la Audiencia Provincial de Castellón declaró la concurrencia de conductas negligentes y, por tanto, atribuyó un tercio de responsabilidad al titular, y 2/3 a la entidad bancaria y a VISA.

la misma, el conocimiento indebido por otras personas del número de identificación secreto y cualquier error o discrepancia observado en los extractos comunicados por el Banco. Con carácter genérico, los titulares se obligan a adoptar las medidas necesarias que les permitan darse cuenta de haberse producido alguno de éstos hechos.

Del contenido de los contratos tipo que realizan las entidades bancarias españolas, se puede inferir que, en general, determinan la responsabilidad del emisor de forma similar al Código de Buenas Prácticas Bancarias. El punto de inflexión del funcionamiento del sistema se encuentra en que el titular queda exento de responsabilidad a partir del momento en que comunica la pérdida o robo de la tarjeta, bien a través de la Banca Telefónica de la propia entidad, bien en los teléfonos de Visa apuntados en el contrato.

Esta configuración de la responsabilidad se plasma en cláusulas tipo en las que se señala que el titular queda exento de toda responsabilidad desde que comunique la pérdida o robo de la tarjeta, a través de los medios puestos a disposición por la entidad. Antes de esta comunicación su responsabilidad queda limitada a 150 euros.[35]

A raíz de esta cláusula, la notificación del incidente delimitará la responsabilidad del titular. Así, hasta que se produzca la misma, en principio, el titular responde por un importe fijo que, actualmente, suele ascender a 150 euros, constituyendo la excepción a dicha regla los supuestos en que actúe el sujeto con negligencia grave o de forma fraudulenta.

Si esta comunicación es inmediata, señalan algunas cláusulas, ni siquiera tendrá el titular que hacer frente a este límite de 150 euros.

La comunicación de sustracción de la tarjeta conlleva una serie de interrogantes, no sólo respecto del modo en que hay que realizarla, el plazo en el que se ha de efectuar, a quién se ha de comunicar, sino también y como punto más importante, qué ocurre si no se comunica, bien porque no se ha detectado o bien porque se ha detectado pero han transcurrido muchos días desde que ocurriera el extravío o robo.

El plazo en el que se ha de comunicar ha de ser de forma inmediata[36] al conocimiento del robo o extravío. No obstante, razonablemente,

---

[35] La mayoría de entidades de crédito han utilizado como medio de publicidad y captación de clientes en uso de tarjetas especiales como las «oro» o «platino», la reducción de este límite de responsabilidad general, dejándolo en cuantías insignificantes, meramente representativas.

[36] El término «inmediato» es ciertamente indeterminado. La sentencia civil de la Audiencia Provincial de Alava, sección 1.ª, de 13 de septiembre de 2001, consideró patente la absolución de la entidad bancaria codemandada debido al actuar negligente del titular de la tarjeta quien no puso en su conocimiento la sustracción de la misma hasta 21 días después.

hay que entender que la advertencia de dichos incidentes, en muchos casos, es tardía, por las propias circunstancias del titular, lo que no se puede implicar una asunción automática de responsabilidad.

La sentencia civil de la Audiencia Provincial de Madrid, sección 9.ª, de 8 de abril de 1999, condenó al Banco por extracciones hechas 10 minutos antes de que se comunicara que la tarjeta había sido extraviada. El Banco defendía que como habían sido anteriores a la comunicación, eran responsabilidad del titular. La entidad bancaria fue condenada sobre la base de que la tarjeta no es segura y de que es fácil extraer el número secreto de la banda por personas expertas, de modo que no podía imputarse a la negligencia del titular, los cargos efectuados con la misma.

La prueba de esta comunicación no siempre será fácil[37], teniendo que acudir a otros elementos externos para su valoración, como puede ser la presentación de una denuncia ante la policía. La sentencia civil de la Audiencia Provincial de Madrid, sección 11, de 11 de mayo de 1999, consideró que el titular sólo había de ser responsable por el pago de cargos anteriores a la fecha de la denuncia del robo que había efectuado en la comisaría de Policía, pues en dicho caso se hizo coincidir dicho momento con el de la comunicación a la entidad bancaria ya que «no consta en autos indicio alguno que haga suponer una comunicación a la demandante, es más la lógica y el sentido común aconsejan hacer coincidir la denuncia en comisaría con la comunicación a la entidad bancaria».

Asimismo, es importante atender a las circunstancias de uso de las tarjetas, para determinar en qué momento es razonable detectar que la misma se ha extraviado o robado y, en consecuencia, realizar la correspondiente comunicación. Por ello, la sentencia civil de la Audiencia Provincial de Baleares, sección 5.ª, 123/1997, de 26 de febrero, considera que no existen indicios de demora cuando la comunicación se ha efectuado tras la recepción del extracto mensual, momento en el que detecta los cargos indebidos y se produce la denuncia del robo de la misma (en el caso la demora se había situado en 38 días).

Del mismo modo, tal como se pronuncia la sentencia de la Audiencia Provincial de Sevilla, Sección Quinta, de fecha 12 de diciembre de 2002, tampoco se estima que concurre una conducta negligente del titular de la tarjeta, dado el *modus operandi* de los delincuentes, cuando, finalizada la operación en el cajero y estando el titular a la espera de

[37] Con carácter general, se estipula que el aviso se realizará telefónicamente. Como es posible que surja una controversia, conviene realizar una confirmación por escrito, que pueda probar el cumplimiento de sus obligaciones por el titular.

que saliera la tarjeta de la ranura del cajero, se le acerca un individuo y le dice que se le ha caído el dinero. Al agacharse, otro individuo le sustrajo su tarjeta y se la cambió por otra de similar aspecto, circunstancia de la que no se percató el titular hasta cuatro días después, al ir a sacar dinero al cajero.[38]

Respecto de los supuestos en los que no ha existido comunicación alguna, se han de valorar circunstancias tales como si el titular puede probar la pérdida de la tarjeta y que las disposiciones no son suyas. La sentencia civil de la Audiencia Provincial de Asturias, sección 1.ª, 493/1997, de 18 de septiembre, condenó al titular a pagar al Banco, por entender que debía soportar su negligencia por no comunicar el extravío, sin perjuicio de que ejercitase las correspondientes acciones contra el autor de la manipulación.[39]

c) Obligaciones del establecimiento comercial

Entre las obligaciones del aceptante se encuentra la de tomar medidas que permitan identificar al titular legítimo de la tarjeta para poder detectar cuándo las mismas están siendo usadas por un no titular (entre otras, las más comunes, pidiendo el carnet de identidad y verificando la firma del talón de compra con la de la tarjeta) y, en su caso, avisar cuando se tome conocimiento de un uso ilegítimo.

En este aspecto, partimos de una práctica en que no resulta infrecuente que las empresas no realicen siquiera las mínimas comprobaciones (solicitud de DNI u otro documento oficial que permita identificar la

[38] La referida sentencia de la Audiencia Provincial de Sevilla, Sección Quinta, de fecha 12 de diciembre de 2002, tras analizar el artículo 10 de la Ley General para la defensa de los Consumidores y la publicidad efectuada por la entidad emisora de las condiciones de la tarjeta, declaró nula por abusiva la condición general insertada en un contrato de tarjeta de débito conforme a la cual se estipulaba que «El titular y el tenedor de tarjeta serán responsables quedando el Banco exento de toda responsabilidad por uso indebido en los casos de carencia de notificación o defecto en la misma…» Entiende la sentencia que «los usuarios de las tarjetas que hayan sido víctimas de actividades delictivas cometidas mediante el uso de las mismas deben quedar exentos de responsabilidad, salvo, evidentemente, que se demuestre la participación del titular en los delitos o que actuó con grave negligencia, en el cuidado y custodia tanto de la tarjeta como del número de identificación personal».

[39] La sentencia civil de la Audiencia Provincial de Ciudad Real, de 20 de mayo de 1993, (Ponente: Álvarez de Toledo Quintana) obligó al cliente a pagar, por no comunicar al Banco, aun cuando el titular defendió que la tarjeta había sido tragada por el cajero automático tras lo cual se habían producido las disposiciones. La sentencia consideró no probada tal pérdida, ni la comunicación a la entidad.

firma), sino que se limitan a hacer firmar la nota de cargo, sin ninguna otra consideración.

La jurisprudencia se ha pronunciado, reiteradamente, sobre los mínimos deberes que obligan a los dependientes de los establecimientos, como plasma la sentencia del Tribunal Supremo, Sala 1.ª, de 2 de noviembre de 2001, al señalar que:

> «el empleado del establecimiento tiene que adoptar precauciones para evitar la defraudación en estos casos en que se utilizan como medio de pago unas tarjetas cuyo uso está sometido a normas de contenido obligatorio y muy elemental, que son las mismas que permiten el que estos instrumentos sean emitidos por unas concretas empresas mercantiles con intermediación de las entidades bancarias».

De igual modo, son frecuentes los fallos de nuestras Audiencias en los que imputa la responsabilidad a los establecimientos, en la medida en que estos incumplieron su obligación de asegurarse de que la persona usuaria de la tarjeta era el titular de la misma, con la simple comprobación de las firmas (la del ticket con la tarjeta) y los rasgos fisonómicos del portador con la de la fotografía del DNI[40].

d) Grado de diligencia exigido a cada uno de los intervinientes referidos

Dados los parámetros utilizados en los pronunciamientos analizados respecto al grado de cumplimiento de los sujetos que intervienen en el uso de la tarjeta de sus obligaciones, podemos extraer que el nivel de diligencia exigido es el que correspondería, conforme al artículo 1258 del Código Civil, al de un buen padre de familia. No se exigen conductas extraordinarias o imposibles para detectar fallos en el sistema, sino hacer comprobaciones mínimas que permitan determinar qué sujeto ha de responder de los daños sufridos[41]. Como señala Díez-Picazo, esta diligencia equivale al normal nivel de esfuerzo y de atención de las personas que poseen un grado de diligencia media[42].

---

[40] Dicha responsabilidad, como señala la sentencia civil de la sección 1.ª de la Audiencia Provincial de Álava, 252/2001, de 13 de septiembre, deriva *ex* artículo 1.902 del Código Civil, pues se entiende que por dicha omisión negligente que ha conllevado a la autorización de la operación, no se ha evitado el hecho dañoso, es decir los cargos en la cuenta corriente.

[41] Vid. Sentencia civil de la Audiencia Provincial de Baleares, sección 5.ª, 123/1997, de 26 de febrero, ya comentada.

[42] Díez-Picazo, L.; *Fundamentos del Derecho Civil Patrimonial*. Ed. Tecnos, 2.ª reimp. Madrid, 1979, pp. 710 y ss.

4. *Consideración final sobre la responsabilidad civil*

En conclusión, consideramos que el sujeto pasivo de la acción defraudatoria, titular del bien jurídico lesionado e inicialmente perjudicado por las acciones fraudulentas realizadas mediante tarjeta de crédito, es la entidad bancaria, propietaria del numerario que se dispone mediante las mismas. Por ello, nunca será de aplicación la circunstancia mixta de parentesco, art. 23 CP, ni la excusa absolutoria entre parientes, art. 268, aun cuando efectivamente se diera la relación de parentesco que tales preceptos contemplan entre el autor de la infracción penal y el titular de la tarjeta o de la cuenta corriente.

Lo anterior, sin perjuicio de que posteriormente —incluso en la propia vía penal, como frecuentemente sucede—, se pueda determinar que asume finalmente dicho perjuicio patrimonial otra persona, en calidad de perjudicada, a tenor de los pactos existentes conforme a otras relaciones jurídicas que unen a estos mismos sujetos y al resto de sujetos involucrados en el uso de la tarjeta, y al grado de cumplimiento de las obligaciones que derivan de tales relaciones o contratos. En tales casos, se produce un traspaso del perjuicio final desde la entidad bancaria, sujeto pasivo del delito, hacia alguno de los sujetos que intervienen en las complejas relaciones contractuales que se hallan en la base de la emisión y uso de una tarjeta de crédito y con fundamento en el incumplimiento de sus obligaciones contractuales.

No obstante, parece conveniente que se excluyan del proceso penal y se derive su conocimiento a la vía jurisdiccional civil todos aquellos casos en que la cuestión de la asunción por terceros del perjuicio sea excesivamente compleja y productora de discusiones relativas al mayor o menor grado de cumplimento de las obligaciones contractuales de las partes o de la validez o no de las condiciones generales de los contratos, habida cuenta de que el objeto del proceso penal —la determinación de la comisión de un delito y su autor, y la consideración de perjudicado del sujeto propietario del dinero defraudado— se vería enturbiada totalmente con la cuestión estrictamente civil contractual relativa a si finalmente asume la entidad bancaria, como sujeto pasivo del delito, o un tercero, como perjudicado final, la condición de perjudicado por el delito. Sólo habrá lugar a ello cuando se trate de una cuestión que por ser sencilla y pacífica pueda ser resuelta directamente en vía penal.

Los delitos informáticos: dudas e incertidumbres en el Proyecto de Reforma del Código Penal

Fermín Morales Prats
Catedrático de Derecho Penal. Universidad Autónoma de Barcelona

I. La traslación de los criterios de ofensividad del Convenio de Cibercriminalidad al Código Penal en materia de delitos informáticos: planteamiento crítico en torno a la asimetría de demarcación típica que postula el Proyecto de Reforma de Código Penal de 2007

Como es sabido, reina la unanimidad a la hora de identificar la ausencia de sintonía legislativa entre el Código Penal de 1995, en materia de delitos informáticos y el Convenio de Cibercriminalidad, firmado en Budapest, de 2001.

Para lo que aquí interesa, una de las principales diferencias de planteamiento entre los referidos textos legislativos, queda cifrada en los criterios de delimitación típica de estas infracciones penales. Más concretamente, el Convenio de Budapest, partiendo de una idea emancipadora de los tradicionales conceptos de bien jurídico, acuñados tradicionalmente, para los delitos informáticos, se adentra en la proposición de unas figuras típicas desancladas de criterios de ofensividad hasta la fecha imperantes en el Código Penal de 1995.

Puede decirse que el Convenio de Budapest viene a cuestionar la columna vertebral de delimitación típica y de reparto de funciones incriminadoras, que el legislador español de 1995 ideó para los delitos informáticos. En efecto, el Código Penal español contempla la exigencia de elementos subjetivos del injusto en los artículo 197 y siguientes (delitos contra la intimidad) y en los artículo 278 y siguientes (delitos contra los secretos de empresa), con una doble función; de una parte, ese plus de intencionalidad viene a proporcionar un filtro de selección típica de las conductas de acceso ilícito a los datos informáticos que merecen respuesta penal; de otro, tal opción legislativa permite establecer una frontera entre las referidas familias típicas. Podrá cuestionarse tal proceder legislativo, por residenciar esenciales criterios normativos en

el elemento subjetivo del injusto, pero lo cierto es que se trata de un modelo que aporta un criterio de frontera entre ambos grupos de infracciones. Además, con todas las críticas que se quiera, permite al juzgador un criterio de selección típica al servicio del carácter de *ultima ratio* del Derecho Penal.

El Convenio de Cibercriminalidad precisamente se encamina a proponer la emancipación de tales figuras delictivas de la exigencia de elementos subjetivos del injusto, decisión que además queda vinculada a un serio cuestionamiento de los tradicionales conceptos de bien jurídico, cifrados en la idea de intimidad y de secreto de empresa. Esto último es importante, porque el referido texto internacional postula la incriminación transversal de las conductas ilícitas de acceso y abusos informáticos, prescindiendo de criterios teleológicos a la hora de agrupar las infracciones.

A todo lo anterior se adosa una incriminación de los daños informáticos en el Código Penal español, parca y desfasada. El artículo 264.2 CP no contempla, en definitiva, el moderno problema del sabotaje de los sistemas informáticos con la dimensión y precisión que lo hace el Convenio de Budapest y la Decisión Marco 2005/222 del Consejo de Europa, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

Identificadas estas faltas de sintonía del Código Penal vigente con las exigencias internacionales suscritas por España en la materia, el Proyecto de Código Penal de 2007 afronta la traslación de contenidos obrantes en los referidos textos internacionales con criterios político-criminales inciertos, por cuanto no permiten establecer con fundamento la asimetría por la que ha optado el prelegislador español, como ahora se verá.

Con relación a los delitos informáticos contra la intimidad, el Proyecto de CP de 2007 incorpora un nuevo número tercero del art. 197, por el que se incrimina la vulneración de medidas de seguridad a propósito del acceso no autorizado a datos o programas informáticos, contenidos en un sistema informático o en parte del mismo. La voluntad del Proyecto de alcanzar una incriminación de amplio espectro queda plasmada en el carácter genérico de la modalidad de ataque, pues no en vano el precepto textualmente dice que la conducta típica puede llevarse a cabo «por cualquier medio o procedimiento». Es singular la opción del Proyecto, por cuanto el nuevo número tercero propuesto para el art. 197 CP no viene a sustituir el tradicional número primero y segundo del precepto. Así, viene a añadirse como modalidad típica atenuada. Tal proceder legislativo suscita ya un problema interpretativo inicial, por cuanto la nueva modalidad típica propuesta no se alcanza a entender que contemple una pena atenuada, puesto que, si por una parte no contempla el plus de desvalor cifrado en la específica intención de vulnerar la intimidad,

por otro lado exige que la conducta típica se perpetre con vulneración de medidas de seguridad, lo que supone un plus de ofensividad o desvalor, no presente en las tradicionales figuras típicas de los números primero y segundo del art. 197 CP.

A buen seguro, esta relación de especialidad recíproca entre el nuevo precepto y los antiguos ofrecerá un laberinto hermenéutico.

Pero el mandato legislativo del Proyecto, al menos parece claro: a la vista del Convenio de Cibercriminalidad, pese a la imprecisión técnica, se incrimina una modalidad típica descargada de vigorosos elementos subjetivos del injusto.

Al margen de lo anterior, debe significarse aquí otra valoración crítica, ahora relativa a que el acceso ilícito incriminado en el número tercero del proyectado art. 197 CP, sigue limitándose a conductas de acceso no autorizado a datos sin aludir como alternativa a los sistemas informáticos, idea central en la normativa internacional. En suma, el Proyecto de CP, desde el punto de vista objetivo, viene a incriminar lo que ya era típico, con exigencia de un plus de vulneración de medidas de seguridad, pero expulsando la referencia al elemento subjetivo del injusto.

La anterior medida legislativa proyectada contrasta con el silencio del Proyecto de CP en lo relativo a los delitos informáticos contra los secretos de empresa o contra la información empresarial sensible (arts. 278 y ss. CP), que quedan inalterados. Esta asimetría de planteamiento político-criminal no alberga fundamento alguno, a la vista del Convenio de Cibercriminalidad de Budapest. Si lo que el Proyecto de CP pretende es transponer en derecho interno la incriminación del intrusismo informático, en cuanto acceso ilícito a los sistemas, la cláusula del número tercero del art. 197 no constituye la vía adecuada.

En efecto, la reforma en materia de delitos informáticos contra la intimidad, además de los defectos antes reseñados, constituye una vía incriminadota insatisfactoria para la protección de los sistemas informáticos de empresa, conforme a las exigencias del Convenio de Cibercriminalidad de Budapest. Se afirma lo anterior a la vista de la ubicación sistemática del art. 197.3 proyectado, residenciado entre los delitos contra la intimidad, lo que aporta ya un criterio teleológico rector de la interpretación. Así, este precepto no puede erigirse en la cláusula típica de la incriminación transversal del intrusismo informático, y por tanto, no podrá ser proyectado a la incriminación de tales conductas para tutelar los sistemas informáticos de las empresas, sin exigencias de elementos subjetivos del injusto.

Y en esta materia, a la vista del Proyecto, siguen suscitándose serias lagunas de intervención penal en punto a la incriminación de conductas que incidan sobre la protección de los datos en su vertiente de integridad

y disponibilidad, esto es, que protejan los secretos empresariales frente a alteraciones, supresiones o destrucciones de los mismos. Por tanto, el Proyecto de 2007 consolida las carencias seculares de los arts. 278 a 280 CP.

Por último, en materia de daños informáticos, el Proyecto de 2007 incorpora una extensa y novedosa disciplina, claramente superadora del vigente art. 264.2 CP.

En primer lugar, el prelegislador incrimina separadamente las conductas de daño, deterioro, alteración, supresión o conversión en inútiles (por inaccesibles) de los datos o programas informáticos, de aquellas otras relativas a la obstaculización, o colapso de los sistemas de información. Obsérvese cómo en esta materia el prelegislador ha sido más cuidadoso y ha comprendido mejor los reclamos del Convenio de Cibercriminalidad y de la Decisión Marco relativa a los ataques contra los sistemas de información. Siendo esto así, de nuevo no se alcanza a comprender la asimetría de planteamientos con relación a los delitos contra la intimidad y los delitos contra los secretos de empresa.

No obstante, también hay resquicio para la crítica de los daños informáticos, por cuanto el Proyecto debería haber reflexionado sobre la necesidad de transportar las conductas del futuro art. 264.2 (sabotajes y obstaculizaciones de los sistemas de información) a un contexto sistemático diverso al de los delitos contra el patrimonio y la propiedad, dado que aquí conforme a las directrices internacionales, se desea tutelar bienes jurídicos de nuevo cuño, de difícil delimitación (sistemas informáticos ligados a los intereses de libertad y seguridad en las relaciones de comunicación e información), pero que en cualquier caso reclaman la idead de intereses o bienes jurídicos supraindividuales.

El Proyecto de Código Penal en la materia analizada no aporta la luz necesaria, probablemente, sólo enciende una vela, que a buen seguro se apagará en cuanto resoplen las primeras interpretaciones profundas de los citados preceptos.

II. **La recepción en derecho interno de las directrices internacionales en materia de responsabilidad penal de las personas jurídicas para los delitos informáticos: de nuevo una propuesta asimétrica en el Proyecto de Código Penal de 2007**

El Convenio de Cibercriminalidad contempla, en su artículo 12, la responsabilidad de las personas jurídicas mediante una cláusula de mandato a los Estados en punto a la adopción de medidas legislativas que hagan admisible la responsabilidad de los entes con personalidad jurídi-

ca para las infracciones tipificadas en el referido texto internacional. El Convenio de Budapest proyecta tal cláusula para los supuestos en los que la persona física actúa ejerciendo un poder de dirección en el seno de la persona jurídica, cuyo origen resida en un poder de representación o bien en una autorización para tomar decisiones en nombre de la sociedad o para ejercer el control en el seno de la persona jurídica. Asimismo, la convención internacional contempla el mandato de política legislativa para los casos de ausencia de vigilancia o control, que posibilite la comisión de las infracciones.

Como puede observarse, el Convenio de Cibercriminalidad no establece un mandato de política penal en sentido estricto, puesto que no se pronuncia sobre la naturaleza de la responsabilidad de la persona jurídica. Por tanto, el Convenio de Budapest viene presidido por un criterio de cautela y de respeto a los principios y sistemática de cada derecho interno, sin prejuzgar que el régimen de responsabilidad sea penal, civil o administrativo.

No obstante, el artículo 12 del Convenio opta por la claridad en punto al establecimiento del régimen de responsabilidad, por cuanto declara nítidamente que esa responsabilidad de la persona jurídica se establecerá sin perjuicio de la responsabilidad penal de las personas físicas, que hubieren cometido la infracción. Esto quiere decir que la condena de una persona física no excluye con automatismo la de una persona jurídica, del mismo modo que también es posible la declaración de responsabilidad del ente jurídico sin previa condena de la persona física. Se trata, por tanto, de una responsabilidad directa, que no es subsidiaria ni accesoria de la correspondiente de las personas físicas. Por consiguiente, estamos ante nuevos criterios que originan un régimen de responsabilidad para entes colectivos.

Atendido lo anterior, en el ámbito interno español, la política legislativa a desarrollar debe transcurrir por los derroteros de un régimen de responsabilidad de personas jurídicas proyectable al conjunto de infracciones que tipifica el Convenio de Budapest. Como se ha dicho, impera un criterio de libertad para ubicar esa responsabilidad en el ámbito penal, civil o administrativo.

El Proyecto de Código Penal de 2007 nos indica claramente que las autoridades españolas han optado por residenciar el régimen de responsabilidad de las sociedades en el ámbito penal, opción posible, siempre que se proyecte sobre la extensión que indica el Convenio de Budapest en cuanto a las infracciones concernidas por la medida. No obstante, la lectura del texto del Proyecto lleva al desconcierto, por cuanto una vez se ha optado por el régimen de disciplina penal, éste sólo se proyecta a los daños informáticos, según el tenor de lo dispuesto en el número

cuarto del proyectado artículo 264 CP. En efecto, la referida cláusula legal indica que, cuando los delitos de daños informáticos se hubieran cometido en el marco o con ocasión de actividades de una persona jurídica —y proceda la declaración de su responsabilidad penal *ex* art. 31 bis del Proyecto—se le impondrá la pena de multa del tanto al duplo del perjuicio causado o bien del tanto al décuplo para los casos de comisión de conductas agravadas.

Este precepto del proyecto remite al art. 31 bis que incorpora el estatuto general de criterios de atribución de responsabilidad penal directa e independiente a las personas jurídicas.

Establecido lo anterior, no se alcanza a comprender el silencio que impera en el Proyecto respecto a la responsabilidad penal de las personas jurídicas para los delitos informáticos contra la intimidad (arts 197 y ss. CP), porque incorpora de nuevo una asimetría en tensión con lo dispuesto en el Convenio de Budapest. En este sentido, la traslación que se hace al derecho interno es incomprensible, sobre todo si tenemos en cuenta que, precisamente —aunque con imprecisión técnica y de ubicación—, el número tercero del art. 197 pretende erigirse en una cláusula típica de amplio espectro, enderezada a la incriminación de acceso ilícito a los datos, sin exigencia de elementos subjetivos que presidan la conducta. Por esta razón, se hace incomprensible que el mandato de política legislativa relativo a la responsabilidad jurídica de personas jurídicas no goce de proyección al art. 197 CP.

Esta conclusión es obligada por cuanto el estatuto de responsabilidad de las personas jurídicas, adopta la técnica de cláusula específica en el Proyecto de 2007, conforme al tenor del art. 31 bis del Proyecto.

No se identifica razón político-criminal suficiente para excluir los delitos informáticos contra la intimidad del nuevo régimen de responsabilidad penal de las personas jurídicas. Esto es, no existen razones para que, en esta materia, el derecho interno se sustraiga al compromiso internacional que deriva del Convenio de Budapest.

Dicho lo anterior, el régimen de responsabilidad de las personas jurídicas incorporado en el Proyecto para los delitos informáticos contra los secretos de empresa y delitos de daños informáticos merece las siguientes reflexiones.

El Proyecto ha optado por un sistema de responsabilidad penal de las personas jurídicas de carácter principal y directo, lo que supone un cambio de modelo en el Código Penal español. Es necesario destacar el carácter principal de la responsabilidad, por cuanto el apartado segundo del artículo 31 bis del Proyecto deja bien a las claras que no se reclama la previa responsabilidad de las personas físicas para la posterior exigencia de responsabilidad a las personas jurídicas.

Ahora bien, el modelo o sistema adoptado requiere de algunos vínculos o presupuestos de activación. El primero de dichos presupuestos se refiere a la identificación previa de la comisión de un delito por parte de persona física, que ostente un poder de dirección fundado en la atribución de representación o en una autoridad, concretada en un poder o facultad para tomar decisiones en nombre de la persona jurídica o bien para controlar el funcionamiento de la sociedad. Además exige que la comisión del delito por persona física se haya verificado en una actuación por cuenta o en provecho de la persona jurídica.

Ahora bien, la exigencia de este presupuesto de vinculación a la actuación de personas físicas con los poderes de actuación antes reseñados, constituye un presupuesto lógico que, en modo alguno, puede comprometer el carácter principal e independiente de la responsabilidad penal exigible a las personas jurídicas.

El segundo vínculo o nexo de conexión con la actuación de personas físicas alude a los delitos cometidos en el ejercicio de actividades sociales (por cuenta y en provecho de las personas jurídicas), protagonizados por personas físicas, sometidas a la autoridad de quienes tienen el poder societario (representativo de autoridad) y han cometido la infracción penal por no haberse ejercido sobre tales personas físicas el debido control societario o empresarial. Obsérvese que, en esta segunda modalidad de vínculo, subyace un reproche o exigibilidad de responsabilidad a la persona jurídica por responsabilidad *in vigilando* o *in eligendo*.

El prelegislador instaura algunos criterios de modulación de la responsabilidad penal de las personas jurídicas, dando cumplimiento a las directrices internacionales que instan al respeto del principio de proporcionalidad. Así, por ejemplo, se establece que, para los supuestos de imposición de penas de multa, respectivamente, para las personas jurídicas y para las personas físicas, un mandato a jueces y tribunales en punto a la modulación de las respectivas cuantías, en evitación de que la suma resultante de las multas supusiese una violación del principio de proporcionalidad en relación con la gravedad del hecho delictivo cometido.

Asimismo, se prevén un conjunto de circunstancias atenuantes, vinculadas con actuaciones *ex post factum* de la persona jurídica, como, pongamos por caso, la atenuante de confesión a las autoridades, con carácter previo a la toma de conocimiento de que el procedimiento penal se dirige contra la persona jurídica; la atenuante de colaboración en la investigación penal a medio de aportación de pruebas, en cualquier fase del proceso, que fueran decisivas, para la declaración de la propia responsabilidad penal de la persona jurídica, que podrá ser esgrimida aun después de haberse conocido que el procedimiento penal se dirige contra el ente jurídico.

Debe destacarse, también, que el prelegislador ha tratado de evitar la elusión de la responsabilidad penal de las personas jurídicas en fraude de ley. En este sentido, el art. 130 del Proyecto, en su apartado segundo, señala que la transformación, fusión, absorción o escisión de una persona jurídica no extingue la responsabilidad penal, de modo que ésta es trasladable a la entidad resultante de la transformación, fusión o escisión. En la misma dirección el texto insiste en que la disolución encubierta o meramente aparente de la persona jurídica tampoco extinguirá la responsabilidad penal. Esta previsión deberá ser interpretada con mesura en salvaguardia de los legítimos derechos de terceros de buena fe, por ejemplo, sociedad ajena a la comisión del delito que se fusiona con otra implicada en el mismo, o sociedad absorbente o absorbida ajena a la comisión del delito.

A la vista de este modelo de responsabilidad penal de las personas jurídicas, debe quedar esclarecido que el estatuto de las consecuencias accesorias, queda reservado exclusivamente a entes asociativos, sociedades u organizaciones que carezcan de personalidad jurídica, según el nuevo texto que se postula para el art. 129 del Proyecto. Conviene precisar que el prelegislador establece el fundamento de estas consecuencias accesorias cifrado en la prevención de la continuidad delictiva y los efectos de la misma. Resulta curioso que el legislador delimita el fundamento de estas medidas penales accesorias, y en cambio no menciona el relativo a la responsabilidad penal de las personas jurídicas, siendo así que ésta constituye una responsabilidad directa y principal.

En este sentido, el art. 31 bis podría haber expresado como fundamento de esa responsabilidad la prevención de la comisión de futuros delitos y la cesación de los efectos de los ya cometidos, mediante el abuso de personalidad jurídica, por cuanto el delito no es ajeno al ente jurídico, en la medida que ha sido cometido en nombre, por cuenta o bien por interés de aquélla. Sin embargo, la elucidación legal del fundamento de esta responsabilidad permitiría afrontar con mayor seguridad el estatuto de medición o modulación de la misma, por medio de un régimen de atenuantes, agravantes y eximentes más pormenorizado o certero que el que ofrece el proyecto.

En cuanto a las penas aplicables a las personas jurídicas, el Proyecto recoge sanciones que, en gran medida, están previstas en la actualidad para las consecuencias accesorias, reguladas en el art. 129 CP. A tal efecto, el art. 31 bis contempla la multa por cuotas o por criterios proporcionales, la pérdida de personalidad jurídica o de capacidad para actuar en el tráfico jurídico mediante la disolución, la suspensión de actividades por un plazo máximo de 5 años, la clausura de locales por idéntico plazo máximo, la prohibición de realizar determinadas actividades relaciona-

das con el delito perpetrado, que puede ser definitiva o temporal hasta 15 años, la inhabilitación para la obtención de subvenciones, ayudas públicas o beneficios fiscales, la inhabilitación para contratar con Administraciones y, por último, la intervención judicial por un plazo máximo de 5 años.

Por último, se prevé la posibilidad de que el juez instructor adopte como medida cautelar la clausura de local, la suspensión de actividades sociales y la intervención judicial. Sorprende con relación a este último extremo que no se prevea como medida cautelar la que admite un mejor maridaje con los principios garantistas de las medidas cautelares, cifrados en las ideas de subsidiariedad, necesidad, proporcionalidad y *bonus fumus iuris,* y que no es otra que la prohibición de realizar determinadas actividades sociales relacionadas con el hecho investigado indiciariamente como delito.

Problemas relacionados con la investigación de los denominados delitos informáticos (ámbito espacial y temporal, participación criminal y otros)

Manuel Viota Maestre

Jefe de la Sección Central de Delitos en Tecnologías de la Información de la Ertzaintza

I. **Introducción**

El enfoque de esta ponencia debería ceñirse al título en lo tocante a los problemas generales del derecho en la sanción de los «delitos informáticos», pero mi limitada formación jurídica hace aconsejable, al menos para mantener intacta mi autoestima, que me aleje de consideraciones legislativas y jurisprudenciales, pues es meridianamente claro que el lector al que va dirigida tiene esos conocimientos a una profundidad a la que yo no puedo llegar.

Voy a desarrollar la exposición tratando de explicar, al menos someramente, los problemas relacionados con la investigación de los denominados genéricamente «delitos informáticos», con los que a lo largo de estos años nos hemos venido enfrentando desde la Sección de la Ertzaintza a la que pertenezco.

La finalidad última de una investigación policial consiste en lograr identificar al autor de unos hechos que el legislador ha definido como delictivos, registrar todas las circunstancias, tanto favorables como desfavorables para el sospechoso que tengan relación con las actividades ilícitas por él desarrolladas y posteriormente hacer entrega de todo lo averiguado al Juez Instructor.

Idealmente, la labor de la policía consistiría en la prevención del delito, pero en la práctica, pese a que esa labor se desarrolla con la mayor eficacia posible, no es menos cierto, que los delincuentes suelen burlar nuestra vigilancia para cometer sus actos ilegales. Es ahí cuando comienza nuestra labor represiva.

Pero esta prevención y represión del crimen no puede hacerse sin ninguna norma reguladora que fiscalice nuestras acciones y es por lo cual, la sociedad, a través de los legisladores, ha desarrollado una serie

de leyes que enmarcan nuestro campo de actuación, de tal forma que ninguna actividad policial tiene sentido ni refrendo si se halla fuera de esos límites.

El respeto escrupuloso a estas normas hace viable que lo obtenido en las investigaciones pueda ser presentado en un juicio con las suficientes garantías para que se transforme en prueba.

Del «tamaño del marco» en el que nos movamos va a depender en gran medida los resultados que se puedan lograr, puesto que en ese espacio es donde podemos hacer uso de nuestras herramientas de investigación.

La reflexión que deberíamos hacer es si con las herramientas que nos hemos dotado, tanto de derecho sustantivo y procesal, y con la interpretación doctrinal y jurisprudencial que de las mismas se han realizado hasta la fecha van a tener «alguna virtualidad» en la investigación y represión de los denominados «ciberdelitos».

Hay que tener en cuenta que los delincuentes no limitan su actuación a ninguna norma, y por lo tanto la lucha contra ellos es de todo punto desigual. Se aprovechan del sistema de garantías cuando les favorece y lo dejan de lado para cometer sus actos ilegales.

La constante evolución de los métodos comisivos e incluso la aparición de nuevas actividades susceptibles de reproche penal motivan que la maquinaria legislativa tenga que estar en constante movimiento para adecuar paulatinamente sus normas con el fin de evitar lagunas de impunidad.

Si alguno de ustedes ha visto (de lo que no hay duda) películas de policías norteamericanos, habrán comprobado cómo, generalmente, cuando investigan un delito tienen a su disposición una ingente cantidad de herramientas para su uso, de las cuales las armas son únicamente el último recurso. El verdadero potencial de esos investigadores se fundamenta en la capacidad de acceder a ingentes cantidades de bases de datos en las cuales es posible buscar y obtener resultados en tiempo real.

Aunque esto puede no ser más que una ficción en determinados aspectos, sí que muestra claramente que uno de los principales activos de un investigador lo conforma la información y que el acceso a la misma pueda ser realizado con la agilidad necesaria.

Con nuestra legislación la obtención de datos es un trabajo arduo, porque en la práctica todo ha de ser solicitado por la Autoridad Judicial y eso dilata en gran manera el tiempo necesario para su obtención. Este retraso en la adquisición de la información se multiplica cuando los conservadores de la misma se encuentran en otro país, llegando a convertirse, *de facto*, en un motivo de impunidad como se explicará posteriormente.

Como se ha dicho al principio, uno de los objetivos principales de un investigador cuando aborda el estudio de un hecho es identificar fehacientemente a su autor. ¡Ahí es nada!.

En el mundo de las nuevas tecnologías de la información en el que se circunscriben nuestras pesquisas, se puede llegar, en determinadas ocasiones, a poder localizar el ordenador desde el que se realizó la conducta ilícita. Ahora bien, cosa distinta es poder individualizar al usuario que controlaba la máquina en el momento de cometerse el delito.

Esta dificultad de identificación está potenciada por varios aspectos que, debidamente combinados entre si, imposibilitan que se pueda poner nombre y dos apellidos al autor de una conducta.

II. **Consideraciones técnicas**

Antes de abordar el desarrollo de este texto considero importante establecer una serie de conceptos que se van a utilizar a lo largo del mismo y cuyo conocimiento va a permitir a los lectores poder comprender aspectos que de otro modo quizás quedasen confusos.

Se parte de la concepción de que el público al que va destinada esta publicación tiene un nivel de usuario medio en informática, esto es, que conoce que existe Internet, los sistemas de mensajería, el correo electrónico y que maneja convenientemente algún paquete ofimático. En esta creencia se van a simplificar lo máximo posible los conceptos, llegando a realizar afirmaciones cuya exactitud no es tanta como requeriría otro tipo de informe, pero que van a servir para acercar los conceptos de una manera más comprensible.

1. *Dirección IP*

Una dirección IP (*Internet Protocol*, Protocolo de Internet) es un conjunto de cuatro números separados por puntos con un valor que puede oscilar entre el 0 y el 255. Suelen adoptar la forma 192.168.12.77.

Estas direcciones IP son imprescindibles para que dos ordenadores o sistemas informáticos se comuniquen en una red. Los ordenadores se identifican entre sí a partir de esa dirección IP, que a la postre se puede asimilar con una dirección física en el mundo real. Por ello, en una red determinada no pueden coincidir dos IPs iguales, en el mismo momento.

Esto es debido a que los ordenadores envían sus informaciones mediante paquetes y utilizan determinados protocolos para esos envíos.

En esos paquetes de información se anotan en sus cabeceras, entre otros datos, las direcciones IP del emisor y del receptor, para que la comunicación pueda llevarse a efecto.

Si en una misma red coexistiesen más de una dirección IP idéntica, no podría discernirse a cual de las dos se dirigiría un paquete de datos, de la misma forma que un cartero se volvería loco si en la misma calle existiesen dos portales 5 con el mismo número de pisos, y en la carta no constase el nombre del destinatario.

2. *Asignación de direcciones IP*

Por su definición, el número de direcciones IP, aunque muy amplio, es limitado y por lo tanto tiene que estar sometido a alguna regulación para que se puedan repartir entre los usuarios de una forma efectiva.

Con este objetivo se creó la IANA (*Internet Assigned Numbers Authority*), cuyas funciones fueron posteriormente asumidas por la ICANN (*Internet Corporation for Assigned Names and Numbers*) que se encarga, entre otras cosas, de distribuir las limitadas direcciones IP entre los solicitantes.

Ante la ingente cantidad de trabajo que les daba esta labor y para una mejor gestión, la ICANN delegó sus funciones en los Registradores Regionales de Internet (RIR) quienes se dividieron el mundo en varias zonas para poder repartir las direcciones IP entre los usuarios sitos en sus áreas de influencia.

Los RIRs que existen en la actualidad son:

a) RIPE, que se encarga de Europa y Asia Central.
b) AFRINIC, que se ocupa de África.
c) LACNIC, cuya zona influencia es el Caribe y Sudamérica.
d) ARIN, que se encarga de América del Norte.
e) APNIC, con responsabilidad sobre Asia y la Región del Pacífico

Cuando un proveedor de servicios de Internet (PSI) desea establecerse, lo que tiene que hacer es ponerse en contacto con el RIR de su demarcación y solicitarle el número de direcciones IP que necesite para su negocio.

Generalmente hacen una estimación a la baja, alquilando únicamente aquel número de las mismas que puedan ser utilizadas a la vez por sus clientes.

Cuando un usuario perteneciente a este PSI desea «navegar por Internet» su ordenador se pone en contacto con el PSI y le informa (utilizando determinados protocolos) de sus intenciones. El proveedor, tras

verificar que se trata de su cliente (mediante usuarios y contraseñas u otros métodos de autenticación) revisa su listado de direcciones IP para ver cual de ellas está libre. Una vez localizada una disponible se la asigna al cliente.

Hasta el momento en el que el cliente cierre la comunicación esa dirección IP seguirá siendo la misma, identificándole en todos y cada uno de los servicios que utilice en Internet. Una vez finalizada la navegación el cliente devolverá su dirección IP al proveedor, quien la tendrá nuevamente disponible para nuevos clientes.

Según lo visto, es perfectamente factible que una misma dirección IP pueda ser asignada consecutivamente a dos clientes completamente distintos. Por ello la fecha y la hora de asignación de una IP es fundamental de cara a identificar qué ordenador estaba detrás de determinada comunicación.

Para explicar este concepto se va a utilizar un ejemplo, que aunque no se refiere al mundo informático, la gestión de los procesos que en él intervienen puede ser aclaratorio. Se trata del caso de un locutorio público.

Imaginémonos: uno de los clientes del locutorio tiene un conflicto personal o profesional con su superior. Harto de no poder expresar lo que piensa por temor a un despido, se «arma de valor» y llama por teléfono a su jefe (sin identificarse claro), y le dice lo que piensa de él y lo que le tiene reservado, a él, a su familia y a su vehículo, es decir le amenaza de gravedad. Finalizada la conversación se paga con una tarjeta de crédito.

Como el amenazado tiene en su casa el sistema de identificación de llamadas, anota el número de teléfono. Pone la correspondiente denuncia y la policía, como consecuencia de la investigación practicada y la tramitación de los oportunos oficios, llega al locutorio.

Si la policía, en su petición al empleado o responsable del locutorio no le especifica la hora en la que se produjo la llamada, es previsible que éste no pueda identificar al usuario, puesto que la misma cabina habría sido utilizada secuencialmente por varios clientes.

Si se explicita la hora, en la mayoría de los casos, el dependiente podría decir que una persona estuvo llamando de tal hora a tal hora desde la cabina número tal, nada más. Pero en este caso, como ha pagado con una tarjeta de crédito, podrá aportarse ese dato. Tras las oportunas gestiones en el banco se podría establecer la identidad real del presunto autor.

El registro de estas direcciones IP y a qué proveedor de servicios se encuentran asignadas se guarda en unas bases de datos de dominio público cuya consulta, a fecha de hoy, puede realizarla cualquier persona.

De esta forma, mediante consultas informáticas en algunas páginas de Internet puede determinarse que cierta dirección IP pertenecería al rango de direcciones asignadas a determinado proveedor de servicios (o empresas).

3. *Rastros en Internet*

Como se ha apuntado anteriormente, cuando un equipo informático realiza cualquier acción en Internet, se identifica mediante su dirección IP, y por lo tanto los distintos servicios que se prestan, desde enviar un correo electrónico hasta consultar una página *web* pasando por el compartir archivos en las redes P2P, hacen un uso intensivo de esta dirección IP, quedando almacenada en varios lugares de los cuales puede ser recuperada.

El primero de ellos es el PSI, otro las páginas *web* que se visita, otra son los mensajes de correo electrónico enviados, y así para casi todas las acciones que se lleven a cabo en Internet.

Por lo tanto nuestra actividad en la Red deja rastro.

No obstante existen métodos, más o menos sofisticados de soslayar este control o al menos de disfrazarlo de tal forma que su identificación sea costosa.

4. *Proxys*

Un *proxy* sería la versión informática de lo que en mi barrio se llamaba «correveidile». Esto es, un intermediario. Generalmente estos sistemas se instalan para aislar de cierta forma una red interna del resto de Internet.

Cuando un ordenador de la red interna solicita algo de un equipo ubicado en Internet, no se lo pide directamente, sino que haría el requerimiento al *proxy*. Este asumiría esa pregunta como propia e interrogaría al destinatario y trasmitiría la respuesta que éste le diese al solicitante.

De esta forma, el destinatario desconoce cual es la dirección IP real del solicitante (el *proxy* se ha presentado en su lugar) con lo cual se aporta cierta anonimato a la comunicación.

Esta forma de funcionamiento es una práctica habitual de las empresas ya que de esta forma únicamente tienen necesidad de contratar una conexión a Internet, siendo el *proxy* el dispositivo que se encargaría de filtrar todas las comunicaciones de la empresa hacia Internet. Pero como todos los servicios y sistemas ha de estar convenientemente con-

figurado y securizado, porque si no, será un blanco fácil de los delincuentes informáticos.

La deficiente configuración de los dispositivos, o incluso en algunas ocasiones, la cesión desinteresada a la «comunidad» para hacer anónimas las comunicaciones hace que puedan ser utilizados por usuarios externos para enmascarar sus direcciones IP aportando un alto grado de impunidad sus acciones.

Es fácil encontrar en Internet listado de *proxy*s anónimos con los cuales ocultar nuestra dirección IP a coste, eso sí, de la velocidad de navegación.

Además, para los no iniciados existen programas que realizan búsquedas en sus bases de datos sobre la ubicación de esos *proxy*s y desvían la navegación de los clientes a través de los mismos para ocultar su origen de forma automática.

5. *Logs*

Una de las palabras más utilizadas cuando se habla de la investigación de un delito en el que se haya utilizado un sistema informático es *log*.

Cuando se crea un programa o un sistema, su autor suele diseñarlo de forma que vayan registrándose datos de su actividad, los cuales son almacenados para su posterior revisión. Estos ficheros serían los *log*.

La finalidad de estos *log*s es la de poder comprobar en cada momento que el funcionamiento del sistema es coherente con el diseño y que todo funciona como se ha previsto, sin interferencias ni internas ni externas.

Casi todos los sistemas o servicios informáticos presentan estos archivos de registro. Unos para informar de las actividades realizadas y otros además para mostrar errores o fallos de funcionamiento para ser posteriormente analizados y proceder a su depuración.

Normalmente estos *log*s son almacenados en soportes magnéticos dentro de equipos informáticos.

El tamaño de estos *log*s varía dependiendo de varios factores: lo «ruidoso» del sistema analizado, los parámetros introducidos por su administrador, o los usuarios concurrentes al mismo.

6. *Borrado de archivos*

Para los profanos, el pulsar la tecla *delete* o *supr* sobre un archivo en un ordenador personal equivale a borrar definitivamente el fichero.

Para los que han leído un par de revistas de informática de consumo, el conocimiento aumenta y ya saben que si utilizan determinados sistemas operativos modernos de una conocida empresa de *software* ubicada en Estados Unidos con implantación mundial, cuyo nombre no voy a dar para no entrar en guerras de publicidad y derechos, el archivo no desaparece, sino que se envía a la papelera de reciclaje. Desde allí se puede recuperar si se desea o hacerlo desaparecer finalmente vaciando la referida papelera.

Bien, todos se equivocan. En la mayoría de los casos, los archivos no desaparecen ni se eliminan, lo que hace el sistema operativo es ocultarlo, borrando su índice y por lo tanto no siendo capaz de localizarlo. Pero los datos siguen grabados en el disco duro hasta que sean sobrescritos por otros datos de otros ficheros.

Utilizando determinados programas informáticos es posible, incluso para los más profanos, recuperar de manera exitosa archivos teóricamente eliminados mucho tiempo antes, dependiendo eso sí, de la actividad realizada en el ordenador, siempre y cuando la parte del disco en la que se alojaban los datos no hayan sido ocupadas por otros datos de otros ficheros.

Existen sin embargo formas de eliminar ficheros utilizando protocolos de seguridad que se basan en la escritura varias veces de caracteres aleatorios sobre la zona de datos, dificultando, y en muchas ocasiones haciendo imposible su recuperación.

Sin embargo, aunque un poco drástico, la mejor forma de eliminar lo contenido en un soporte informático es destruir físicamente el mismo. Si quemamos el disco de plástico en el que se graban las informaciones de un disquete, difícilmente podrá ser recuperada su información.

Muchas veces se han dado casos de empresas que venden sus equipos informáticos a tiendas de «segunda mano» con los discos duros utilizados en su trabajo diario, sin más precaución que formatearlos. En muchas ocasiones estos discos duros todavía contienen de forma latente información que la empresa no querría que se revelase y que pueden ser reactivados con los conocimientos necesarios (y no son muy elevados).

III. **Problemas en la investigación**

Tras esta somera explicación de estos conceptos se va a entrar de lleno en el desarrollo de la ponencia, para explicar las dificultades que entraña la investigación de los denominados «delitos informáticos».

Haciendo uso del título, se van a distribuir estos aspectos en varios campos: el ámbito espacial, el ámbito temporal, la participación criminal y otros.

1. *El ámbito espacial*

A) Necesidad de mecanismos de cooperación

La generalización de Internet ha supuesto una dilución de las fronteras, una supresión de las mismas, aunque no de una forma universal.

Para los estamentos policiales y judiciales las fronteras siguen existiendo. La concepción de los códigos penales tradicionales se basan en la capacidad de los estados para poder ejercitar la persecución de los delitos cometidos dentro de su territorio.

Viendo la edad que tienen los códigos penales, es fácilmente comprensible el porqué de esta concepción. En los tiempos de su creación, delincuente y víctima solían coincidir en el tiempo y en el espacio para que el delito pudiese perpetrarse y por lo tanto la persecución de aquél podría realizarse sobre el terreno en el que el estado tenía soberanía.

Estos estados estaban separados entre sí por fronteras con guardianes a ambos lados de la misma, por lo que si un delincuente quería huir de un país para trasladarse a otro, obligatoriamente debería tener que pasar por dos controles fronterizos, uno de salida y otro de entrada.

Con el concepto de «aldea global» estas fronteras carecen de sentido y hoy es perfectamente factible establecer comunicación a través de la Red de Redes con una persona ubicada en cualquier país del mundo con la misma facilidad que con nuestro vecino de al lado.

Lo único que se necesita para ello es una conexión a Internet y un equipo que permita la comunicación.

Por ello, cada vez con mayor frecuencia, los delincuentes hacen uso de estas tecnologías para facilitar sus labores comisivas, al poder tener acceso a potenciales víctimas con las que no van a tener que establecer un contacto físico que les permita reconocerles, y pueden estar ubicados en un lugar tan lejano, que a la policía le resulte realmente difícil seguirle la pista.

Esta persecución de «delitos informáticos» en la que se ven involucrados dos o más países se complica enormemente puesto que es necesario hacer uso de los convenios de colaboración suscritos entre ambos países (caso de haberlos).

Obviamente, estos protocolos son costosos de poner en funcionamiento puesto que la «maquinaria» no está convenientemente engrasada, lo que hace que haya que vencer una gran inercia para ponerla en marcha.

Señalar por ejemplo, que determinados Centros Nacionales de INTERPOL sólo atienden solicitudes en base a dos parámetros que han de cumplirse:

a) Que la cantidad defraudada sea superior a cierta cantidad o
b) Que sea claro que el delito se ha cometido por una red organizada.

Conscientes de esas ventajas, cada vez más delincuentes están realizando sus «timos» en España estableciendo su base de operaciones en otros países, limitando las cantidades defraudadas a una cantidad que no suele superar los límites establecidos.

En estos casos, la cantidad no puede ser el parámetro utilizado para solicitar colaboración y debería ser la pertenencia a una red organizada. Aquí viene el problema: si se puede investigar a los autores, ¿cómo se puede determinar si conforman una red o si por el contrario son estafadores individuales?

B) Distintas legislaciones

El derecho generalmente es territorial, esto es, el Estado establece qué conductas son susceptibles de reproche penal y tiene la limitación territorial de sus fronteras, lo que deriva en que, si no existe la conveniente armonización entre las legislaciones de distintos países, lo que es delito en uno de ellos no lo será en el segundo y por lo tanto, no podrá ser perseguido.

Si esta diferencia de legislaciones se da dentro del marco de la Unión Europea ¿qué no pasará cuando se tratan de hacer compatibles legislaciones de países de los llamados «otros mundos» en los que la concepción de los derechos difiere bastante de lo que se entiende en Europa por los mismos?

La solución de estos conflictos pasaría por la creación de un estamento supranacional que aunase los distintos códigos penales. Obviamente, y tal y como va el mundo en nuestros días, esto pasa de ser utópico a convertirse directamente en ciencia ficción.

Como ejemplo baste señalar que el 23 de noviembre de 2001, en Budapest, el Consejo de Europa confeccionó el Convenio sobre la Ciberdelincuencia en la que se definían los marcos legislativos que deberían adoptar los diferentes países que lo conformaban de cara a la armonización de las distintas legislaciones nacionales en la lucha contra los

denominados «delitos informáticos» y hasta la fecha sólo ocho de los cuarenta y nueve países firmantes lo han ratificado.

Y eso pese a que en su Preámbulo se especificaba claramente la necesidad de «… aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional».

2. *El ámbito temporal*

A) Caducidad de los logs

El limitado espacio de los discos duros en los que se suelen almacenar los archivos de registro, hace necesario que transcurrido un tiempo, los *log*s más antiguos sean sustituidos por otros más modernos.

Dependiendo de los tamaños relativos del soporte en el que se almacenan y de los ficheros de *log*s, la sobreescritura se realizará con mayor o menor frecuencia.

Aunque en todos los delitos el tiempo transcurrido entre el hecho delictivo y el análisis de las evidencias es aconsejable que sea el mínimo posible, en los «delitos informáticos» o cuando las evidencias a investigar se hallen en sistemas informáticos con actividad, esta premura cobra mayor importancia por el riesgo de pérdida y destrucción que presenta este tipo de evidencia. Sin embargo, si el sistema informático no presenta actividad, los datos pueden permanecer inalterados indefinidamente.

Estos *log*s pueden encontrarse básicamente en tres lugares: en el ordenador de la víctima, en el del autor y los sistemas intermedios, entre los que se encuentra el proveedor de servicios de Internet.

Dependiendo del lugar en el que se hallen esos registros su riesgo de destrucción será distinto y los datos a intentar localizar serán también diferentes.

En el caso de sistemas informáticos intermedios, entre los que se destacan los PSIs, el principal escollo es el paso del tiempo, que podría hacer que la información, que *a priori* se habría almacenado para su posterior consulta por las autoridades, sea destruida al pasar el tiempo máximo de almacenamiento.

Así en España, a fecha de hoy, es inútil realizar una solicitud a un PSI sobre la identidad de una persona a la que se le asignó determinada dirección IP en una fecha anterior a un año.

La LSSI y CE establece un tiempo *máximo* para el resguardo de *log*s de 12 meses, pero no habla de un tiempo mínimo, con lo que en la práctica no existe normativa sobre el asunto.

Esto parece que va a cambiar, según se desprende del Anteproyecto de Ley de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, según el cual se está proponiendo que el tiempo mínimo de almacenamiento de estos datos sea de 12 meses, si bien también se contempla en la Disposición Final Tercera la posibilidad de ampliar o reducir el plazo de conservación hasta un máximo de 2 años o un mínimo de seis meses, previa consulta con los operadores.

B) Riesgo de destrucción de las evidencias

El riesgo de destrucción o la no existencia de evidencias puede deberse a varios factores, alguno de los cuales son ajenos a las voluntades, tanto de víctima como del autor.

Por ejemplo, en la víctima existen básicamente dos riesgos:

a) De que no se hallen activados los *log*s de los diferentes servicios, con lo que no quedaría ningún registro de las actividades realizadas en su equipo. Casi todos los sistemas operativos tienen la posibilidad de establecer unos sistemas de seguridad que permiten que se monitoricen determinados servicios o accesos.
   Lo que ocurre es que, dependiendo del nivel de formación de cada usuario y del sistema operativo utilizado, estas monitorizaciones se activan o no.
   Si bien existen sistemas que funcionan bajo el concepto de «seguro por defecto» hay otros en los que el concepto es de «permitido por defecto». Obviamente los datos que se pueden obtener de un sistema y de otro son completamente distintos. En el primero de ellos se configuran los servicios como «si no me lo permites expresamente todo está prohibido», en los segundos la filosofía es la contraria «si no me lo prohíbes está permitido» y como la seguridad es un concepto bastante engorroso la mayoría de usuarios medios prefiere prescindir de la seguridad a favor de una mayor usabilidad.
b) De que la información se borre. Si ante determinado ataque informático, el usuario procede a formatear el equipo informático y a reinstalar el sistema operativo y sus aplicaciones es más que probable que no puedan recuperarse los indicios necesarios para continuar la investigación.

El riesgo de no poder recuperar información aumenta exponencialmente cuanto más tiempo pase desde la comisión del delito, ya que en el funcionamiento normal de un sistema informático continuamente se están creando y borrando ficheros, pudiendo llegar a sobrescribir la información que se había borrado.

Si las evidencias a buscar se encuentran en el ordenador del presunto autor los riesgos de destrucción de evidencias son bastante mayores, dependiendo, eso si, de su capacitación técnica y su paranoia de seguridad.

Así, y a modo de ejemplo, se pueden señalar:

a) Que los *log*s de acceso a los servicios no se guarden. Generalmente motivado por el hecho de que no quiere que se almacenen datos en sus sistemas que puedan incriminarle.
   Si voy a acosar a jovencitas/os con un programa de mensajería instantánea, no voy a configurarlo para que se grabe toda mi actividad en disco duro.
b) Que utilicen sistemas externos de almacenamiento. Si no se puede acceder a esos sistemas no se podrá observar que guardaban en su interior. Un disco duro externo, con una capacidad de 1 *Terabyte* (cabrían unos 1.099.511.627.776 caracteres) tiene unas dimensiones de 180 × 110 × 40 mm) y puede ser fácilmente ocultable y trasladable.
c) *Sobreescritura* de registros. Si bien es factible recuperar información de un soporte lógico incluso una vez que se ha borrado el mismo, esta labor se dificulta con el tiempo ya que la información que se sobrescribe puede eliminar parte de la información subyacente imposibilitando su recuperación. A mayor paso del tiempo el riesgo es mucho mayor.
d) Borrado seguro. Se pueden utilizar programas informáticos que imposibilitan la recuperación de los archivos eliminados mediante la reescritura de los mismos una cantidad determinada de veces.
e) Destrucción física de una evidencia. El mejor método para evitar la recuperación de datos de un disco duro es su destrucción. Sin lugar a dudas, si un delincuente hace desaparecer físicamente su sistema de almacenamiento muy pocos datos podremos obtener por muy sofisticados que sean nuestros equipos.
f) Encriptación de contenidos. Esta encriptación puede realizarse de dos formas: o bien codificando un archivo con una clave o bien escondiendo un archivo dentro de otro.
   En el primero de los casos, mediante técnicas informáticas sería posible, en algunos casos el descubrir la clave de encriptación y

recuperar la información codificada. En estos casos estos ficheros son claramente visibles.

En el segundo de los casos también sería posible actuar contra esos ficheros, pero su detección es mucho más difícil y si no se conoce que algo está escondido ¿se buscaría? La respuesta es no.

3. *Participación criminal*

A) Existencia de varios usuarios

En el caso de que se pueda llegar a la identificación del ordenador desde el que se ha cometido el acto ilícito, no significa que se pueda lograr la individualización del usuario que gobernaba este sistema.

Esto es particularmente preocupante cuando al sistema origen pueden acceder una pluralidad de personas, y no sólo en el caso de locutorios y cibercafés, sino en un domicilio en el que convivan al menos dos personas.

Para poder señalar a uno de los potenciales usuarios serían necesarias otras gestiones, tanto técnicas como policiales.

Las técnicas pasarían por el análisis de los equipos informáticos interesados para estudiar la existencia de usuarios diferenciados u otros indicios que pudieran indicar la autoría de los hechos.

Las gestiones policiales serían las tradicionales tomas de declaración.

B) Falta de gravedad del delito

En un gran número de casos de los denominados «delitos informáticos» la gravedad de los mismos no suele ser elevada, lo que dificulta la adopción de medidas restrictivas de derechos fundamentales, como pueden ser la intervención de las comunicaciones y las entradas y registros.

Sin embargo, en caso de no concederse las mismas, se dotaría a estos delitos de una impunidad casi absoluta, teniendo en cuenta que los últimos indicios se ubicarían en los ordenadores utilizados para realizar las conductas delictivas y estos se pueden hallar instalados en domicilios privados.

Cuando siguiendo todos los pasos para la averiguación de la autoría de un hecho delictivo y superando todos aquellos obstáculos con los que cualquier investigación se topa, se logra llegar hasta el número de teléfono (o la ubicación del Terminal de comunicaciones) en el que se ha originado la conexión a Internet, no se pueden lanzar las campanas al

vuelo, ya que aunque la dirección IP identifique una máquina, no individualiza a su usuario.

Para poder identificar al usuario responsable de la conducta ilícita es preciso ahondar más en la investigación y el único paso posible para ello pasa por la intervención del ordenador y del *router* utilizados para intentar determinar la autoría.

Aunque este es el único paso positivo a dar, en ocasiones nos encontramos con que la entidad del delito no es tan grave como para justificar una diligencia tan gravosa como es la entrada y registro en un domicilio y la misma se deniega por la autoridad judicial. En tal caso, nada puede hacerse ya para seguir la investigación.

C) Sistemas facilitadores del anonimato

Existen en Internet numerosos sistemas que permiten ocultar o disfrazar una comunicación haciéndola muy difícil de rastrear. Estos sistemas pueden haber sido diseñados por sus autores para ocultar la navegación de forma consciente o simplemente consisten en utilizar sistemas informáticos mal configurados a los que se puede tener acceso, y que sirven como trampolines entre los que ir saltando para tratar de despistar a las Autoridades que deseen investigar determinada actividad.

Por ejemplo si una persona decide atacar el ordenador de otra puede hacerlo directamente, pero en este caso es posible que la dirección IP utilizada por el atacante pudiera ser rastreada hasta el origen.

Pero también puede optar por hacer uso de sistemas intermedios, de esta forma, conociendo que existen numerosos *proxy*s con acceso a y desde Internet mal configurados, hace una lista de varios de ellos (frecuentemente ubicados en distintos países) y accede secuencialmente a varios de ellos para lograr finalmente atacar a su víctima. En este caso los investigadores deberían ir hacia atrás en el ataque e ir descubriendo todos y cada uno de los sistemas intermedios utilizados.

Si se han usado los suficientes, el tiempo invertido para lograr la identificación última hará que la obligación del PSI de identificar al atacante haya caducado, o que alguno de los sistemas intermedios no guarde registros que permitan continuar con la investigación.

D) Conexiones wifi

Las conexiones *wifi*, tal y como están siendo instaladas, se comportan de hecho como un nuevo sistema de anonimato en las comunicaciones.

Se ha comprobado que los diferentes proveedores de acceso a Internet dotan a sus nuevos clientes de sistemas de comunicación inalámbricos (*wifi*) cuando firman el contrato con ellos.

Estos dispositivos, en la inmensa mayoría de los casos estudiados, venían instalados con las opciones básicas de seguridad, las contraseñas de acceso a los mismos eran conocidas de sobra en los foros de Internet y los sistemas de registro de *log*s, caso de existir se encontraban desactivados.

Así las cosas es relativamente fácil para un usuario medio con algo de interés por el «reverso tenebroso» de la informática hacerse con el control de uno de esos dispositivos y utilizarlo para sus conexiones.

Si las acciones que realiza este individuo se limitan a navegar por la Red, el único perjuicio que causará al usuario legítimo sería la merma en la velocidad de acceso a Internet, pero si por el contrario el uso es la descarga y/o envío de pornografía infantil, los perjuicios para el legítimo usuario podrían ser más importantes: desde la imputación de un delito hasta la entrada y registro en su domicilio, pasando por la incautación de los sistemas informáticos.

Por todo ello, es importante que en las diligencias de entrada y registro se proceda también a la incautación y posterior estudio de los *router*s utilizados para la conexión a Internet, para poder descartar la existencia de otros sospechosos de las conductas investigadas.

4. *Otros*

A) Oscuridad en la tipificación penal

Otro de los problemas con los que nos encontramos es, a mi juicio, falta de concreción en el articulado del Código Penal, lo que redunda en que ante determinada situación los agentes no tengan claro como actuar.

Hay que tener en cuenta que para tomar una decisión, jueces y fiscales disponen del tiempo suficiente para ello, sin embargo, los agentes son generalmente sorprendidos por la actuación a la que deben dar una respuesta, y esto sin tener los amplios conocimientos que disponen los estamentos judiciales.

Se deberían aclarar determinados artículos del Código Penal para que la Policía pueda realizar su labor correctamente.

Sólo a modo de ejemplo voy a detallar uno de los que ha suscitado más controversia, sobre todo por la gran repercusión que las conductas absolutorias tienen en la sociedad, el de los delitos contra la propiedad intelectual.

Antes de la LO 15/2003 de modificación del Código Penal, este tipo de delitos eran de los considerados semipúblicos, es decir, se precisaba denuncia de los afectados para poder perseguirlos, salvo que concurriesen determinadas circunstancias, siendo la más importante la de que el delito afectase a varios perjudicados.

Con esos parámetros era difícil perseguir la piratería y por ello el legislador habilitó a los agentes para actuar sin que existiese denuncia previa. Uno de los objetivos de esta reforma, desde mi punto de vista era el poder atajar la venta ilegal de CDs en las calles debido a su inmediatez, ya que otras investigaciones a más alta escala no tienen la urgencia de aquellas y es posible esperar a la interposición de las denuncias por parte de los perjudicados.

Pero, sin embargo, ante la misma acción: venta ambulante de CDs pirateados, las sentencias son dispares, unas condenatorias y otras absolutorias y eso cuando la legislación a aplicar es la misma. Esto aporta un punto de oscuridad que es preciso aclarar.

Otro aspecto que arroja dudas se concentra en la transmisión de obras protegidas por medio de las redes de compartición entre iguales denominadas genéricamente P2P.

Según la circular n.º 1/2006 de Fiscalía, estas conductas realizadas entre particulares serían impunes, al carecer del ánimo de lucro comercial necesario para su incardinación dentro del tipo penal. No obstante existen sentencias en las que se condena a los usuarios por poner a disposición y/o descargarse obras protegidas, aunque también existen otras que los absuelven.

B) ¿Escasa formación de los estamentos judiciales en temas informáticos?

La irrupción en nuestra sociedad de las tecnologías de la información en general y la de Internet en particular ha tenido lugar de una manera vertiginosa. Lejos de la calma con la que otros desarrollos tecnológicos llegaron a nuestras vidas, en pocos años los ordenadores se han hecho un hueco muy importante en nuestros puestos de trabajo y ya no sólo en el ámbito laboral, sino también como forma de ocio y comunicación.

Los avances en la miniaturización de componentes y el abaratamiento en la fabricación de los mismos ha determinado que el acercamiento de los usuarios a esas tecnologías sea cada vez más fácil, puesto que la reducción de los costes de manufacturación de los sistemas informáticos posibilita su adquisición de forma masiva por parte de los consumidores.

Estos cambios han tenido como protagonistas a nuestros hijos, quienes parecen que han nacido con un séptimo sentido dirigido a entenderse con esos conglomerados de *chip*s unidos por senderos de cobre.

Es curioso observar cómo cualquier tierno infante es capaz de lograr el control de cualquier consola u ordenador en breves minutos y cómo, sin leer ningún tipo de instrucción, manejar con destreza cualquier juego informático al que se enfrente, acción que los de mayor edad sólo podemos lograr tras repetidas lecturas de los manuales.

A las personas que en nuestros días rondan la cincuentena, estos cambios les ha «pillado» un poco a contrapié, de la misma forma que a la generación anterior le pilló a desmano la proliferación de los reproductores y grabadores de vídeos.

El conocimiento que generalmente tienen de estas nuevas tecnologías, salvo determinados casos, se limita a hacerlos funcionar con las opciones básicas que se van aprendiendo a partir de la experimentación.

El habernos «pillado» con una cierta edad estos cambios tecnológicos ha impedido que comprendamos con profundidad su forma de funcionamiento. Este distanciamiento hace que muchas de las personas con las que tengo que mantener reuniones de trabajo, siempre comiencen sus alocuciones con «yo es que de ordenadores sé lo justo». Esta especie de disculpa, manifiesta la relación de amor-odio que se establece con los sistemas informáticos y parece ser que se precisa una justificación por no comprender los protocolos de Internet.

Cuando yo me dirijo a la consulta de un médico, no le digo «perdona pero yo de medicina entiendo lo justo». Con uno de los dos que sepa del tema, creo que sobra; se trata de colaborar, de trabajar en equipo. A la reunión uno lleva el problema y el otro el conocimiento. Lo mismo viene a pasar en el tema que nos toca.

Esto viene a colación con algunas afirmaciones que determinados estamentos hacen sobre el pretendido desconocimiento que jueces y fiscales tienen de los temas informáticos. Desde mi punto de vista, si bien sería muy interesante que comprendiesen mejor como funciona este mundo, no es del todo imprescindible.

Lo que le exige la sociedad a Jueces y Fiscales es que sepan discernir entre lo que es delito y no lo es, no que comprendan como se ha producido, de la misma forma que ante un homicidio deben de dilucidar quién ha realizado la conducta y cómo lo ha hecho, no siendo imprescindible que comprendan el mecanismo físico por el que la vida se ha escapado del cuerpo de la víctima.

En mi experiencia profesional, muy pocas veces me he encontrado con problemas de comprensión con estos estamentos que hayan tenido su base en un problema técnico, pues a fuerza de ser sincero, y tras las explicaciones que les hemos aportado, han entendido lo suficiente para hacerse una composición de lugar sobre cómo se ha podido producir el delito y el porqué de las solicitudes que les realizábamos.

Se ha hablado mucho sobre la necesidad de que existan jueces y fiscales especialistas en «delitos informáticos» y aunque obviamente la especialización siempre aporta un plus de calidad al trabajo realizado, no creo que deba ser imprescindible, ni que el hecho de que no existan estas especialidades impida la persecución de los delitos. Sobre todo porque la gran mayoría de los denominados «delitos informáticos» no son más que delitos tradicionales que utilizan las nuevas tecnologías de la información para facilitar su comisión, o bien para impedir el descubrimiento de su autoría.

Aunque sí existen otros delitos en los que el objetivo de los mismos sí son las redes de ordenadores, estos no son los más numerosos.

Sin embargo esta especialización sí sería conveniente que se diese en los legisladores, para que los nuevos delitos detectados sean rápidamente añadidos al Código Penal y otras leyes que faciliten su prevención y si ésta no ha sido posible, su persecución.

Es de todos sabido que los delincuentes suelen ir por delante de la ley y sus agentes en sus conductas ilícitas y ésta tiene que ir paulatinamente adaptándose a nuevas formas comisivas o incluso a nuevas actividades que cuando sus artículo fueron redactados eran imposibles de cometer.

Así, en el ordenamiento actual, el denominado «*hacking* blanco» podría ser impune. Estas palabras tratan de definir las conductas de aquellas personas que intentan acceder a sistemas informáticos sin ningún ánimo dañino, únicamente para probar vulnerabilidades y avisar a sus administradores, o por un reto personal de superación.

Existen controversias en lo referente a si estas conductas deberían sancionarse o no. Por un lado están los defensores de los autores quienes justifican su actividad en la mejora general de la seguridad informática, ya que gracias a estos individuos se conocen vulnerabilidades que de otro modo quedarían ocultas, excepto para unos cuantos especialistas y las compañías de *software* no podrían modificar sus productos para adecuarlos a los nuevos requerimientos de seguridad. Por otro lado están los que justifican que los administradores de sistemas no tienen por qué soportar el acoso constante de estos individuos que intentan lograr acceso a sus máquinas y redes.

El símil en la vida real es muy conocido, pues ha sido publicado en numerosas ocasiones. Se trataría de un individuo que va probando puerta por puerta si esta está abierta o si se puede abrir. Una vez abierta, no sustraería nada y en algunos casos dejaría una nota al propietario informándole de que su casa es vulnerable.

En el caso de que un sujeto de estos fuese pillado *in fraganti* desconozco cual sería el veredicto final del Juez, pero me parece que sus

antecedentes penales ya no seguirían en blanco, y esto tiene su lógica, puesto que una vez obtenido el acceso a un lugar, sería difícil no «echar una miradita».

En nuestro ordenamiento jurídico estas conductas son, desde mi punto de vista y reitero mis limitaciones jurídicas, atípicas, puesto que para que pudieran incardinarse en un delito de daños deberían realizar cuando menos alguna modificación en algún fichero de los sistemas atacados. Si este parámetro no se diera, el delito no existiría. El otro posible encuadre de esta conducta es el de descubrimiento de secretos, pero para ello sería necesario constatar que se ha accedido a información reservada.

En el Proyecto de ley de modificación del Código Penal, se está intentando poner freno a esta situación según se desprende de la redacción del siguiente texto:

> «Se caracterizan como delitos las intromisiones ilegales en sistemas informáticos ajenos (*hackers*). Se castigarán tanto los ataques contra la intimidad como los posibles delitos por daños que puedan producir grave perjuicio a empresas u organismos públicos. También queda tipificada como delito la clonación, uso y posesión de tarjetas de crédito.»

IV. **Conclusiones**

A modo de conclusión, me gustaría señalar que para la efectiva protección de la sociedad frente a esa parte de la misma que únicamente busca su beneficio en detrimento de los del resto, aquélla debería dotar a los encargados de su protección de las herramientas necesarias para que puedan cumplir su labor con eficacia. En caso contrario, la impunidad para esas acciones compensará a los delincuentes, ya que disminuirá de forma importante, el riesgo de ser detenidos.

La lucha contra la delincuencia es desigual puesto que únicamente una de las partes está sometida a control y a las leyes, mientras que la otra campa por sus respetos.

La obtención de los datos almacenados en bases de datos para la investigación de delitos debería, siempre a mi modo de ver, ser mucho más ágil de lo que es ahora. Y conste que no pretendo sugerir que se elimine el control judicial de lo solicitado, sino que el mismo pueda ser realizado *a posteriori*.

Me refiero a que ante la investigación de un delito en concreto, la Policía pueda recabar de los proveedores de servicio de Internet, de

compañías telefónicas, bancos y cuantos servicios se hallen implicados en la comisión de este delito en concreto aquellos datos necesarios para la identificación del autor.

Posteriormente todos estos datos tendrían que ser validados por la Autoridad Judicial, sin cuyo refrendo no podrían ser utilizados en el juicio oral.

De esta forma se dotaría de una mayor efectividad a las investigaciones que podrían realizarse con una gran inmediatez.

Es importante recalcar que los datos así obtenidos lo serían *únicamente* para la investigación *de un delito concreto*, nunca para una prevención del delito en general. No se trata de recrear «el Gran Hermano» de Orwell, sino de dotar de herramientas eficaces a los investigadores.

Responsabilidad penal de los proveedores de enlaces

José Manuel Ortiz Márquez
Fiscal del Tribunal Superior de Justicia del País Vasco

I. **Planteamiento**

En Internet operan distintos sujetos que la doctrina ha identificado de forma pacífica, hasta el momento, como proveedores de acceso, proveedores de servicio y proveedores de enlaces. Desde el punto de vista del derecho penal material se plantea la cuestión de determinar la responsabilidad penal de estos operadores respecto de las conductas delictivas que se cometen a través de medios telemáticos. A grandes rasgos y con carácter general, se entiende que el proveedor de acceso está exento siempre de responsabilidad penal, el proveedor de servicios cuando acredite que desconocía el contenido ilícito que se alberga en su servidor o bien, conociéndolo, acredite que no disponía de los medios técnicos necesarios para eliminar dicho contenido de su servicio.

La distinción entre el proveedor de accesos y el proveedor de enlaces se basa en el control que tenga el proveedor sobre los contenidos a los que remite, es decir, si puede controlarlos individualmente o por el contrario, proveer una conexión a datos en el servidor de terceros que el proveedor no puede desactivar individualmente —porque sólo puede activar o desactivar el conjunto de las conexiones— sólo se califica como proveedor de acceso. Por este motivo el proveedor de acceso siempre estará exento de responsabilidad penal pues nunca podrá decirse que tiene el dominio del hecho, es decir, no puede impedir el acceso a un contenido determinado, o permite el acceso a todos o a ninguno.

El objeto de esta ponencia es determinar responsabilidad penal del proveedor de enlaces por los contenidos ilícitos de las páginas web a las que reenvía a través de conexiones preestablecidas en su propia página, así como poner de manifiesto la suficiencia o insuficiencia de las normas penales vigentes para dar respuesta a los distintos supuestos que se pueden plantear. Como veremos, la misma idea que sirve para distinguir al proveedor de accesos del proveedor de enlaces, servirá para determinar

la responsabilidad penal del último. Esa idea es el dominio del hecho, el control que el proveedor de enlaces tenga sobre el acceso que oferta al usuario de su página de acceder a otras. Para ello es necesario analizar, con carácter previo, como funcionan los proveedores de enlaces y, desde este punto de vista, clasificarlos.

II. **Aspectos técnicos de los proveedores de enlaces**

Para alcanzar el fin propuesto debe hacerse referencia con carácter previo a las distintas clases de proveedores de enlaces que operan en Internet y cómo funciona cada uno de ellos. En este sentido, debe distinguirse entre los proveedores de enlaces que ponen a disposición del usuario mecanismos de búsqueda de páginas web, mostrando al usuario una serie de enlaces relacionados con las palabras o frases previamente introducidas por este (buscadores) y aquellos que incluyen como contenido de sus páginas web enlaces a otras páginas. En este último supuesto debe diferenciarse a su vez, entre los *link*s o enlaces y los *banners* o pancartas.

1. *Proveedores que incluyen en sus contenidos instrumentos de búsqueda*

Como se ha dicho anteriormente, antes de analizar la responsabilidad penal de estos sujetos es necesario hacer referencia al funcionamiento de los mismos y, en concreto, al mecanismo empleado para seleccionar los directorios que van a ser mostrados al usuario una vez que este ha rellenado los campos exigidos por el buscador con palabras clave o frases clave. Desde este punto de vista y relevante a los efectos del tema que estamos tratando, podemos distinguir tres clases de buscadores.

A) Índices

Son los buscadores que mantienen una organización de las páginas incluidas en su base de datos por categorías, es decir, tienen un directorio navegable de temas. Dentro de cada directorio podemos encontrar páginas relacionadas con ese tema. Para mantener esta organización, los buscadores tienen unos administradores humanos que se encargan de visitar las páginas y vigilan que todas se encuentren clasificadas en su lugar correcto. Índices típicos son Yahoo, Terra o TodoEnlaces.

Para que una página quede registrada en un índice hay que mandar la dirección a los administradores humanos de ese índice. La página pue-

de estar elaborada por cualquier persona física o jurídica, generalmente acompañada de una serie de datos que les ayuden a clasificar la página de una forma correcta, como la descripción, temática, título, lenguaje, etc. Además, si se desea que varias páginas de un sitio web estén en el buscador, deben registrarse todas ellas una a una.

B) Motores de búsqueda

Son buscadores que basan su recolección de páginas en un robot, denominado araña, que recorre constantemente Internet en busca de páginas nuevas que va introduciendo en su base de datos automáticamente. Los motores de búsqueda no tienen por qué tener un índice, aunque cada vez es más habitual que dispongan de uno. Motores de búsqueda típicos son Altavista o Sol.

Los motores de búsqueda no necesitan que se les mande la dirección de la página para tenerla en su base de datos, puesto que el robot puede haberla encontrado previamente. De todos modos, es posible mandarles la dirección si no se quiere esperar a que el robot la encuentre, práctica muy habitual.

Para clasificar una página, los motores de búsqueda son capaces de leer el contenido de ésta y encontrar aquellos datos que permitan su catalogación. Por eso, cuando se registra una página en un motor de búsqueda, generalmente, no piden información adicional, como ocurre con los índices.

Cuando un robot recorre la página guarda sus datos y luego se dirige a las distintas páginas que están enlazadas a esta. De este modo, solo hace falta registrar la página inicial de un sitio web, pues el motor de búsqueda se encargará de recorrer todo el sitio de manera automática. Adicionalmente, estos motores o arañas, volverán a recorrer las páginas de su base de datos en busca de cambios que se hayan producido en estas, con objetivo de mantener su información lo más actualizada posible.

C) Multibuscadores

Estos últimos no tienen una base de datos propia, lo que hacen es buscar la página en unos cuantos motores de búsqueda e índices y combinar los resultados de la búsqueda en esos buscadores. Como ejemplos de multibuscadores podemos destacar Meta buscador de desarrollo web, en castellano, o *Metacrawler*, en inglés.

Para registrar una dirección de manera que aparezca en un multibuscador debemos mandársela a algún buscador donde éste va a recoger los resultados.

También entendemos que es relevante a los efectos del tema propuesto la clasificación de los buscadores por el tema: genéricos, donde podemos encontrar todo tipo de páginas, y específicos, donde solo hay páginas que tratan sobre una temática determinada.

D) Registro de las páginas web

Esta cuestión es muy importante en relación a los buscadores pues incide directamente en el funcionamiento de los mismos. Existen unas reglas y recomendaciones básicas para conseguir que el buscador localice fácilmente la página web. Existen una serie de técnicas al efecto. Sin embargo, hay que tener en cuenta que el uso excesivo de estas puede ser contraproducente ya que muchos motores de búsqueda interpretan que la página esta haciendo «trampa» para situarse entre los primeros puestos de manera injusta. Cuando esto sucede la página es catalogada como *spam page* o «página tramposa». Entonces será relegada por el buscador a los últimos puestos en los resultados de manera automática.

De lo expuesto, se deduce que las posibilidades de que el buscador remita al usuario a una determinada página web con contenidos ilícitos dependerá del acierto que el creador de la misma haya tenido a la hora de manejar esas técnicas, entre otras, las palabras clave, frases clave y descripciones contenidas en la página creada, lugar de la misma en el que esas palabras, frases y descripciones se encuentren situadas dentro de la página (título, primer párrafo, etiquetas META o META *tags*, éstas empleadas únicamente por los motores de búsqueda).

Pero además, se ha de tener en cuenta que un *link*, desde una página, no sólo envía visitas al sitio web al que apunta sino que, desde la aparición del sistema de posicionamiento por popularidad introducido por Google con su mecanismo de *PageRank*, si es de un tipo determinado, en concreto *<A HREF=…* se considera como un «voto» al sitio que recibe el enlace, lo que ayuda a mejorar su posición en los resultados de las búsquedas. Por eso es necesario que se puedan contabilizar los *clicks* que hacen los usuarios en los enlaces salientes. En este sentido debe tenerse en cuenta que en los programas de intercambio de *links* por efectividad, también conocidos como *tops*, los *links* salientes no son «verdaderos *links* hacia el sitio destino», sino que al tomar la forma *<a href= «out.php?URL = www.sitiodestino.com»>* este enlace, para Google, es un enlace a una página interior de nuestro sitio. Por ello Google ignorará el parámetro recibido por el *script* por no considerar el destino del enlace como «real». Por lo tanto, en este caso concreto, se añade un factor más, de carácter mecánico, relevante a la hora de

determinar las posibilidades de que un motor de búsqueda ofrezca una determinada página al usuario.

En relación con lo expuesto en el párrafo anterior, según la propia documentación de Google, el *Googlebot*, el robot de Google que periódicamente explora la web, es capaz de seguir sólo enlaces de dos tipos: *anchors* (<*A HREF=*… >) e imágenes (<*IMG SRC=*… >). La misma documentación también aclara que Google es incapaz de seguir enlaces desde *flash*, *javascript* y parámetros en los enlaces a otras *URLs*. Otros *webmasters*, optan por tener un mayor control del intercambio, e instalan programas de gestión de intercambios (como ser *AWG Trade*, *Traffic Drive*, *CJ-Ultra*, *TM3*, etc). Pero al instalar estos programas, los enlaces desde sus sitios web dejan de ser seguidos por los robots de los buscadores (*crawlers*). Por lo tanto, las visitas que un usuario realice a una página web cuyo directorio figura como enlace en otra que ha visitado previamente, si esta impide que el *clic* que el usuario realiza en el *link* pueda computarse mediante alguna de las técnicas enumeradas el robot buscador de Google no contabilizará el *clic* y no dará puntos a la página receptora de una visita por reenvío de otra.

2. *Proveedores que incluyen en sus contenidos directorios*

A) Links

Son enlaces a otras páginas web incluidos en una determinada. Pueden clasificarse en enlaces salientes y entrantes. De esta clasificación, a los efectos de la cuestión que estamos tratando, únicamente nos interesan los enlaces salientes pues son aquellos enlaces, para entendernos, en sentido propio, es decir, la remisión que una página efectúa a otra. Sin embargo, los enlaces entrantes son las visitas recibidas por una página a consecuencia de la remisión de otra. Enlaces salientes y entrantes son las dos caras de una misma moneda.

B) Banners o pancartas

Son rectángulos insertados en una página web consistentes en imágenes o en animaciones que publicitan un determinado lugar en la Red y que constituyen a su vez un enlace hacia la página publicitada.

Si bien, desde el punto de vista técnico, no existen grandes diferencias respecto de los *links*, si las hay respecto de los sujetos que deciden su inclusión en la página web que sirve de soporte publicitario. Así la incorporación a la página puede ser efectuada por:

1.º El administrador de la web
2.º Empresas de gestión, dentro de las cuales:

—algunas supervisan antes el contenido de las páginas a las que van a dar publicidad a través de los *banners* que deberán ser validados y moderados antes de su publicación y se reservan la facultad de modificarlos, editarlos o rechazarlos sin previo aviso, así como de suprimir o retirar de los distintos servicios de la web toda información que pudiera resultar ilegal o simplemente ofensiva y
—otras no se hacen responsable de la información contenida en los enlaces de webs a terceros que figuren en el sitio web. Esto, sin perjuicio de la efectividad real que pueda tener en el orden penal, es relevante a los efectos de la omisión impropia, como más adelante veremos.

3.º Intercambio de *banners*: que puede tener lugar a través de una de las dos vías anteriormente señaladas.

III. **Cuestiones jurídicas**

1. *Cuestiones previas*

Concluida la exposición de los aspectos técnicos, es hora de entrar en materia. Al tratar el tema de la responsabilidad penal de los proveedores de servicios de la sociedad de la información, ya sean de acceso, de servicios o de enlaces, la doctrina se ha planteado dos cuestiones de carácter general, la primera, la consideración de las disposiciones de la Ley 34/02 de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) en el campo del Derecho Penal. Dicha ley supone la trasposición al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) y de la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, si bien esta última con carácter parcial.

La segunda, si es aplicable a los delitos cometidos a través de Internet la «responsabilidad en cascada» regulada en el artículo 30 del Código Penal de 1995 para los delitos cometidos a través de medios o soportes de difusión mecánicos.

A) Las disposiciones de la LSSICE

De las disposiciones contenidas en dicha ley, una de ellas, el artículo 17, se refiere a la responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda. Este artículo se estructura en dos párrafos y tienen el contenido siguiente:

> «1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:
>
> a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
>
> b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.
>
> Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
>
> 2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos».

Evidentemente, este precepto que acabamos de transcribir no se refiere a la responsabilidad penal de los proveedores de enlaces, sino a la responsabilidad disciplinaria de los mismos regulada en el Título VII, arts. 37 a 45 de la L 34/02. Sin embargo, estos supuestos de exención de responsabilidad sancionadora en ámbito administrativo, ya están previstos en el Derecho Penal, de modo que el apartado 1.a) del art. 17 hace referencia al dolo, acogiendo en este sentido el concepto de dolo neutro, conocer y querer la realización de los elementos del tipo. De esta manera, la conducta realizada por el administrador de una página web al incluir en la misma un enlace a otra con un contenido ilícito, en primer lugar debe poder subsumirse en el tipo penal, si se le está imputando en la correspondiente causa en concepto de autor y en segundo lugar, ha de conocer la existencia del contenido ilícito o al menos que se

represente su existencia como probable a efectos de poder mantener la existencia de dolo eventual.

El apartado 1.b) tiene su reflejo en el art. 16 párrafos 2 y 3 del Código Penal o en el concepto de autor, en concreto en el tercero de los requisitos establecidos por la Jurisprudencia del Tribunal Supremo, el dominio del hecho.

Respecto de los párrafos segundo y tercero del art. 16, porque, evidentemente, el supuesto previsto en párrafo 1.b) del art. 17 LSSICE constituye para el Derecho Penal un supuesto de desistimiento, lo que determina según el citado artículo del Código Penal la exención de responsabilidad penal. Lógicamente, de existir el mismo la exención de responsabilidad no opera, tal y como queda reflejado en el apartado segundo del artículo 17.

Respecto del tercero de los elementos del concepto de autor, previamente tener en cuenta que los dos primeros se refieren a la realización de alguno de los elementos del tipo y a la realización de los mismos con ánimo de autor, esto es, concebir el acto que realiza como un acto propio y no como el acto de otro al que contribuye. Esto supone que el enlace ha de poder subsumirse en la conducta descrita en el precepto penal y que el *webmaster* ha de concebir la remisión desde su web a la página en la que se encuentra el contenido ilícito como un acto propio. Pero volviendo al tercero de los elementos, el dominio del hecho, en relación con el apartado b) el supuesto previsto en dicho apartado supone tanto como excluir tal dominio puesto que si actúa con diligencia para suprimir o inutilizar y no lo consigue, no detenta el mentado dominio. Ello sucede respecto de los *links*, *banners* o índices pero no ocurre si hablamos de motores de búsqueda pues como hemos visto se trata de un robot que sigue una serie de parámetros para buscar las páginas a las que reenviar y mostrarlas al usuario en un orden que depende de múltiples factores a los que hicimos referencia y que se escapan al administrador de la web.

El último párrafo del apartado primero que establece una serie de supuestos en los que se presume *iuris et de iure* el conocimiento de los contenidos ilícitos por el *webmaster*, no es aplicable en el campo del derecho penal material puesto que consagra un supuesto de responsabilidad objetiva incompatible con el principio de culpabilidad, base de la responsabilidad penal, pero pueden servir como medios de prueba de los que podrá valerse el Fiscal para sostener la acusación y acreditar el dolo del proveedor de enlaces, además, en su caso, de poder constituir un delito de desobediencia.

En el derecho comparado alemán encontramos el referente del Estatuto de los Teleservicios (TDG) en cuyo § 5 estipula:

«1. Los proveedores de servicios son responsables, según las disposiciones legales generales, por los contenidos propios que ponen a disposición de los usuarios.

2. Los proveedores de servicios sólo son responsables por contenidos de terceros que ponen a disposición de los usuarios si tienen conocimiento de estos contenidos, están técnicamente capacitados para impedir su utilización y se puede esperar razonablemente de ellos que lo hagan.

3. Los proveedores de servicios no son responsables por los contenidos de terceros, a los que sólo proporcionan acceso. El almacenamiento automático y provisional de contenidos de terceros respondiendo a la demanda de un usuario es considerado equivalente a proveer acceso.

4. El deber de impedir el acceso a contenidos ilegales bajo las disposiciones generales de la ley no ha sido modificado si el proveedor de servicio tiene conocimiento de esos contenidos en cumplimiento del requisito de privacidad de las telecomunicaciones bajo el § 85 de la Ley de Telecomunicaciones, si es técnicamente capaz de impedir el acceso y si se puede esperar razonablemente que así lo haga.»

Lo estipulado en la § 5 del TDG limita cualquier responsabilidad potencial de un proveedor de servicios en cualquier ámbito de la ley, independientemente del tipo de acción judicial emprendida. Se aplica a la responsabilidad civil, penal y administrativa.

B) El art. 30 del Código Penal

El art. 30 CP reza:

«1. En los delitos y faltas que se cometan utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente.

2. Los autores a los que se refiere el artículo 28 responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden:

1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo.

2.º Los directores de la publicación o programa en que se difunda.

3.º Los directores de la empresa editora, emisora o difusora.

4.º Los directores de la empresa grabadora, reproductora o impresora.

3. Cuando por cualquier motivo distinto de la extinción de la responsabilidad penal, incluso la declaración de rebeldía o la residencia fuera de España, no pueda perseguirse a ninguna de las personas comprendidas en alguno de los números del apartado anterior, se dirigirá el procedimiento contra las mencionadas en el número inmediatamente posterior.»

Respecto de la aplicación del artículo trascrito, existen dos posturas encontradas. Manuel Gómez Tomillo defiende la aplicación del art. 30 a los delitos cometidos a través de Internet siempre y cuando la conducta consista en difundir un contenido ilícito, entendiendo que no cabe mantener la inaplicación de dicho precepto amparándose en que el ordenador no es un aparato mecánico sino técnico, por las siguientes razones:

1.ª Con el paso del tiempo y de la evolución de la tecnología el art. 30 quedará vacío de contenido pues los medios mecánicos quedarán obsoletos.
2.ª Teleológica: por la finalidad del precepto, cual es salvaguardar la libertad de expresión a la vez que se lucha contra el anonimato.
3.ª El concepto de «mecánico» que tiene en cuenta el precepto es amplio puesto que se incluye al director de un programa o de la empresa de emisión.
4.ª Etimológica: el ordenador es una máquina.
5.ª Igualdad: puede llegar a darse un tratamiento distinto a supuestos iguales. Por ejemplo, una información injuriosa que se publica en un periódico, tanto en su edición impresa como en la edición digital. Al primer supuesto le sería de aplicación el régimen especial de la autoría previsto en el art. 30, mientras que en el segundo supuesto el autor de la información y los partícipes en la difusión de la misma responderían conforme a las reglas generales previstas en los arts. 28 y 29 del CP.
6.ª La analogía *in bonam partem*. En el caso de que se entienda que bajo la expresión «medios mecánicos de difusión» no queda incluido Internet siempre cabe la aplicación por analogía pues esta sería a favor del justiciable pues determina la exclusión de la punibilidad de la conducta, siempre que la acción penal pueda dirigirse contra uno de los responsables previstos en el precepto en un estadio anterior.

Oscar Morales García, por el contrario, considera que el art. 30 no es aplicable a los delitos cometidos a través de Internet por los siguientes motivos:

1.º Existen servicios de la sociedad de la información que son excluidos del concepto de difusión por la legislación sectorial como sucede con la transmisión punto a punto, por lo que, en este caso, aunque se entienda que estamos ante un medio mecánico no lo es de difusión y por lo tanto no será aplicable el art. 30 del Código Penal.

2.º Por «máquina» hay que entender una estructura compleja o conjunto de estructuras alimentada de energía y susceptible de funcionar cada uno de los elementos de la estructura por sí solo. Este concepto no es aplicable a Internet pues no funciona por sí misma sino que es un medio técnico que permite el tráfico de información.

3.º La dificultad de subsumir a los sujetos que operan en Internet en los sujetos a los que se refiere el art. 30. Así, para poder dirigir algo, ese algo, la información en este caso, ha de ser limitado, mientras que en Internet esta se caracteriza precisamente por ser inabarcable, salvo excepciones, por ejemplo, las ediciones digitales de los periódicos, pero si a partir de este supuesto se quiere extender la aplicación del art. 30 a todo Internet, entiende este autor que se está confundiendo la parte con el todo. Por otro lado, la dificultad de aplicar a sujetos que operan en Internet los conceptos de impresión, grabación o emisión.

4.º Incompatibilidad del régimen de responsabilidad del art. 30 con el régimen de responsabilidad establecido por la LSSICE y al que ya hemos hecho referencia.

Desde nuestro punto de vista, entendemos preferible la última de las posiciones expuesta, puesto que la primera tiene una serie de objeciones que son las siguientes:

1.ª No cabe la aplicación analógica en nuestro Derecho Penal, conforme a lo dispuesto en el art. 4 del Código Penal y la interpretación que de dicho precepto ha establecido el Tribunal Supremo en su Jurisprudencia, en concreto en la referida al párrafo tercero. El Alto Tribunal ha entendido que la analogía *in bonam partem* queda excluida por lo dispuesto en los párrafos primero —que prohíbe la aplicación de las normas penales a supuestos distintos de los previstos en ellas— y tercero del art. 4 —este último obliga al Juez a dirigirse al Gobierno exponiéndole las razones pertinentes cuando considere que una conducta no deba ser penada y resulte serlo por la aplicación rigurosa de la ley—. Esta doctrina resulta aplicable al supuesto planteado por el profesor Gómez Tomillo pues supone aplicar una exención de responsabilidad penal a un sujeto que no está contemplado por la norma que contiene dicha exención, es decir, el art. 30 del Código Penal.

2.ª La igualdad alegada por Gómez Tomillo entre los sujetos que realizan una misma acción, si bien a través de medios distintos,

en un caso telemáticos y en otros en papel, queda igualmente rota. Esa ruptura no se produce respecto del supuesto mencionado sino, como pone de manifiesto el profesor Morales García, en muchos supuestos que nos podamos encontrar en Internet al no ser posible la subsunción de sujetos que operan en la web en los sujetos contemplados en el art. 30.

3.ª En relación con lo dicho anteriormente, la aplicación del art. 30 no está exenta de problemas, en función del proveedor de acceso, de servicios o de enlaces al que nos estemos refiriendo.

4.ª Finalmente, entendemos que el art. 30 es un precepto obsoleto que debe desaparecer por dos motivos. El primero, porque tal y como reconoce el profesor Gómez Tomillo los medios mecánicos a los que hace referencia el precepto están desapareciendo. El segundo, porque entendemos que actualmente el art. 30 no tiene razón de ser. Su introducción en el ordenamiento jurídico español tiene lugar cuando la libertad de prensa es un derecho recién nacido en nuestro país. En un estado de derecho como el que está instaurado en España desde la Constitución de 1978 la libertad de prensa es un derecho suficientemente garantizado por las leyes sin que sea necesario privilegiarlo en el Derecho Penal de tal forma que se exima de responsabilidad penal a personas que contribuyen a la difusión de un contenido ilícito por el solo hecho de haber realizado la acción a través de un determinado medio. La única razón para la pervivencia del art. 30 es mantener un estado de total impunidad de los medios de comunicación que amparados en la libertad de expresión lesionan otros derechos fundamentales constitucionalmente reconocidos e igualmente merecedores de protección frente a conductas lesivas constitutivas de infracción penal.

La protección de la libertad de expresión no requiere de un precepto como el art. 30, puesto que, en el campo del Derecho Penal, queda suficientemente protegido con las causas de justificación que excluyen la antijuridicidad, en concreto el ejercicio legítimo de un derecho y por las categorías generales de la autoría y la participación, así como la exigencia del elemento subjetivo del injusto, pues como reiteradamente ha exigido el Tribunal Supremo, para proceder contra el sujeto del escalón siguiente del art. 30 es necesario probar la culpabilidad del mismo. Por lo tanto, concurriendo los elementos de la definición de delito referidos a la tipicidad, la antijuridicidad, por no concurrir la causa de justificación de actuar en ejercicio de un derecho y la culpabilidad, en el tema que estamos tratando no hay motivo para introducir a través del art. 30 una

condición objetiva de punibilidad que excluya este elemento y por lo tanto el carácter delictivo de la conducta, salvo la voluntad de privilegiar a determinadas personas.

2. *Parte General*

A la hora de determinar la responsabilidad penal de los proveedores de enlaces habrá que distinguir, siguiendo la exposición realizada por Markus Stephanblome, si esa responsabilidad se les exige:

1.º por los contenidos propios, entendiendo que son aquellos contenidos creados por o para el proveedor de enlaces, o
2.º por los creados por terceros pero mostrados como propios por el proveedor, al tratar los contenidos de la página a la que envía el enlace incluido en la suya o al referirse a ellos de modo que se identifica objetivamente con esos contenidos o bien
3.º por los contenidos ajenos que hacen disponibles o accesibles.

A) Autoría y participación

a) Autoría

De autoría hablaremos cuando se exija la responsabilidad por contenidos propios o de terceros que se han hecho propios.

El primer supuesto no plantea problemas especiales dado que en ese supuesto el proveedor de enlaces no opera como tal, sino como el administrador de una web puesto que no está reenviando al usuario a la página de otro sino mostrándole un contenido que es propio de su página web.

En el segundo supuesto el proveedor de enlaces actúa como tal, dado que reenvía al usuario a los contenidos de la página web de un tercero, si bien se los presenta como propios. En este caso, el proveedor de enlaces nunca reconocerá como propio el contenido puesto que le puede acarrear consecuencias penales. Por lo tanto, se plantea el problema de determinar cuando el proveedor de enlaces ha hecho suyo el contenido de un tercero. Las reglas que ha establecido la Jurisprudencia de los Tribunales Federales alemanes son:

1.ª Los enlaces han de considerarse citas que el propietario de una página web hace de otras en la suya. Por lo tanto no hay deber de controlar el contenido de la página web que se cita y, por lo tanto, no hay responsabilidad por reenviar al usuario a un página web con contenidos ilícitos.

2.ª Sólo en supuestos excepcionales se podrá entender que el proveedor de enlaces ha hecho suyo el contenido de un tercero.
3.ª El proveedor de enlaces habrá hecho suyo el contenido de un tercero cuando el vínculo hacia dicho contenido no se haya establecido únicamente para comodidad del usuario sino que es parte integral del servicio prestado por el proveedor. El caso más emblemático se encuentra en la decisión *Unipool*. En este supuesto el objetivo del sitio de informar acerca del producto y publicitarlo sólo se podía lograr en conexión con el enlace. Se declaró responsable al acusado por vincular su página principal al sitio en inglés de *Unip*ool, que contenía publicidad engañosa de un producto vendido por el acusado. Sin embargo, en este caso los contenidos del enlace se habían convertido en los contenidos propios del acusado. Uno de los hechos que el tribunal examinó fue que el sitio del enlace complementaba la oferta del acusado. Además, el tribunal del caso *Unipool* observó que el sitio al que remitía el enlace aparecía con el mismo nombre de dominio que la página que contenía dicho enlace.

De estas reglas establecidas por la Jurisprudencia alemana, entendemos que la primera de ellas no se puede compartir en el derecho español, tanto desde el punto de vista de la legislación sectorial (LSSICE) como desde el punto de vista del derecho penal. Desde el primer punto de vista porque el proveedor de enlaces está sujeto a responsabilidad disciplinaria conforme al art. 17 de la LSSICE, como ya vimos anteriormente y desde el penal porque podrá predicarse la responsabilidad penal en concepto de autor en aquellos supuestos en los que por la redacción del tipo, la conducta realizada por el proveedor de enlaces, es decir, establecer en su página web un vínculo hacia otra página, pueda considerarse incluida en al ámbito del precepto al que nos refiramos.

Finalmente, el autor anteriormente citado entiende que de la Jurisprudencia alemana puede extraerse como conclusión que, para afirmar que el proveedor de enlaces ha hecho suyo el contenido de un tercero, será necesario analizar el enlace en su contexto y esto supone:

1.º Analizar el contenido de la página que ofrece el enlace, las declaraciones adjuntas, el texto o foto que constituyen el enlace y el enlace buscado.
2.º Analizar si se trata de un enlace que remite a la página principal del sitio web o bien el enlace remite directamente a la página secundaria dentro del sitio web, siendo ésta página la que muestra el contenido ilícito.

3.º Analizar la función del enlace dentro de la estructura del sitio web, es decir, si el enlace dirige al usuario fuera del sitio o forma parte integral del mismo sitio. Por eso se considera que el proveedor de enlaces hace suyos los contenidos de un tercero cuando:

—los dos operadores tienen el mismo dominio, puesto que en este caso deberá entenderse que están asociados;
—se trate de enlaces *in line,* es decir, aquellos que, incluyendo un comando en el código fuente del sitio, ordena al navegador descargar automáticamente un sitio web de terceros e integrarlo en el sitio que se está consultando;
—se trate de enlaces que ocultan el hecho de que no son propios los contenidos que muestra sino que proviene de terceros.

4.º Analizar la filiación comercial. A pesar de aplicarse equivocadamente en el caso «Compuserve», donde se declaró responsable a un subsidiario por los actos de la empresa matriz, los tribunales tienen la tendencia a declarar culpable a una empresa que enlaza con contenidos ilegales de una empresa afiliada.

Como dijimos anteriormente, podrá predicarse la responsabilidad penal del proveedor de enlaces en concepto de autor en aquellos supuestos en los que por la redacción del tipo, la conducta realizada por éste, es decir, establecer en su página web un vínculo hacia otra página, pueda considerarse incluida en al ámbito del precepto al que nos referiramos. Así sucederá en los tipos penales previstos en los arts. 189.1.b), relativo a la corrupción de menores y 270, relativo a los delitos contra la propiedad intelectual, del Código Penal, entre otros.

Ahora bien, para que puede predicarse del proveedor de enlaces la cualidad de autor, será necesario que concurran todos los elementos exigidos por la Jurisprudencia del Tribunal Supremo: Primero, haya realizado algunos o todos los elementos del tipo objetivo; segundo, actúe con ánimo de autor; y tercero, tenga el dominio del hecho, es decir, el control del *iter criminis* pudiendo poner fin al mismo en cualquier momento. Junto a estos elementos, por supuesto, deberá poder imputarse al proveedor la conducta a título de dolo, directo o eventual.

Para analizar la concurrencia de los elementos anteriormente señalados, en concreto del dolo y del dominio del hecho, en la conducta realizada por el proveedor de enlaces será necesario tener en cuenta lo que dijimos al inicio sobre el funcionamiento técnico de los proveedores de enlaces y su clasificación, pues la forma de funcionar será determinante para poder afirmar que el proveedor conocía el contenido ilícito

que alberga la página web a la que ha remitido al usuario y que pudo por sus propios medios suprimir el vínculo hacia dicho lugar. Por ello, entendemos que, dentro del grupo de proveedores que incluyen en sus contenidos instrumentos de búsqueda, no cabe imputar a los motores de búsqueda y a los multibuscadores, estos últimos en la medida en que muestren al usuario páginas localizadas por un robot y no por una persona, de manera que la localización de la página con contenido ilícito depende más de la destreza del autor de la página web mostrada a la hora de diseñar la misma que de la programación del robot realizada por el proveedor de enlaces. Por lo tanto, dado que la búsqueda de la página web que alberga el contenido ilícito se produce de forma automática, el proveedor de enlaces no tiene conocimiento de dicho contenido ni tiene el dominio del hecho, puesto que el orden en el que aparecerá la página con contenidos ilícitos depende de factores que el proveedor no controla, factores como el que el robot decida calificar a la página como *spam page* o página tramposa o como la puntuación otorgada a la página por el número de visitas que recibe, influyendo todos estos factores en el orden en el que las páginas aparecerán mostradas al usuario.

Respecto de los proveedores que incluyen en sus contenidos directorios sí será posible imputar a los *links* y a los *banners* que dependan del administrador de la web y no de una empresa de gestión, pues en este último supuesto el administrador de la web no tiene el dominio del hecho dado que no es él quien determina la página de la que se hace publicidad a través de la suya. Tratándose de una empresa de gestión, la exigencia de la responsabilidad penal se deberá diferir a dicha empresa.

En cuanto a la responsabilidad penal de los *links* y *banners*, independientemente de quien los gestione, no será exigible en el supuesto en el que el contenido ilícito se halle oculto en la página web del lugar al que se envía al usuario y ello por afectar al dolo del sujeto que no abarca el contenido ilícito.

En los demás casos estaremos hablando de partícipes.

b) Participación

Atendiendo a la teoría de los bienes escasos, el proveedor de enlaces incurrirá en las figuras de cooperación necesaria y complicidad. Se trataría, por ejemplo en los delitos de estafa informáticos cuando el proveedor de enlaces establece un vínculo hacia una página en la que se ofertan productos que posteriormente no son enviados al solicitante.

Evidentemente, la prueba deberá ir encaminada a acreditar que concurren los requisitos que con carácter general son exigibles en la participación como son el objetivo, realización de actos que contribuyen a que

el autor alcance el resultado típico propuesto y el subjetivo, la *conscientia scaelaris*. Entendemos que en Internet los supuestos más probables serán los de participación adhesiva, es decir, aquellos en los que no hay previo acuerdo, si bien será necesario acreditar que conocía la finalidad ilícita de la página a la que envía al usuario, así como acreditar el dolo sobrevenido.

B) Omisión impropia

La cuestión de si cabe imputar al proveedor de enlaces el contenido ilícito que se encuentra en la página a la que reenvía al usuario por comisión por omisión no presenta peculiaridades respecto del proveedor de servicios.

Esto supone que es aplicable al proveedor de enlaces el razonamiento que se ha seguido respecto del proveedor de servicio, esto es, no es factible la imputación por comisión por omisión. Esta posición es unánime hasta el momento entre los autores que han tratado la responsabilidad penal de los proveedores y se fundamenta en que no cabe afirmar que el proveedor de enlaces haya asumido frente al usuario la posición de garante, de tal forma que el usuario, confiando en la tutela del proveedor, asuma un riesgo que de otra forma no asumiría.

Ahora bien, cabe plantearse si el proveedor de enlaces puede constituirse en garante por voluntad propia y si ello tiene consecuencias en el orden penal.

Respecto de la primera posibilidad, al analizar los proveedores que incluyen en sus contenidos directorios y en concreto, los *banners* o pancartas, vimos que los mismos, en ocasiones, son gestionados por empresas que a veces supervisan previamente el contenido de las páginas a las que van a dar publicidad, reservándose la facultad de validarlas, así como de modificarlas, editarlas o rechazarlas sin previo aviso. Entendemos que a través de estas cláusulas la empresa asume una posición de garante de la licitud de los contenidos a los que da publicidad. Ahora bien, para poder imputar a la empresa de gestión la autoría de un contenido ilícito en comisión por omisión habrá que determinar en cuál de las fuentes de posición de garante subsumimos las facultades mencionadas. Esta cuestión nos lleva a otra, discutida por la doctrina, relativa a si posible la asunción voluntaria y unilateral de la posición de garante. La respuesta ha de ser afirmativa si esa asunción tiene origen contractual y en el supuesto que estamos tratando entendemos que así sucede pues las facultades que las empresas de gestión se reservan sobre las páginas web que publicitan se hallan contenidas en las condiciones que exigen para prestar el servicio y bajo denominaciones como contrato de pres-

tación de servicios publicitarios. Por lo tanto, nos encontramos ante un contrato adhesivo, constituido por cláusulas que son condiciones generales y que son fuente de la posición de garante.

III. **Conclusión**

De lo expuesto, se deduce que, si bien el empleo de la informática es una novedad cuyas amplísimas posibilidades todavía están por descubrir, la responsabilidad exigible a los proveedores de enlaces por los delitos cometidos por el empleo de tal herramienta no precisa de reforma legal alguna, dado que los comportamientos han de ubicarse en figuras ya recogidas en la Parte Especial del Código Penal y siempre con la aplicación de la Parte General en lo referente a la participación, autoría y elementos subjetivos del injusto, siendo así que el Código Penal actual se presenta como válido para hacer frente a este nuevo tipo de criminalidad.

Bibliografía consultada

GÓMEZ TOMILLO, M.: *Responsabilidad penal y civil por delitos cometidos a través de Internet*, Ed. Thomson-Aranzadi, Pamplona, 2004.

MORALES GARCÍA, O.: «Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información», *Revista de Derecho y Proceso Penal*, Junio 2001.

STEPHANBLOME, M.: «Responsabilidad legal de los proveedores de Internet por infracciones de los derechos de autor bajo la legislación alemana y europea». *Boletín de derecho de autor*, (Ed. Unesco) Vol. XXXV Abril-Junio 2001.

La cuestión informática en el ámbito procesal (y también penal). Aproximaciones a partir del caso Bitel

Ladislao Roig Bustos
Fiscal del Tribunal Superior de Justicia de las Islas Baleares

I. **Introducción**

Se dice casi como axioma jurídico que el Derecho siempre llega tarde (y el Derecho Penal tarde y mal). Pero lo que puede aparentar ser una crítica no es sino un necesaria realidad social.

Si entendemos el Derecho como un conjunto de normas que la propia sociedad se da a sí misma para, a través de sus representantes en el legislativo, regularse en sus conflictos, lógico es que la sociedad vaya por delante del Derecho, pues el buen legislador lo que debe hacer es, por un lado, detectar los conflictos sociales y, por otro, determinar cuáles son los intereses que en esos conflictos deben salvarguardarse de manera preferencial, en el bien entendido que una sociedad es un cuerpo que indefectiblemente está en permanente evolución y que, por tanto, de manera constante, elimina algunos conflictos hasta hacerlos desaparecer al tiempo que crea nuevos conflictos. Unas veces es el propio comportamiento de los humanos quienes van variando los supuestos sobre los que la ley debe incidir y otras veces es la ciencia (esa que, decían nuestros padres, «adelanta que es una barbaridad») quien genera los nuevos presupuestos a regular. Así, por poner tan sólo dos ejemplos desde una fecha estándar, el nacimiento de la Constitución en 1978, hemos pasado de despenalizar el adulterio a reconocer el matrimonio entre homosexuales o de regular los derechos de los hijos naturales e ilegítimos a tener que legislar sobre los niños probeta y la clonación animal. Así han variado las relaciones sociales y así ha progresado la ciencia.

No hay legisladores que puedan prever los conflictos de futuro y regularlos antes de que se produzcan. Porque incluso en aquellas sociedades cuyos componentes no son ciudadanos, sino súbditos y donde las normas no nacen del sentir de la sociedad sino del Poder Dictatorial,

protegiendo intereses no generales sino de la élite imperante, incluso en estos supuestos, el pseudo-legislador de esos llamados estados nunca podrá tener la imaginación suficiente para poder legislar anticipadamente y siempre, siempre, la sociedad le sorprenderá.

Por eso no debe alarmarnos el anterior axioma: El Derecho siempre llega tarde. Lo que debe importarnos es que el Derecho llegue y que esa llegada no sea demasiado tardía. Exactamente lo que sucede con el delito informático.

Afirmar que en el campo informático no hemos hecho sino empezar no es sino una afirmación de Perogrullo. Por eso, por muchos que sean los conocimientos y por desbordante que sea la imaginación del legislador, de cualquier legislador, es imposible prever cual va a ser o cual deba ser la regulación legislativa que vaya a regir nuestras vidas en relación con esta materia dentro de 10 ó 15 años. Los nuevos descubrimientos que sin duda se producirán en el ámbito informático y la aplicación que de los mismos se haga lo predeterminarán, aunque en su regulación nunca debiera olvidarse el sentir social. Por poner un ejemplo: Es más que probable que los avances informáticos permitirán que nuestras sociedades tengan en el futuro cada vez más medios y sistemas que nos proporcionen una mayor seguridad, aunque también es más que probable que el precio a pagar por esa mayor seguridad suponga limitaciones en nuestra intimidad y en nuestras libertades individuales. Lo que no debe es olvidarse que es a la sociedad, no al legislador, a quien le corresponde fijar ese precio. A la ciencia le compete el descubrimiento de esos nuevos métodos que permitan acrecentar la seguridad, pero es a la sociedad a quien compete fijar ese precio del que antes hablábamos, es decir, fijar donde está el límite infranqueable de nuestra intimidad y de nuestra libertad individual y hasta dónde la búsqueda de la seguridad puede invadir tales derechos personalísimos. Para el legislador queda la nada sencilla tarea de aprehender ese sentir social y volcarlo en el campo normativo en conformidad con lo que la mayoría de la sociedad desea.

Es claro pues que el Derecho debe ir siempre por detrás de la sociedad, porque sólo así el legislador podrá saber qué es lo que piensa y lo que quiere la sociedad a la que está obligado a servir

¿Y cómo afrontamos Jueces y Fiscales este nuevo campo del saber que es la informática? Puede y debe hacerse desde una doble perspectiva cuales son como litigios que se nos presentan para su resolución y como instrumento propio de trabajo

Probablemente la primera de esas dos perspectivas es, o debiera ser, la menos preocupante. En efecto, para resolver un litigio basado en un tema informático, desde una cuestión civil hasta un delito informático,

no es estrictamente necesario que el juzgador sea un experto conocedor de la informática, de la misma manera que para juzgar un delito de imprudencia médica no es preciso que el Juez tenga conocimientos de cirugía o para resolver una reclamación de daños y perjuicios por defectos en la construcción de una vivienda no se necesita que sea un conocedor de cálculos matemáticos arquitectónicos. Lo que sí se precisa es que la Administración de Justicia cuente con peritos independientes que elaboren informes objetivos en los que el juzgador, tras el racional estudio de los mismos, pueda conectarlos con la legislación vigente para finalmente basar en esa conexión su resolución final. No se trata tanto de hacer una especie de cuerpo de Jueces especializados en informática (que con casi total seguridad nunca llegarán a ser tan expertos como los propios informáticos) como de dotar a la Administración de Justicia de un cuerpo de peritos cuya independencia y objetividad esté asegurada.

Distinta es la perspectiva de la informática como instrumento propio de trabajo. Es evidente que al día de hoy se ha avanzado enormemente en la utilización informática en los puestos de trabajo de la Administración de Justicia, desde la petición de antecedentes penales hasta lo que constituye el mero registro de las Diligencias, con la mayor facilidad que ello supone a la hora de la búsqueda de datos que veces se necesitan de manera urgente. Y se hace esta afirmación pese a que quien esto suscribe pertenece a una Fiscalía, la de Palma de Mallorca, cuyos componentes han dispuesto de un ordenador propio sólo desde noviembre del 2006, es decir, desde hace apenas cinco meses, pues hasta entonces, por problemas de espacio físico, la treintena de Fiscales de Palma contábamos con tres ordenadores y dos impresoras a compartir. Ello no obstante, anécdotas personales aparte, la informatización de la Justicia es un hecho que se viene haciendo felizmente realidad y los ordenadores empiezan ya a funcionar como tales pese a la resistencia de quienes se empeñaban en utilizarlos como meras máquinas de escribir, eso sí, perfeccionadas, o de quienes se negaban a utilizarlos con la excusa de que el uso de la informática no estaba entre los temas de la oposición aprobada. Aunque, también es de recibo decir la parte negativa, la informática ha traído consigo la aparición de «formatos» y «modelos» que de alguna manera han hecho que los razonamientos propios de los antiguos «considerandos» hayan sido sustituidos por la más cómoda operación de «cortar y pegar». Buena es la utilización de la informática como instrumento de trabajo, pero malo es que se sustituya la muy noble función de pensar y razonar por la más cómoda de limitarse a buscar una sentencia hecha por otros y que sea más o menos aplicable al caso concreto a resolver.

En este sentido, se afirma que en un futuro ya no muy lejano desaparecerán los procedimientos entendidos éstos como un conjunto de folios grapados entre sí (a veces incluso por su orden) e incluso, si ha habido suerte, hasta foliados, componiendo en no pocas ocasiones aparatosos volúmenes divididos en tomos numerados que Magistrados, Fiscales, Abogados y Procuradores acarrean consigo hasta su domicilio particular o profesional. Bastará con *disquettes* e incluso ni eso, bastará con remitir todo el procedimiento a través del correo electrónico. La firma electrónica ya utilizada en algunos Juzgados no es sino un avance de ello. Pero éste es un punto en el que necesariamente debemos detenernos para comentar un proceso que tuvo lugar en Palma en los finales de los años 90 y que, además de su especial relevancia política, social y jurídica, tiene una incidencia especial en esta concreta materia de la informatización del proceso judicial. Se trata del llamado caso «Bitel»

II. **El caso «Bitel»**

En marzo de 1998 el Gobierno de la Comunidad Autónoma de Baleares era del Partido Popular mientras que el Gobierno del Consell Insular de Mallorca pertenecía, por pactos postelectorales, a Unión Mallorquina y al Partido Socialista Obrero Español, habiéndose adjudicado la gobernación del área de urbanismo a un miembro del PSOE.

Por razones de operatividad, en marzo de 1998 la Presidencia de la Comunidad Autónoma solicitó a la empresa «Bitel» que el correo electrónico recibido en la cuenta «gabinet del president@bitel.es» fuese reenviado a la cuenta «svallori@gabpresi.caib.es», cuenta gestionada por S.V., auxiliar administrativo, quien daba cuenta diaria del correo electrónico recibido a F.C., secretaria particular del Presidente de la Comunidad.

Por un supuesto error de la empresa «Bitel», el correo que empezó a redireccionarse a la cuenta de S.V. no fue el de la dirección reseñada (del PP), sino el correo electrónico de «president@urbanisme.cim.net», cuyo titular era el Presidente de la Comisión de Urbanismo del Consell Insular de Mallorca (del PSOE). De esta forma, entre marzo de 1998 y marzo de 2000 al menos 34 correos electrónicos dirigidos al Presidente de la Comisión de Urbanismo fueron redireccionados a la cuenta de S.V., quien, a su vez, los entregaba a la secretaria particular del Presidente de la Comunidad. Entre dichos documentos uno de ellos era el que llevaba como título «Criteris per al Pla territorial de Mallorca.-Bases de l'enquadrament», de innegable incidencia social y política, documento

que llegó a manos del Presidente de la Comunidad y que éste utilizó, e incluso exhibió, en el debate político que sobre el estado de la Comunidad se celebró en el Parlament Balear durante los días 13 a 15 de octubre de 1998.

Tras las elecciones autonómicas en 1999 se produjo un cambio de gobierno en la Comunidad Balear y el llamado «Pacto de Progrés» (una unión de todos los partidos políticos salvo el PP) asumió el Gobierno balear. Y fue al producirse el trasvase de poderes cuando el nuevo equipo de Gobierno detectó el error en el redireccionamiento antes descrito decidiendo realizar una doble actuación: Por un lado, el Conseller de Interior y el Secretario General Técnico de Presidencia acudieron a Fiscalía a denunciar estos hechos como presuntamente constitutivos de delito, remitiéndoles el Fiscal al Juzgado de Guardia, donde acudieron esa misma mañana, al entender el Fiscal que posiblemente fueran necesarias actuaciones urgentes que sólo podría adoptar la Autoridad judicial, como la incautación de ordenadores y demás material informático (A destacar en ese punto que el Fiscal entendió que la incautación de ordenadores podría llevar consigo la recogida de datos sensibles que podía haber en la memoria y archivos de esos ordenadores, entendimiento que, como luego veremos al analizar las sentencias, fue de todo punto erróneo, error que puedo particularmente resaltar ya que el Fiscal que adoptó tal decisión fue el mismo que quien suscribe estas líneas). Por otro lado, y de manera simultánea a la presentación de la denuncia, el President del Govern convocaba una rueda de prensa en la que publicitaba los hechos y comunicaba la presentación de denuncia penal

Es evidente que no es momento ni lugar para detallar los avatares de la instrucción sumarial, pero sí deben destacarse dos puntos de ella:

El primero la posición del Fiscal, avalada por unanimidad por la Junta de Fiscales de Baleares,quien interesó la declaración como imputado del entonces President de la Comunidad, D. Jaume Matas, para que explicara como llegó hasta su poder el documento que exhibió en el debate sobre el estado de la Comunidad, si bien al ser en ese momento de la instrucción Ministro del Gobierno Central, en concreto de Medio Ambiente, tal declaración llevaba aparejada la inhibición a favor del Tribunal Supremo por su aforamiento. Tal petición no llegó a formularse formalmente al ser vetada por la Fiscalía General del Estado, si bien si fue formulada, a instancia de la acusación particular y asumida por las Sección 2.ª de la Audiencia, que remitió la causa al Tribunal Supremo de donde fue devuelta por entender que no había indicios de entidad suficiente para tal declaración del Sr. Matas como imputado

El segundo punto es que el Instructor decidió el archivo de las Diligencias por entender que los hechos no eran constitutivos de delito. Tal

decisión de archivo fue recurrida por la acusación particular. El Fiscal, por su parte, partidario igualmente de recurrir el auto de archivo, recibió orden del Fiscal General del Estado de interesar la confirmación del archivo. Ello no obstante, en la vista oral de sustanciación del recurso, el Fiscal pidió formalmente la confirmación del auto de archivo pero, amparándose en el art. 25 del Estatuto Orgánico del Ministerio Fiscal, de viva voz explicó los motivos por los que personalmente entendía que debía revocarse el auto de archivo y abrir el acto del Juicio Oral

La Sección 2.ª de la Audiencia acordó finalmente la apertura del Juicio Oral contra S.V., el auxiliar administrativo que gestionaba la cuenta del correo electrónico, y contra F.C., quien fuera secretaria particular del President del Govern, Vista Oral que finamente se celebró en la Sección 2.ª de la Audiencia si bien conformada por los magistrados de la Sección 1.ª al haber sido recusados sus componentes originales por su actuación en la decisión de revocación del auto de archivo.

La Sentencia de la Sección 2.ª de la Audiencia Provincial de Mallorca de 19 de mayo de 2005 absolvió en base a los siguientes argumentos: «Solo la Administración Insular, y no el ciudadano particular, era el destinatario de tales escritos» sin que «… ninguno de los mensajes fueran atinentes a su vida privada» ya que eran «… documentos cuyo destinatario era el Área de Urbanismo de dicha Administración Pública» de manera que «jamás pertenecieron ni pudieron pertenecer, por su propia naturaleza y contenido, al acervo de la privacidad o intimidad del denunciante. A mayor abundancia, dichos mensajes no eran ni podían ser secretos, pues tras ser recibidos por la Administración Pública destinataria de los mismos e integrados en su correspondiente procedimiento administrativo, los interesados en su contenido tienen derecho a obtener copia de los mismos en los términos establecidos por los artículo 105.b de la Constitución y 35.c de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común».

Continúa la sentencia señalando que «sucede que así como los particulares y las empresas privadas pueden ser titulares del derecho a la intimidad, este bien jurídico es esencialmente incompatible con las normas que regulan la actividad de la Administración Pública, que se rige irrenunciablemente por los principios de publicidad y transparencia, por lo que el Consell Insular de Mallorca no puede ser sujeto pasivo del tipo penal descrito en el artículo 197.1 del Código penal».

Por todo ello «… pese a que los acusados no solo se habían apoderado indebidamente de dicho documento ("Criteris per al Pla teritoral d Mallorca.-Bases de l'enquadrament") recibido en la cuenta del Consell Insular de Mallorca a través del redireccionamiento en cuestión, sino que

además lo cedieron al Presidente de la Comunidad Autónoma quien lo utilizó en la sesión del Parlamento Autonómico celebrado los días 13,14 y 15 de octubre de 1998…» y dado que «… lo redireccionado y difundido no atañe a los secretos ni a las intimidades del denunciante…» procede absolver libremente a los acusados.

A su vez, la sentencia de la Sala 2.ª del Tribunal Supremo de 19 de junio de 2006, de la que fue ponente D. Perfecto Andrés Ibáñez, confirmó la anterior reseñando, básicamente:

> «(…) Es claro que los acusados se injirieron en la cuenta de correo abierta al querellante en la Comisión insular de urbanismo en su calidad de presidente del órgano… y ello hizo posible que de los mensajes dirigidos a ella (a su cuenta de correo electrónico) se remitiese un duplicado a la cuenta existente en el Gabinete de la Presidencia de la Comunidad Autónoma de las Islas Baleares a nombre de S.V.D., auxiliar administrativo, que la gestionaba, y daba traslado diariamente de su contenido a F.C.P., a la sazón secretaria particular del President de la Comunidad… dándose la particularidad de que una de las comunicaciones ("Criteris per al Pla territorial de Mallorca. Bases de l'enquadrament") habaría sido usada en un debate sobre el estado de la Comunidad Autónoma».

Para la consideración de si los hechos son o no delictivos, es necesario delimitar el campo semántico de los términos «secreto» e «intimidad» apareciendo el primero de ellos (el secreto) concebido «con un sentido formal» ya que «se asimila textualmente el descubrimiento de los secretos a la vulneración de la intimidad» de manera que «la idea de secreto en el artículo 197-1.º del C. Penal resulta conceptualmente indisociable al de intimidad: ese ámbito propio y reservado frente a la acción y el conocimiento de los demás, ámbito que por su naturaleza personalísima, normalmente, no debe verse implicado en el desempeño habitual de las actividades político-administrativas… por lo que hay que decir que comunicaciones del género de las interferidas no están destinadas institucionalmente a ser el regular cauce de contenidos de carácter íntimo, y lo cierto es que no suelen serlo en la práctica y tampoco lo fueron en este caso».

Por todo lo cual se concluye que «no cabe afirmar que los acusados, al operar del modo acreditado, hubieran pretendido vulnerar la intimidad del titular,…» si bien «dicho esto hay que afirmar también que la cuestión enjuiciada no pude considerarse ética ni jurídicamente indiferente, y que las comunicaciones del querellante fueron interferidas de manera ciertamente ilegítima aunque, según se ha hecho ver, no calificables como delito».

III. **Comentario**

Una primera aproximación a las sentencias reseñadas debe hacer especial referencia a la recogida de pruebas o, mejor dicho, al intento de recogida de pruebas. Porque, en efecto, tanto durante la instrucción del proceso como en el acto del Juicio Oral, nunca llegaron a ser materialmente leídos los contenidos de los correos redireccionados. Solo se consiguió obtener una lista del origen o de nueva remisión de esos correos, además del documento exhibido por el President durante el debate sobre el estado de la Autonomía, documento ya reseñado en las anteriores sentencias. El ordenador donde se descubrió el error de redireccionamiento cometido por la empresa Bitel había sido previamente manipulado y borrado buena parte de su contenido cuando el Juzgado lo intervino. Es evidente, además, que el dato de que los hechos fueran denunciados simultáneamente al Juzgado de guardia y la opinión pública mediante rueda de prensa no facilitó en absoluto la posible recogida de pruebas materiales. Probablemente sea por lo que ambas sentencias hacen siempre referencia a que en el contenido de los correos no se incluye ningún mensaje «atinente a la vida privada del denunciante» ni se trata en ellos de «contenidos de carácter íntimo».

Un segundo problema habido en este proceso judicial derivó de que en él sólo hubo peritos de parte alguno de los cuales parece que más entorpeció la instrucción que ayudó a mejorarla. Por ello conviene reafirmar lo antedicho de la importancia, mejor, de la necesidad de que los órganos judiciales puedan contar en este tipo de procesos con peritos objetivos que ayuden a desentrañar aquellos puntos a los que Jueces y Fiscales, por más conocimientos técnicos que puedan tener en materia informática difícilmente podrán llegar a aprehender.

Pero lo más importante de estas sentencias es, a mi juicio, la afirmación taxativa que ambas contienen de que la Administración no tiene intimidad, ya que ésta es «un bien jurídico esencialmente incompatible con las normas que regulan la actividad de la Administración Pública» (sentencia de la Audiencia de Palma) y a que al «asimilarse el descubrimiento de los secretos a la vulneración de la intimidad… porque la idea de secreto del artículo 197,1.º CP resulta conceptualmente indisociable de la de intimidad» (sentencia del Tribunal Supremo), se llega a la conclusión de que cualquier ciudadano puede introducirse en los ordenadores de cualquier órgano de la Administración, entendida ésta en el mayor sentido global que se quiera, sin que tal actividad sea calificable como delito porque, en definitiva, la Administración no tiene intimidad, es decir, no tiene secretos.

Uno de los temas de esta Mesa es, precisamente, la informatización del procedimiento penal. Pues bien, con la tesis jurisprudencial del lla-

mado caso Bitel, todos los avances informáticos que se han producido en los últimos años, tanto desde la perspectiva material como desde la procesal, pueden quedar en entredicho porque cualquier *hacker* podrá entrar en los ordenadores de un Juzgado o de una Fiscalía y acceder a todos los datos que en se contengan en sus archivos con la tranquilidad que supone el saber que está realizando una actividad «ilegítima aunque no calificable como delito» (sentencia del Tribunal Supremo). Y tal afirmación no es un aviso para el futuro, sino una advertencia actual

Podrá aducirse que el proceso penal tiene una garantía añadida cual es el secreto del sumario. Cierto, al menos teóricamente. Pero tal cautela no sólo no es válida para el resto de los procesos judiciales como los civiles, los contenciosos, los mercantiles…, sino que tampoco es válida para todas aquellas actuaciones penales realizadas al margen de la investigación sumarial. Por ejemplo: El Fiscal Anticorrupción de Canarias remite por correo electrónico al Fiscal Jefe Anticorrupción, con sede en Madrid, un resumen de las actuaciones practicadas a través de unas Diligencias de Investigación sobre blanqueo de dinero. O, por ejemplo, el Fiscal Jefe de Baleares remite consulta, también por correo electrónico, al Fiscal General del Estado sobre la posible interposición de recurso de casación respecto de un tema que, por razones de la materia o de la personalidad de los acusados, es especialmente sensible. Quien intercepte tales correos, cualquiera que sea la finalidad de la intercepción, estará actuando con total impunidad porque la Administración no tiene ni intimidad ni secretos

Los ejemplos aducidos pueden multiplicarse cuantas veces se desee y extenderse, por supuesto, al resto de las Administraciones. Y no parece que la futura reforma del Código Penal vaya a solucionar este problema porque aunque el proyecto de reforma que ya ha entrado en el Congreso incide expresamente en este tema, lo hace de modo y manera que, como veremos, va a suponer dejar la situación descrita en el mismo estado. Dice la Exposición de Motivos:

> «La tutela penal de la intimidad y de los secretos ha sido tradicionalmente fragmentaria y condicionada a la realización de conductas de apoderamiento de papeles, cartas o mensajes, o de instalación de aparatos de captación de imagen o sonido, pero a la vez que la importancia fundamental de ese bien jurídico exige cada vez más atención y medidas legales, como son esencialmente las recogidas en la legislación sobre protección de datos, crecen los riesgos que lo rodean, a causa de las intricadas vías tecnológicas que permiten violar la privacidad o reserva de datos contenidos en sistemas informáticos. Esta preocupante laguna, que pueden aprovechar los llamados hackers, ha aconsejado incorporar al artículo 197 un nuevo apartado que castiga a quien por

> cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático».

Consecuentemente con lo anterior, el proyecto incorpora un nuevo apartado al artículo 197, al que le asigna el número 3:

> «El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo será castigado con pena de prisión de seis meses a dos años».

Sin embargo, como ya dijimos, esta reforma no solucionará el problema toda vez que el Legislador se centra en el cómo, pero no en el quien. En efecto, la reforma se sigue operando centrada en el art. 197, es decir, dentro del Título X (Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio), Capítulo I (Del descubrimiento y revelación de secretos) del Libro II del Código Penal. Consecuentemente, de concluirse la reforma en el sentido proyectado, la situación de protección de datos de la Administración no se alterará un ápice

IV. **Epílogo**

Dijimos al inicio de esta exposición que el Derecho siempre llega tarde y mantuvimos, y mantenemos, que tal afirmación no debe ser preocupante. Pero lo que sí es preocupante es que el Derecho, o su aplicación, pueda llegar a ser un sinsentido. Y esto es, en nuestra modesta opinión, lo que ha pasado con el caso Bitel al haberse centrado la sentencia absolutoria en que ninguno de los mensajes interceptados, o redireccionados, eran atinentes a la vida privada.

Es decir, y como conclusión, que si el Presidente de la Comisión de Urbanismo del Consell Insular de Mallorca, en vez de remitir a otro organismo oficial los «Criteris per al Pla territorial de Mallorca.-Bases de l'enquedrament» hubiera hecho un uso indebido del correo electrónico oficial y hubiera remitido un correo electrónico a su esposa diciendo «Margalida, ve poniendo la sopa a calentar que ya salgo», entonces sí habría habido delito. Y esta conclusión es la que, modestamente, sí nos parece un sinsentido.

La cuestión informática en el ámbito procesal. Algunos aspectos

Luis Carreras del Rincón
Abogado

I. **Piratería del *software* en España: Planteamiento de la cuestión**

Según los estudios más recientes del sector, referidos al año 2005, la Unión Europea padece una tasa media de piratería de *software* del 35%. Dentro de la Unión el índice más alto es el de Grecia, con un 64%,y el más bajo el de Austria y Finlandia, con un 26%, mientras que en España el índice de piratería se sitúa en el 46%.

Estos datos, por lo que a España se refiere, confirman una tendencia lamentablemente estable a lo largo de los últimos años.

Tales cifras se explican por varios motivos:

1.º Por un lado es evidente la baja percepción social que todavía existe sobre la ilegalidad que representa la distribución y también el uso de programas informáticos sin licencia del titular de los derechos de propiedad. Aunque las acciones promovidas por los operadores legítimos del sector, tanto a nivel informativo como judicial, han hecho disminuir en los últimos años esta baja percepción, todavía queda desde luego mucho camino por recorrer.

2.º Por otro lado, la rentabilidad que este tipo de actuaciones representa para quienes actúan de forma organizada para enriquecerse colocando en el mercado programas informáticos sin licencia, es altísima. Según cálculos realizados en el sector se ha llegado a afirmar que se trata de un negocio potencialmente más lucrativo incluso que el del tráfico de estupefacientes, si se atiende al beneficio comparado con la inversión.

3.º En tercer lugar, las consecuencias penales que nuestro ordenamiento jurídico prevé para los infractores de la legalidad, son considerados por distintos operadores jurídicos como demasiado suaves. De hecho, un somero análisis de la jurisprudencia

dictada en casos de defraudaciones de los derechos de propiedad intelectual sobre programas informáticos, revela que prácticamente no se dictan sentencias que comporten la efectiva entrada en prisión de los condenados.

4.º En cuarto lugar, el lento desarrollo normativo de la legislación penal protectora de la propiedad intelectual en general, y por ende también del sector informático en particular, ha sido motivo en muchos casos de una aplicación titubeante e incluso a veces contradictoria, dando lugar en tantas ocasiones a sentencias absolutorias dictadas en supuestos de hecho meridianamente infractores de aquellos derechos.

5.º En quinto lugar, la peculiaridad propia de las operaciones delictivas en este sector, exige que la obtención de pruebas incriminatorias pase habitualmente por dos dificultades: por un lado, el sujeto pasivo que se propone denunciar a un supuesto infractor de sus derechos de propiedad intelectual, ha de lograr reunir suficientes indicios sobre la existencia de la actividad ilícita, que normalmente pasan por adquirir al presunto delincuente un ejemplar del programa pirateado; y por otro, a partir de la denuncia las medidas de investigación y comprobación del delito pasan casi sin excepción por la intercepción de comunicaciones y la entrada y registro en empresas y/o domicilios. Y lamentablemente, en la práctica se producen infracciones de garantías constitucionales, con el resultado de que a menudo el supuesto delincuente no pueda ser condenado por causa de las irregularidades formales con que se obtuvieron las pruebas incriminatorias.

6.º Y en sexto y último lugar, la acreditación de los perjuicios económicos derivados de la actuación criminal en este ámbito, —para cuya cuantificación, como es sabido, el Código Penal se remite a las disposiciones de la Ley de Propiedad Intelectual—, es a menudo muy difícil. Por un lado, porque exige la participación de peritos muy especializados y, por otro, porque la actividad instructora no siempre consigue reunir pruebas de cargo suficientes sobre el alcance de la actividad ilícita anterior al inicio del procedimiento, limitándose generalmente a la incautación del material ilícito que se halla en poder del supuesto delincuente. Todo lo cual produce que, en la práctica, aun cuando se consiga una condena firme, tampoco la consecuencia económica de dicha condena parece lograr el deseado efecto disuasorio. Dicho de forma sencilla, sigue siendo un buen negocio.

Vamos a ver ahora algunos de estos aspectos con cierto detenimiento, siempre desde la óptica de la realidad jurídico-penal propia de la mesa redonda de la que forma parte esta intervención.

II. **Piratería, falsificación e importación paralela de programas informáticos y de la documentación acreditativa de su autenticidad**

Aunque en términos generales se suele identificar la actividad ilícita con programas de ordenador como de piratería, en la práctica conviene distinguir distintos supuestos.

Por piratería solemos referirnos generalmente a la reproducción ilegal de discos compactos (o CDs o *cederroms*, según la terminología que se prefiera), que se comercializan por medio de vendedores ambulantes que reciben el calificativo de «*top manta*» con contenidos que pueden ser musicales, de películas o de programas informáticos destinados ya sea al simple ocio (juegos) o a la gestión de información en ordenadores. En estos casos el comprador sabe que lo que adquiere no es original, que en el caso de las películas la calidad del producto es deficiente o incluso muy deficiente, y que el precio que paga por el producto escogido es netamente inferior al del producto original. La tecnología necesaria para esta actividad está al alcance de cualquiera hoy en día y el «producto» puede «bajarse» desde una infinidad de páginas de Internet.

Otra actividad próxima a la piratería es la instalación en un ordenador de un sistema operativo o de otros programas de gestión, careciendo de la oportuna licencia para ello, burlando los sistemas de protección que habitualmente configuran estos programas, ya sea introduciendo un código obtenido ilegalmente o de otra forma igualmente ilegal.

Pero más allá de la piratería está lo que en el sector denominamos como falsificación. Se trata de la reproducción en grandes cantidades de discos compactos conteniendo programas de ordenador, creando una apariencia de originalidad tanto en su aspecto externo como en su funcionamiento, con el fin de colocarlos en el mercado como si de originales se tratara. Este tipo de actividades requieren de una tecnología muy cara y por tanto al alcance solamente de unos pocos, y suelen llegar a nuestro país habitualmente por medio de organizaciones delictivas con ramificaciones en países muy diversos, aunque excepcionalmente se lleven a cabo también en nuestro país. Además suelen ir acompañadas de la falsificación de la documentación que acompaña a esta clase de productos, como manuales de funcionamiento y otro tipo de documentos

que supuestamente acreditan su «originalidad». Contrariamente a lo podría pensarse, por otro lado, la colocación en el mercado de este tipo de programas suele hacerse a un precio también inferior al del producto original, aunque la casuística real en este aspecto es muy variada y no se puede resumir en unas pocas líneas.

En todo caso, es de notar que en la conectividad de algunos de estos programas a través de Internet permite a los titulares de los derechos defraudados detectar la existencia de estas copias ilegales, contándose en ocasiones su número por centenares de miles solamente en España.

Queda por último un tipo de actividad igualmente delictiva pero de índole muy distinta, que es la importación denominada «paralela». Aquí se coloca en el mercado producto ciertamente original, auténtico, pero adquirido en otros mercados, como pueden ser en ciertos países árabes o en determinadas zonas del África subsahariana. El perjudicado en este caso es el distribuidor o distribuidores autorizados de ese producto en nuestro país, aunque en ocasiones también lo pueda ser el titular de los derechos originales y comercializador de origen. De nuevo la casuística es muy variada para resumirla en esta intervención.

Esta distinción tiene evidente interés práctico, por cuanto la correcta identificación del producto intervenido suele condicionar la calificación de la actividad delictiva y de sus consecuencias jurídico-penales. No hay ni que decir que en ocasiones se requiere de un alto grado de especialización técnica para distinguir unos casos de otros, por lo que habitualmente la cooperación del perjudicado por el supuesto delito —y de sus técnicos— puede ser en la práctica presupuesto indispensable.

III. **Intervención de detectives privados en la obtención de elementos de prueba del tráfico ilícito**

Como ya he apuntado en el planteamiento con que he dado comienzo a esta intervención, la necesidad de reunir elementos de prueba respecto de un caso determinado de supuesto tráfico ilícito, que permitan al perjudicado iniciar los trámites de la denuncia y en su caso obtener las medidas policiales y/o judiciales para su comprobación, hace que en muchas ocasiones se opte por acudir a la intervención de un detective privado, al que se le pide que acuda al establecimiento respecto del que han surgido las sospechas y adquiera un ejemplar del producto interesado, que será después analizado por los técnicos para determinar la legalidad o ilegalidad de dichos programas.

En la práctica parece que este sistema de obtención de pruebas es adecuado para lograr el inicio de las actuaciones correspondientes, pues un estudio de la jurisprudencia sobre estos temas así lo pone de manifiesto[1].

Sin embargo, no han dejado de aparecer dudas a la hora de valorar la trascendencia jurídico-penal de tales pruebas, hasta el punto de que en ocasiones se ha llegado a la a la sentencia absolutoria del que fuera supuesto delincuente, llegando incluso a afirmarse en algún caso que la intervención del detective constituyó tanto como una provocación al delito. Así en la Sentencia dictada por el Juzgado de lo Penal n.º 2 de Alicante en 24 de noviembre de 2005 (JUR 2006/42354) se puso en duda si el detective se limitó, por decirlo así, a constatar la existencia de la actividad ilegal, o si bien, influido por la convicción preconcebida de que dicha actividad efectivamente existía, llegó a inducir la venta del producto pirata; y ante la duda la sentencia optó, naturalmente, por la absolución[2].

IV. **Entrada y registro. Incautación de soportes informáticos y ordenadores, volcado de la información y garantías. Asistencia de expertos**

Como ya he comentado al inicio de esta intervención, la naturaleza de las actividades delictivas que examinamos comporta, casi sin excepción, que la comprobación de los hechos incriminatorios se produzca por medio de diligencia de entrada y registro acordada judicialmente.

En la práctica el éxito de este tipo de diligencias exige tener en cuenta las características propias de este ámbito de actividad ilegal; características que en muchas ocasiones se traducen en verdaderas dificultades que deben ser atendidas correctamente. Así, por un lado, cabe señalar que los «instrumentos y efectos» que puedan ser hallados y tener relación con el delito investigado suelen ser muy variados: CDs u otros soportes magnéticos en los que se contengan programas de ordenador que supuestamente se comercializan de forma ilegal, discos duros contenidos en ordenadores que almacenen tales programas, documentación técni-

---

[1] Como ejemplo puede examinarse la sentencia dictada por la Audiencia Provincial de Tarragona el 24 de junio de 2001 (JUR 2001/310368), que confirmó la condena del Juzgado de lo Penal 4 de la misma ciudad.

[2] En idéntico sentido se pronunció el Juzgado de lo Penal de Orihuela en sentencia de 6 de abril de 2006 (JUR 2006/126469), aunque en este caso la absolución se fundamentó además en la falta de acreditación de la actividad ilícita.

ca, manuales de uso, certificados de autenticidad, licencias de uso (que por extralimitación no amparan el copiado o instalación en la forma en que se traduce la actividad ilícita), facturación y documentación contable en general, que puede hallarse a su vez en soporte informático (correos electrónicos, mensajería instantánea) que puede ser además reveladora de la implicación de terceros en al actividad investigada en cualquier de las modalidades de participación penalmente perseguibles.

Esto exige naturalmente que, por un lado, la diligencia de entrada y registro prevea ya *ab initio* el alcance de la misma y la posibilidad de incautación de esta variedad de «instrumentos y efectos», —con la adecuada fundamentación fáctica y jurídica que asegure el respeto de los derechos fundamentales que tal incautación pueda afectar, sobre todo en cuanto a comunicaciones telemáticas se trate—, así como los medios adecuados para ello, que garanticen que no se produzca una alteración cuantitativa y cualitativa de las piezas de convicción a lo largo del proceso.

Por exigencia de lo dispuesto en los artículo 334 y concordantes de la Ley de Enjuiciamiento Criminal, todo cuanto sea objeto de incautación ha de ser cuidadosamente descrito en el acta de la diligencia, y ser ordenado y sellado con la mejor organización posible. En la práctica esto puede ser muy laborioso, según la cantidad y variedad de elementos hallados, sin que en ningún caso esta dificultad pueda justificar un «empaquetado», por decirlo así, general. De hecho la conocida Sentencia del Tribunal Constitucional 170/2003 de 29 de septiembre (RTC 2003/170) hubo de anular una sentencia condenatoria dictada por la Audiencia Provincial de Zaragoza por la forma en que se llevó a cabo el sellado y precintado de las piezas de convicción recogidas en entradas y registros realizadas en distintos lugares (en este caso principalmente CDs de apariencia ilegal), que había llevado luego a confusión sobre su número y procedencia, entendiéndose que se había vulnerado el derecho fundamental del condenado a un proceso público con todas las garantías[3].

La incautación de ordenadores comporta muchas veces la necesidad de proceder sin demora al volcado de la información contenida en sus discos duros a otro soporte, para que puedan ser devueltos a su titular. De otro modo puede producirse un daño irreparable a la empresa objeto de la diligencia, ya que en el mismo ordenador suele coexistir información y programación ajena a las actividades delictivas que son objeto de investigación. Esto naturalmente exige realizar dicho volcado con las garantías suficientes, que garanticen la efectividad de la prueba incrimi-

[3] La Audiencia Provincial hubo de dictar nueva sentencia, absolutaria en este caso, ya que no podía tenerse en consideración la principal prueba incriminatoria.

natoria que pueda hallarse, y por ello deben ser previstos con antelación los medidos adecuados.

En otro orden de cosas, el examen de los posibles «instrumentos y efectos» hallados en la diligencia comportan en la generalidad de los casos una dificultad técnica a veces muy compleja, lo que hace imprescindible contar en su desarrollo con la colaboración de expertos informáticos con experiencia suficiente. Ya hemos hecho referencia más arriba a los diferentes tipos piratería y/o falsificación de programas informáticos. Distinguir sobre el terreno qué programas son aparentemente simples copias piratas no suele presentar dificultad, pero sí en cambio puede ocurrir con las falsificaciones, en proporción directa a su «calidad». Y lo mismo hay que decir respecto de la tenencia para su distribución de programas auténticos, originales, pero no amparados por licencia legítima de su titular. En la práctica no suele haber inconveniente para que el denunciante aporte sus propios técnicos forenses para colaborar en estos trabajos iniciales, sin perjuicio de lo cual hay que decir que la preparación técnica de algunas unidades de las fuerzas y cuerpos de seguridad del Estado es más que notable y cada día más alta.

En otras ocasiones hay que tener en cuenta que los equipos informáticos suelen estar conectados en red, por lo que también es aconsejable tomar las medidas oportunas para que no se pueda eliminar información de algunos discos duros, a través de la manipulación subrepticia desde otro terminal, durante el curso de la misma diligencia de entrada y registro, circunstancia que por otro parte se ha llegado a producir realmente.

Por otro lado, según sean las características del material incautado en la diligencia, en ocasiones surgen dificultades para examinar fuera de la sede judicial determinadas piezas de convicción. En el caso, por ejemplo, de replicado masivo de CDs por medio de tecnología punta, del examen de un solo ejemplar en un laboratorio especializado puede llegar a conocerse datos de suma importancia para la investigación, que quizá no puedan ser obtenidos de otra forma, como pueda ser el número de copias realizadas, el origen del disco llamado «*master*» (para entendernos, el molde utilizado para obtener copiados masivos), etc. El problema hoy por hoy es que este tipo de laboratorios son tan especializados que suelen pertenecer a las grandes compañías titulares de derechos sobre programas informáticos y hallarse incluso allende nuestras fronteras. La dificultad por tanto reside en determinar si nuestro ordenamiento permite entregar en depósito un ejemplar de las piezas incautadas al perito designado por el perjudicado por el supuesto delito, para que pueda examinarla en el laboratorio escogido, cuestión que en la práctica no es pacífica.

V. **Acreditación de los perjuicios causados por la actividad ilícita**

El último aspecto que trataré en esta aportación a la Mesa redonda es el relativo a las dificultades que comporta la acreditación de los perjuicios causados a los titulares de los derechos sobre programas informáticos.

Parece oportuno hacer a este respecto dos observaciones previas. En primer lugar, cuando se formula denuncia contra un supuesto infractor de los derechos de propiedad intelectual sobre programas informáticos, y se produce como hemos visto generalmente la diligencia de entrada y registro para confirmar los indicios sobre los que se basa la denuncia, se obtiene por decirlo así una foto fija de la situación en ese preciso instante; dicho de otro modo, se comprueba si hay o no hay actividad ilícita y se incautan los instrumentos y efectos que en ese momento puedan hallarse. La actividad ilícita queda así en principio eliminada en cuanto al futuro, y esto naturalmente entra dentro de los intereses del perjudicado por la utilización ilegítima de sus derechos. Ahora bien, y aquí viene la segunda observación, generalmente al perjudicado le interesa todavía más acreditar el alcance de la actividad ilícita hasta ese momento, en el pasado inmediatamente anterior, y ello por dos razones: primero porque, como es sabido, según prevé el art. 271 del Código Penal, las circunstancias del delito varían cuando el beneficio obtenido por el supuesto delincuente o el perjuicio causado revisten especial trascendencia económica, con lo que las penas de prisión que podrían imponerse son proporcionalmente mayores[4]; y segundo, porque es del todo punto lógico que el perjudicado busque obtener una compensación adecuada al real perjuicio que ha sufrido.

Dicho esto, no hace faltar recordar que la extensión de la responsabilidad civil derivada de los delitos contra la propiedad intelectual se rige, *ex* art. 272 del Código Penal, por las disposiciones de la Ley de Propiedad Intelectual relativas a la indemnización de daños y perjuicios. Como es sabido, estas normas permiten al perjudicado optar, como indemnización, entre el beneficio que hubiere obtenido presumiblemente, de no mediar la utilización ilícita, o la remuneración que hubiera percibido de haber autorizado la explotación[5]. Esto quiere decir que para la reparación del delito en términos reales se hace imprescindible contar con una

[4] De uno a cuatro años, en lugar de seis meses a dos años.

[5] También es verdad que en ocasiones los tribunales han tenido en cuenta el daño moral sufrido por el perjudicado, como una partida distinta y complementaria de la indemnización estricta, aunque hay que reconocer que esta «duplicación» dista mucho de ser una práctica consolidada.

adecuada instrucción que, desde el primer momento, se dirija también a reunir toda la información que conduzca a acotar con la adecuada precisión la extensión real de la actividad ilícita perseguida.

En la práctica esto no siempre es fácil. En ocasiones querer «llegar hasta el final», como diríamos en términos coloquiales, comporta una complicación añadida a la instrucción, que a veces puede requerir, por ejemplo, el interrogatorio como testigos de gran cantidad de personas, quizá los usuarios finales de los programas ilícitamente colocados en el mercado a lo largo de mucho tiempo, quizá porque en los albaranes y facturas de las operaciones de detalle no se reflejó la realidad y hay que contrastar los hechos con quienes pueden arrojar luz suficiente. Ni que decir tiene que la resistencia del supuesto delincuente a facilitar estos datos es a veces insalvable. Se ha dado el caso, por ejemplo, de que se ha hecho desaparecer la facturación de los períodos «sensibles», aprovechando que en la primera entrada y registro se centraron los esfuerzos únicamente a localizar el producto supuestamente ilegal, y sólo después se trató de reunir la información contable, cuando ya era de alguna manera demasiado tarde. Se comprenderá fácilmente que reunir los datos al margen de la contabilidad real puede ser en ocasiones una tarea ímproba, y en no pocas ocasiones casi imposible, o sin el casi.

En cualquier caso, con dificultades o sin ellas, la cuantificación de los daños y perjuicios acaba siendo materia de la correspondiente prueba pericial, que requiere casi sin excepción el concurso de expertos conocedores de la materia de la que se trata, lo que no siempre es sencillo. A la postre esta tarea, en la práctica y como es lógico, acaba recayendo sobre el titular de los derechos que han sido ilícitamente perjudicados.

Tutela de la privacidad e interceptación pública de las comunicaciones

Antonio Narváez Rodríguez
Fiscalía Ante el Tribunal Constitucional

I. **Introducción**

El peligro que amenaza a las sociedades democráticas del siglo XXI radica, en muchos casos, en la tentación en la que incurren los poderes públicos de conseguir un cada vez más alto grado de intromisión en el conocimiento de los conflictos sociales que afecten a los intereses generales, pero también y en buena medida su tendencia no queda limitada a tales conflictos con trascendencia colectiva, sino que en otros supuestos el grado de injerencia en intereses propiamente privados de la esfera íntima de los ciudadanos puede alcanzar límites intolerables, pues produce en éstos la sensación de que, de una u otra manera, pueden ser controlados en muchas facetas de su vida privada, que transcurre desde aspectos esenciales de sus relaciones con los demás, como por ejemplo, en el modo de expresar sus opiniones, no siempre conformes con las del Poder Público que les gobierna, hasta llegar a intromisiones en el ámbito de su círculo privado que van desde su propio hogar hasta en sus comunicaciones con los demás utilizando toda la amplia gama de medios que hoy proporciona la tecnología moderna.

Tal percepción de la realidad, evidentemente, genera también un factor de preocupación cada vez más creciente por la necesidad de tutela de derechos fundamentales que forman parte de la cultura jurídica de una democracia. En efecto, el Estado, para atender las necesidades de la política social y económica, pero también utilizando como pretexto la seguridad de sus ciudadanos y la eficacia en la investigación de los delitos, ha introducido con demasiada frecuencia un cada vez más intenso intervencionismo en la órbita individual de cada ciudadano, corriéndose así el riesgo que ya ponían de manifiesto determinados estudios que se realizaron en la década de los 80[1] en el seno del Consejo de Europa,

[1] Las Conversaciones sobre Orwel, que se celebraron en la ciudad francesa de Estrasburgo el día 2 de abril de 1984 y la Conferencia sobre Bancos de Datos de Madrid de 13

de que se pudieran establecer en un futuro no muy lejano regímenes y métodos propios de un sistema que, a modo de «Gran Hermano», controlara la vida privada de los ciudadanos de aquella comunidad, tal y como magistralmente lo reflejara Orwel en su conocida obra.

La preocupación de todo Estado de Derecho de velar por la seguridad de sus ciudadanos y garantizar eficazmente la represión y castigo de los delitos en ningún momento puede conducir a la enorme tentación de restringir hasta límites intolerables sus derechos fundamentales, entre ellos y en lo que ahora concierne, el derecho a su vida privada y a su intimidad personal, porque en la dual concepción que de los derechos fundamentales en su conjunto hizo ya tempranamente el Tribunal Constitucional[2] (en adelante, TC), en cuanto que no son sólo derechos subjetivos e individuales de los ciudadanos, que les garantizan un status jurídico o la libertad en un ámbito de la existencia, sino al propio tiempo también, elementos esenciales de un ordenamiento objetivo de la comunidad nacional, por cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada en el actual Estado Social y Democrático de Derecho, exigen de una reacción enérgica de los poderes públicos para velar por que tales principios constitucionales alcancen una efectiva realidad.

En el marco europeo de nuestro entorno, ciertamente, la gran mayoría de sus Ordenamientos Jurídicos, encuadrados en la órbita del Consejo de Europa y suscritores, por ello del Convenio de Roma, han puesto especial cuidado y dedicación en arbitrar normas legales[3], escritas o no escritas, según las particularidades de cada sistema jurídico, que tienden a proteger tales derechos fundamentales y, en lo que se refiere a los particulares derechos que ahora interesan, a restringir cualquier injerencia que desde el punto de vista del art. 8 del Concenio Europeo de Derechos Humanos (en adelante CEDH), 18.3 en nuestro Texto Constitucional, pueda resultar incompatible con las necesidades de una sociedad democrática, utilizando en este sentido los términos del propio CEDH.

---

de junio de ese mismo año, que tuvieron lugar bajo los auspicios del Consejo de Europa, ya iban en la misma línea de protección del individuo amenazado por los métodos de acopio y transmisión de las informaciones sobre sus datos personales.

[2] STC 25/81, FJ 5.

[3] Buena muestra de ello son, por ejemplo, la Ordenanza Procesal Alemana de 1975, § 100 a) y b). Otro tanto sucede, con el CPP Italiano en cuyos artículo 266 a 271 se regula en parecidos términos la limitación de este derecho. Finalmente, el CPP francés, en su artículo 100 dispone una normativa muy parecida a los anteriores. En otra nota a pie de página de este trabajo se hace una descripción más detallada de la normativa procesal de estos tres países en relación con las exigencias de previsión legislativa que deben cumplir los ordenamientos procesales de los Estados miembros del Consejo de Europa para cubrir las exigencias del art. 8 del CEDH.

El TC asumió ya a partir del año 1984, con su conocida STC 114/1984, la ingente tarea de la defensa de este derecho fundamental, partiendo de una normativa legal a todas luces insuficiente y que aunque fue atemperada en cierto modo por su propia doctrina jurisprudencial y por la reforma que fue introducida por la LO 4/1988, de 25 de mayo, aún hoy, como tendremos ocasión de constatar a lo largo de este trabajo, resulta enormemente insuficiente por los vacíos esenciales que se advierten y que han tratado de ser suplidos por una Jurisprudencia, tanto del propio TC, como del Tribunal Supremo, que, a veces, resulta vacilante en algunos extremos.

Sin duda, después de más veinticinco años de funcionamiento y de casi otros tantos desde que fue afrontado por primera vez el reto de establecer el contenido propio del derecho al secreto de las comunicaciones, hoy el TC se mantiene firme en su papel de guardián de los derechos fundamentales consagrados en nuestra Carta Magna, particularmente en el que ahora será objeto de nuestro estudio, teniendo en cuenta su notable incidencia en una jurisdicción como la penal que es especialmente sensible para el bienestar social de los ciudadanos.

La tarea, sin duda apasionante, de abordar en este trabajo el estudio de la doctrina del Tribunal sobre el derecho al secreto de las comunicaciones y las tolerables o intolerables injerencias en el mismo, según lo resuelto en cada caso por los distintos pronunciamientos realizados, presenta notables retos no ajenos a alguna dificultad en la exposición de la doctrina más reciente del Tribunal, motivada en cierta manera por la propia evolución que ha experimentado en los últimos años como consecuencia, en unos casos de la establecida por el Tribunal Europeo de Derechos Humanos, que es referente obligado en la práctica de nuestros Tribunales por la vinculación constitucional y la incorporación al ordenamiento interno de los postulados doctrinales de aquél en relación con los derechos contenidos en el Convenio de Roma, sino también por la jurisprudencia del Tribunal Supremo en algunos extremos, como por ejemplo, en lo relativo a la validez y eficacia de las pruebas derivadas de otra obtenida con vulneración de derechos fundamentales con las que se halle relacionada por una «conexión de antijuricidad»[4] que, de

[4] Doctrina esta introducida por vez primera por la STC 81/1998 y que, en cierto modo, ya había ido dibujando la jurisprudencia del TS en pronunciamientos de fecha anterior, aunque no de modo tan claro. En este sentido, por ejemplo, la STS de 4 de marzo de 1997 (RJ 2215), al referirse a la prohibición de la prueba constitucionalmente ilícita, destacaba de modo textual lo siguiente: «La prohibición alcanza tanto a la prueba en cuya obtención se haya vulnerado un derecho fundamental como a aquellas otras que, habiéndose obtenido lícitamente, se basan, apoyan o deriven de la anterior ("directa o indirectamente"), pues sólo de este modo se asegura que la prueba ilícita inicial no surta efecto alguno en el proceso. Prohibir el uso directo de estos medios probatorios y tolerar su aprovechamiento

alguna manera, fue ya vislumbrada para la resolución de determinados casos. De todos modos, lo que ahora se pretende es la exposición sistematizada de la doctrina del TC más actual, tanto de lo relativo al contenido del derecho fundamental al secreto de las comunicaciones, como de lo atinente a la limitación de dicho derecho.

Para estructurar mejor el presente estudio, distinguiremos, por ello, dos grandes apartados en la ponencia: De una parte, el estudio del derecho al secreto de las comunicaciones y de otro lado su limitación mediante el procedimiento de intervención de las comunicaciones, para finalizar con una breve referencia a las limitaciones de este derecho en un ámbito específico y sensible como es el penitenciario.

II. **El derecho al secreto de las comunicaciones**

1. *Su reconocimiento normativo*

En la Constitución Española, a diferencia del CEDH que no lo reconoce explícitamente[5], se contempla de modo expreso como derecho fundamental el secreto de las comunicaciones postales, telefónicas y telegráficas, que sólo puede quedar limitado mediante resolución judicial motivada, salvo, lógicamente, el consentimiento del o de los interesados, que en este caso serían los propios interlocutores en la comunicación.

Por su parte, la normativa legal del reconocimiento de este derecho viene contenida en el art. 33 de la L 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo que se refiere a las comunicaciones mediante aparatos electrónicos, telefónicos o de cualquier otra índole; y, en lo que atañe a las comunicaciones postales en el art. 3 de la L 24/1998, de 13 de julio, de Regulación del Servicio Postal Universal y de Liberali-

---

indirecto constituiría una proclamación vacía de contenido efectivo, e incluso una incitación a la utilización de procedimientos inconstitucionales que, indirectamente, surtirían efecto. Los frutos del árbol envenenado deben estar, y están (art. 11.1 de la LOPJ), jurídicamente contaminados. El efecto expansivo prevenido en el art. 11.1 de la LOPJ únicamente faculta para valorar pruebas independientes, es decir, que no tengan conexión causal con la ilícitamente practicada, debiéndose poner especial atención en no confundir "prueba diferente" (pero derivada), con "prueba independiente" (sin conexión causal)».

[5] Aunque ya el TEDH desde su primer pronunciamiento sobre la materia, recaído en la STEDH de 6 de septiembre de 1978, Caso Klass y otros contra Alemania, convino en destacar de modo textual que «aunque el párrafo 1.º del artículo 8 no menciona las conversaciones telefónicas, el Tribunal estima con la Comisión que se encuentran comprendidas en las nociones de "vida privada" y de "correspondencia", señaladas por este texto». Tal afirmación ha sido sostenida por todas las sentencias que sobre la materia ha dictado con posterioridad el Tribunal.

zación de los Servicios Postales. Igualmente, el RD 1829/1999, de 3 de diciembre, que aprobó el Reglamento por el que se regula la prestación de los servicios postales y de correspondencia, establece en su art. 13 un concepto auténtico de lo que ha de entenderse por envíos postales, siendo de particular relevancia a los efectos del derecho fundamental que estudiamos, los conceptos de carta y de paquete postal que son aquellos envíos que gozan primordialmente de la protección del derecho al secreto por parte de la doctrina constitucional. Asimismo, en el art. 15 de este Reglamento se establece una detallada normativa sobre los envíos que se consideran prohibidos.

Igualmente, en el ámbito que ahora nos interesa, la normativa legal que se refiere al procedimiento de limitación de este derecho viene recogida con carácter general en los arts. 579 a 588 de la LECrim, regulando, de una parte la limitación del derecho al secreto de las comunicaciones telefónicas y telegráficas, y de otro la de la comunicación postal, teniendo en cuenta, no obstante, que respecto de esta última también guarda relación la normativa específica en materia de entregas controladas que contempla el art. 263 bis de la LECrim.

Tampoco hay que olvidar, al respecto, lo establecido en los arts. 188 y ss. del Código Procesal Militar, aprobado por LO 2/1989, de 13 de abril, que reconocen la competencia de los Jueces Togados Militares para acordar la intervención y grabación de las conversaciones telefónicas así como de la interceptación y apertura de la correspondencia, en términos semejantes a los regulados en la norma procesal común, dentro del ámbito estrictamente castrense.

Y, finalmente, también en el campo del Derecho Penitenciario, el art. 51 de la LOGP y los arts. 41 y ss. del Reglamento que la desarrolla aprobado por RD 190/1996, de 9 de febrero, establecen la regulación de la limitación de este derecho de comunicación para los internos en Centros Penitenciarios.

2. *Su concepto y ámbito de protección*

Dado que nos hallamos ante un derecho fundamental que se encuentra dentro de la órbita de la «vida privada», de la «privacy» en propia terminología original del TEDH[6], y de la «correspondencia», en el sentido de que la «vida privada» engloba el libre ejercicio del derecho

[6] SSTEDH de 6 de septiembre de 1978, Caso KLASS y otros contra Alemania, 2 de agosto de 1984, caso MALONE contra el Reino Unido, 24 de abril de 1990, casos KRUSLIN y HUVIG contra Francia, o mucho más recientemente, de 16 de febrero de 2000, caso AMANN contra Suiza.

del individuo a llevar a efecto y desarrollar relaciones de toda índole, ya sean personales, comerciales o profesionales, con sus semejantes, el TC[7], siguiendo a este respecto la doctrina de aquél, ha destacado que «la observación de las telecomunicaciones supone una grave injerencia en la esfera de la intimidad personal constitucionalmente reconocida (y) como tal injerencia ha de estar sometida al principio de legalidad y, en especial, al de proporcionalidad».

E, igualmente, la jurisprudencia del TC, ya desde su primera sentencia[8] sobre la materia, se encargó de poner de manifiesto, con apoyo en el art. 18.3 de la CE, que el derecho al secreto de las comunicaciones consagra, de modo implícito, la libertad de las comunicaciones y, expresamente, su secreto, destacando su aspecto eminentemente formal.

De esta definición conceptual, puede decirse, por tanto, que el derecho al secreto de las comunicaciones se configura en un doble sentido. De una parte, abarcando el derecho a comunicarse libremente, esto es a utilizar los medios técnicos de comunicación sin ningún tipo de trabas o limitaciones. Y de otro lado, extendiéndose, también, en cuanto «secreto» que es, al contenido de lo comunicado o conversado, cualquiera que fuere éste, es decir, con independencia de que hubiere sido de índole personal, comercial o simplemente intranscendente. Finalmente, también cubre otros aspectos de la comunicación, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales[9].

Sobre este último particular ha establecido también el TC[10], siguiendo en este punto la doctrina del TEDH, que forman parte del contenido de este derecho determinados elementos de información que tienen que ver con la comunicación, con los interlocutores o con el propio procedimiento o sistema de comunicación. Así, el denominado sistema de recuento o «comptage», procedimiento éste que consiste en limitar la observación al conocimiento del registro de los números marcados desde un aparato telefónico, a la hora y duración de la llamada, así como también al acceso a la identidad de los titulares de listas de llamadas

[7] STC 85/94, FJ 3. En el mismo sentido, SSTC 54/96 y 123/97, así como ATC 344/90. También el Tribunal Supremo en SSTS de 23 de mayo de 1996 (RJ 4556), 20 de diciembre de 1996 (RJ 9038) y 2 de diciembre de 1997 (RJ 8762).

[8] La conocida STC 114/1984, luego reiterada en sus criterios doctrinales por la STC 34/1996, entre otras.

[9] SSTC 123/2002 y 56/2003.

[10] SSTC 123/2002 y 56/2003.

enviadas o recibidas desde un aparato de comunicación, son aspectos periféricos que también integran el contenido del derecho[11].

En el mismo sentido y por lo que se refiere al secreto de las comunicaciones postales, el art. 3 de la L 24/1998, que hemos citado anteriormente, establece la extensión del derecho al secreto, no sólo a la libre circulación de envíos postales y al contenido de lo enviado, sino también y de modo expreso, a la propia existencia de dicho envío postal, a su clase, a sus circunstancias exteriores, a la identidad del remitente y del destinatario y a sus direcciones postales. El ámbito del contenido de este derecho, según la normativa ahora citada, es por tanto bastante amplio, pues alude no sólo a lo que es propiamente la comunicación postal, es decir la carta personal o el paquete postal, sino también a determinados datos periféricos que integran la misma.

Como podemos apreciar de lo expuesto hasta ahora, los perfiles de este derecho fundamental resultan bastante amplios pudiéndose concretar en la afirmación de que sea cual sea el ámbito objetivo del concepto de «comunicación» y del artilugio o aparato técnico utilizado para su realización, el derecho fundamental se dirige inequívocamente a garantizar su impenetrabilidad por terceros, ya sean personas públicas o privadas, ajenos a la comunicación misma, de tal manera que el derecho no puede ser vulnerado por ninguno de los que intervienen en la comunicación[12], sino que sólo resulta intolerable esta injerencia cuando, al margen de los mecanismos de control y garantía, un tercero no partícipe en la comunicación, interviene de cualquier manera en la misma y obtiene datos no autorizados que puedan derivarse del contenido de lo comunicado o de la identificación de los interlocutores.

En definitiva, la casuística jurisprudencial ha delimitado en muchos casos el contenido de este derecho, si bien puede afirmarse con carácter general que habrá afectación del derecho al secreto de las comunicaciones cuando se trate de un tercero que incide en el ámbito de la comu-

---

[11] En concreto, en la STC 123/2002, se destaca que la entrega de los listados por las compañías telefónicas a la Policía, sin el consentimiento del titular del teléfono, requiere resolución judicial «pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones».

[12] No de ninguno de los interlocutores o que hayan intervenido en el acto de la comunicación. (STC 56/2003). En alguna legislación interna como la suiza esto no ocurre así, pues, la STEDH de 12 de julio de 1988, caso SCHENK contra Suiza, hubo de tomar en consideración, entre otros extremos, que, conforme al art. 179 ter del CP suizo de 27 de febrero de 1980 aplicable al caso, las grabaciones de conversaciones telefónicas propias sostenidas con otra persona, sin el conocimiento de ésta o sin la oportuna autorización aparecen tipificadas como delito.

nicación entre dos interlocutores mediante la utilización de aparatos de captación, sintonización o desvío de la señal[13], cuando la comunicación se realice, bien a través de un artilugio técnico, cualquiera que sea[14] éste, si se trata de comunicaciones telefónicas o telegráficas, bien a través de un envío postal, en el caso del secreto de la correspondencia.

Además, únicamente habrá afectación de este derecho cuando la injerencia se produzca en el transcurso de la comunicación o con relación a la misma. Este aspecto es importante porque, en algún caso, determi-

---

[13] En el caso del secreto de las comunicaciones, si el soporte en el que se recoge el contenido de una conversación y dicha conversación se ha realizado directamente sin utilizar ningún artilugio técnico de comunicación (es decir, la conversación realizada directamente entre dos personas), en este caso no habrá afectación de este derecho sino del derecho a la intimidad. Resulta interesante en este sentido la STS de 10 de febrero de 1998 (RJ 948) que alude a la grabación mediante aparatos de escucha de la conversación sostenida por dos internos que compartían celda en un establecimiento penitenciario y que implicaban a un tercero en el mismo. La grabación había sido autorizada judicialmente. Igualmente, es interesante el ATC 15/2004 que se refiere a un supuesto en el que un policía, situado cerca de una cabina telefónica desde la que con anterioridad se habían dado algunos comunicados en nombre de una organización terrorista, de la falsa colocación de artefactos explosivos, escuchó a la acusada realizar una de estas llamadas a un Organismo de recepción de llamadas de urgencia, anunciando la explosión próxima de un artefacto explosivo; en tales casos, tampoco habrá incidencia en el derecho al secreto de las comunicaciones, por cuanto el conocimiento del contenido de la misma lo fue directamente. Así, el FJ 4 de esta resolución destaca textualmente lo siguiente: «Hemos sostenido (últimamente en nuestra STC 123/2002, de 20 de mayo) que este derecho fundamental al secreto de las comunicaciones garantiza a los interlocutores o comunicantes la confidencialidad de la comunicación telefónica que comprende el secreto de la existencia de la comunicación misma y el contenido de lo comunicado, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino; y ello con independencia del carácter público o privado de la red de transmisión de la comunicación y del medio de transmisión —eléctrico, electromagnético u óptico, etc.— de la misma. En consecuencia, la vulneración del *derecho al secreto de las comunicaciones telefónicas requiere la interferencia directa en el proceso de comunicación mediante el empleo de cualquier artificio técnico de captación, sintonización o desvío y recepción de la señal telefónica como forma de acceso a los datos confidenciales de la comunicación*: su existencia, contenido y las circunstancias externas del proceso de comunicación antes mencionadas, lo que no se ha producido en este caso en el que la audición de la conversación se produce de modo directo, sin intervención técnica alguna».

[14] Fax, módems, correo electrónico, teléfonos fijos (públicos o privados) o móviles, etc. Ver a este respecto las SSTC 34/1996 y 70/2002 y también la STS de 8 de febrero de 1999 (RJ 291) que alude a la captación por medio de un escáner de una conversación telefónica realizada con teléfono móvil. Por su parte, al STS de 14 de junio de 2006 (RJ 5581) señala que no afecta al contenido del secreto de las comunicaciones «el control de las señales de posicionamiento del dispositivo correspondiente a un teléfono», toda vez que se limita a determinar el punto geográfico desde el que se hacen la comunicaciones pero sin incidir en las mismas.

nadas conversaciones telefónicas o simplemente un mensaje telefónico que haya quedado registrado en una cinta de grabación de mensajes o en el buzón de voz de un teléfono y el acceso a su contenido, cuando ya se ha emitido el citado mensaje o la conversación ha tenido lugar, no determinará la existencia de una afectación del derecho fundamental al secreto de las comunicaciones, sino al mencionado de la intimidad[15].

Destacar, para terminar que, con relación al específico derecho al secreto de las comunicaciones postales, la STC 281/2006, de 9 de octubre ha establecido un importantísimo cuerpo de doctrina que ha delimitado el entorno propio del contenido del derecho. A este respecto, la doctrina del Tribunal la podemos sistematizar en los siguientes puntos:

1.º Contenido del derecho al secreto de la comunicación postal:

El Tribunal ha señalado que este derecho no se refiere al secreto postal, sino a la comunicación postal. La consecuencia de esta afirmación es que no todo envío o intercambio de objetos o señales que puedan realizarse por medio de los servicios postales es una comunicación postal amparada por este derecho fundamental.

A este respecto, precisa que, por comunicación ha de entenderse todo proceso de transmisión de mensajes entre personas determinadas. Por tanto, la comunicación postal y el derecho al secreto que la ampara sólo protege el intercambio de objetos a través de los cuales se transmiten mensajes mediante signos lingüísticos. Sólo en este sentido, la comunicación postal equivale a correspondencia, quedando amparada por el derecho fundamental.

2.º Objeto de la correspondencia (comunicación postal):

Más adelante, puntualiza el Tribunal que, en la medida en que los mensajes pueden expresarse, no sólo a través de palabras, sino también mediante otros signos o señales que pueden recogerse, además de en papel, en otros soportes (cintas de cassette, vídeo, CD, DVD, etc.) a los efectos de delimitar el objeto de la correspondencia y teniendo en cuenta la normativa que se ha establecido legalmente sobre el Servicio Postal Universal, habrá que tener en cuenta los siguientes criterios delimitadores:

a) En primer lugar, las características externas sobre el tamaño del envío, que contienen los soportes físicos en donde se guarde el mensa-

[15] Dice a este respecto la STC 70/2002 (FJ 9 b) que «la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos». Ver, también, la STS de 27 de junio de 1994 (RJ 5034).

je: cartas, paquetes, … Quedan excluidos, por tanto, del concepto de envío postal aquellos objetos que por sus propias características no sean usualmente utilizados para contener correspondencia individual sino que sirvan para el transporte de mercancías. Si en ellos se contienen mensajes no modificará su régimen de protección constitucional (se tratará de injerencias al derecho a la intimidad pero no al secreto de la correspondencia)[16].

b) Tampoco se incluyen aquellos tipos de paquetes que, aún teniendo características propias de tales y que pudieran contener correspondencia, sin embargo la regulación legal los excluye expresamente (p. ej., los paquetes que tienen unas dimensiones que exceden de la establecida normativamente en el RD 1829/1999, de 3 de diciembre, art. 13.2).
c) Finalmente, no estarán tampoco bajo la protección de este derecho, aquellas formas de envío de la correspondencia que se configuran legalmente como comunicación abierta para inspección postal (p. ej., los paquetes con etiqueta verde), en la medida en que los titulares de los mismos habrán renunciado previamente al secreto para que así puedan aquellos circular.

Por último, destacar que la protección constitucional del derecho al secreto se extiende a cualesquiera tipos de envío, con independencia de que se realicen a través de un servicio público de correos o, por el contrario, mediante empresas privadas de mensajería, pero en todo caso es necesario que el porte del envío lo sea a través de profesionales de la mensajería (no de terceras personas que por razón particular porten el paquete en un determinado momento).

3.º Vulneración del derecho al secreto de la comunicación postal:

Se vulnera este derecho cuando, empleando cualquier modo o procedimiento, se accede, llegándose a conocer, al contenido del mensaje, con independencia de que se abra o no el paquete o envío. Igualmente, se producirá una injerencia intolerable en el derecho al secreto cuando, iniciada la comunicación, se tiene conocimiento de cualesquiera datos relacionados con la propia comunicación: La existencia misma de dicha comunicación, la identidad del remitente y destinatario, el momento en que se produce, los lugares de remisión y de destino (ver art. 6 del RD 1829/1999, de 3 de diciembre).

---

[16] Puede citarse al respecto, el supuesto de hecho que fue enjuiciado en el ATC 395/2003, en que el paquete no era otra cosa que un tubo en forma de cilindro de madera al que estaban enrollados de forma visible varios metros de cable del tendido eléctrico en cuyo interior se encontraba la cocaína que fue aprehendida.

Ahora bien, no se vulnera cuando sin tomar conocimiento del contenido del mensaje, lo que se identifica dentro del sobre o del soporte es un contenido ilícito, pero no sirve para conocer el mensaje mismo (p. ej., inspecciones mediante perros, scáneres, etc.). El dato es importante, porque según esta doctrina no queda afectado el derecho fundamental si, por ejemplo, se taladra un pequeño agujero con un punzón en el paquete y se llega al convencimiento de que lo que hay dentro es droga, pero sin llegar a tener conocimiento del mensaje que pueda contener.

Para finalizar, por tanto, este apartado, sería necesario deducir cuáles son las consecuencias de esta novedosa doctrina, que podemos concretar en las siguientes precisiones:

1.ª Este derecho no ampara el envío de mercancías o el transporte de enseres personales (maletas, maletines, bolsas de viaje, etc.) aunque lo sean por medio de empresas que realicen un servicio postal (lo afectado en este caso sería el derecho a la intimidad, pero en estos supuestos, la Policía Judicial, con criterios de proporcionalidad y con la necesaria habilitación legal, puede abrirlos sin requerir autorización judicial).

2.ª Este derecho no protege directamente el soporte físico donde se contenga el mensaje (sino el contenido del mensaje), de tal modo que cualquier objeto que pueda servir de soporte para la comunicación postal (sobre, paquetes, cartas, cintas, etc.) únicamente gozará de esta protección cuando de modo efectivo sirva para el acto comunicativo y el proceso de comunicación haya sido iniciado, de tal modo que la interceptación ocurra mientras dicho proceso tiene lugar. Por tanto, no queda afectado este derecho cuando los soportes (cartas, paquetes, etc.) se portan por su propietarios o por terceros ajenos a los servicios postales, o viaja con ellos o los mantiene a su disposición durante el viaje. Este aspecto es importante porque la carta o el paquete intervenido a una persona que no realice un servicio de mensajería o de envío postal, podrá ser interceptado y abierto sin vulnerar este derecho. Sería el derecho a la intimidad el que sufriera en tal caso la injerencia.

3. *Los titulares del derecho*

A la hora de delimitar el ámbito de la titularidad del derecho consagrado en el art. 18. 3 CE hay que partir de que la dicción literal de este precepto se limita al reconocimiento expreso de la garantía del derecho sin especificar quiénes hayan de ser los titulares del mismo.

Por tanto, en principio, la titularidad de este derecho ha de ser entendida en un sentido amplio y flexible[17], abarcando, en consecuencia, tanto a las personas individuales (mayores y menores de edad) como a las jurídicas (públicas como privadas) a los nacionales como a los extranjeros, incluso entiendo que a los residentes, legales o ilegales, o a los meros transeúntes que se encuentren temporalmente en nuestro País, e, incluso, a las personas que puedan encontrarse fuera del mismo si la investigación del delito compete a las autoridades judiciales españolas, de acuerdo con los criterios de extensión y límites de la jurisdicción establecidos en el art. 23 LOPJ, conforme a la interpretación establecida por la propia doctrina del TC[18] y siempre que los medios técnicos, lógicamente permitan la limitación efectiva del derecho. Es decir, desde la perspectiva de la titularidad se tiene una visión general de protección y así lo ha entendido el Tribunal al analizar el problema.

A pesar de ello y en lo que concierne al ámbito del proceso penal, hay que matizar que, aún cuando hemos afirmado que las personas jurídicas son titulares de este derecho, es evidente que, a ellas en sí mismas consideradas, no es posible la limitación de aquél con fines de investigación criminal, pues en nuestro ordenamiento penal, a diferencia de otros de nuestro entorno europeo como el francés, las personas jurídicas no pueden delinquir, por lo que, en tales casos, aún cuando los sistemas de comunicación presuntamente empleados para la comisión de hechos delictivos y que puedan ser por ello objeto de intervención, figuren a nombre o bajo la titularidad de dichas personas jurídicas, la limitación del derecho fundamental sólo será posible respecto de los representantes o personas físicas que tengan reconocido el poder de actuar en su nombre, pues a ellos les será imputado el delito correspondiente.

Otro de los aspectos a considerar en este apartado, por la relevancia que le ha concedido el Tribunal en algunos de sus pronunciamientos, se refiere al reconocimiento que su doctrina hace de la titularidad de este derecho, de su ejercicio y también de sus limitaciones, a los internos en Centros Penitenciarios. En concreto, siguiendo una línea uniforme,

---

[17] Así lo pone de manifiesto la Jurisprudencia del TS (SSTS de 2 de abril y de 19 de octubre de 1996 (RJ 3215 y 7834), 4 de febrero y 8 de febrero de 1997 (RJ 1275 y 888), 2 de diciembre de 1997 (RJ 8762) y 22 de abril de 1998 (RJ 3811) entre otras muchas). En concreto, la última de las sentencias citadas destaca textualmente que «son titulares las personas físicas y las jurídicas, tanto nacionales como extranjeras, mayores y menores de edad, porque el secreto de las comunicaciones presupone la libertad, y su restricción se produce en un sentido de control y observación, no propiamente de impedimento a las comunicaciones, y se extiende tanto al conocimiento del contenido de las mismas, como a la identidad de los interlocutores».

[18] STC 237/2005, Caso Rigoberta Menchú.

el Tribunal pone de manifiesto que «en principio el recluso goza… del derecho al secreto de las comunicaciones, aunque pueda verse afectado por las limitaciones mencionadas» (se refiere a los derechos que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria), agregando al respecto:

> «este derecho tiene una incidencia sustancial en el desarrollo de la personalidad de los internos y adquiere por ello suma relevancia en orden al cumplimiento de la finalidad, no exclusiva, de reinserción social de las penas privativas de libertad que establece el primer inciso del art. 25.2 CE. Mediante la comunicación oral y escrita con otros sujetos, el preso no queda reducido exclusivamente al mundo carcelario y ello le permite relacionarse con el exterior y, en definitiva, prepararse para su futura vida en el seno de la sociedad»[19].

Otro de los temas a abordar en este apartado se refiere a la mención obligada a la doctrina del TEDH sobre este extremo, destacando también que ese Tribunal, a pesar de los términos estrictos del art. 34 del CEDH, en lo que se refiere a la legitimación para formular demanda, ha interpretado de modo flexible los términos «personas individuales» a que se alude en el mismo, extendiendo su cobertura tanto a las personas físicas como jurídicas, por tratarse de un derecho que, por su naturaleza, puede ser ejercido por unas y por otras. Además, como hemos visto anteriormente, ha sido siempre una línea directriz de su doctrina que el concepto de «vida privada» abarque a todo tipo de relaciones[20], extendiendo a toda clase de personas la idea de «vida privada» y de «correspondencia» contemplados en el art. 8.1 del CEDH, a los efectos de su protección.

Sí es importante también destacar, porque en este punto difiere la doctrina del TEDH del tratamiento jurisprudencial que le brindan los Tribunales de nuestro País, el hecho de que el art. 8 del CEDH contemple un abanico mucho más amplio que el que ofrece el ordenamiento español en materia de limitación de este derecho fundamental, lo que, a la larga, amplía también el ámbito del ejercicio de este derecho, al abarcar

---

[19] STC 200/1997 (FJ 2); en el mismo sentido, SSTC 170/1996, 128/1997 y 175/1997, entre otras.

[20] Tal es el caso, por ejemplo, tanto de los despachos de abogados como empresariales. Respecto de los despachos de abogados pueden consultarse en este sentido las SSTEDH de 16 de diciembre de 1992, caso Niemietz contra Alemania, 25 de junio de 1997, Caso Halford contra el Reino Unido y de 25 de marzo de 1998, caso KOPP contra Suiza; y SSTEDH de 30 de junio de 1998, caso Valenzuela Contreras contra España y de 16 de febrero de 2000, caso Amann contra Suiza, respecto de los despachos empresariales.

aspectos o cuestiones que no son estrictas del procedimiento penal ni de la investigación de los delitos, pero que dan idea de la especial relevancia que el Tribunal Europeo concede a la protección de este derecho y al establecimiento de unos límites precisos a la injerencia por parte de los poderes públicos. Así, es posible destacar que, junto al enjuiciamiento de cuestiones que en su gran mayoría tienen que ver con lesiones al derecho fundamental que guardan relación con el proceso penal y, en concreto, con el enjuiciamiento de los casos de limitación de su ejercicio como consecuencia de una intervención acordada judicialmente y de la eventual afectación del derecho a un proceso justo y equitativo, también el TEDH ha tenido ocasión de pronunciarse cuando la interceptación de las comunicaciones ha tenido lugar como consecuencia de otros fines ajenos a la investigación penal, esencialmente cuando se han perseguido objetivos políticos, fundamentando en razones de seguridad interna y defensa nacional la razón de tales escuchas[21], o para supervisar, en el ámbito de las relaciones funcionariales, las conversaciones telefónicas sostenidas desde teléfonos instalados en despachos públicos y conectados por una red interna[22], estableciendo un cuerpo de doctrina al

---

[21] Además de la anteriormente citada STEDH de 6 septiembre de 1978, caso KLASS, podemos destacar la STEDH de 16 de febrero de 2000, caso AMANN contra Suiza. En este último supuesto el Tribunal tuvo ocasión de pronunciarse sobre la normativa suiza que regulaba la posibilidad de que el Ministerio Público Federal de dicho país ordenara, en determinados casos, la intervención de las comunicaciones para prevenir todos aquellos actos que pudieran poner en peligro la seguridad interior o exterior de la Confederación. Dicha normativa se fundamentaba en una Decisión del Consejo Federal Suizo de 29 de abril de 1958.

[22] En la STEDH de 25 de junio de 1997, caso HALFORD contra el Reino Unido se analizó la denuncia planteada por la Sra. Halford, por la que se alegaba que las líneas telefónicas, tanto de su despacho oficial en la Comisaría de Policía de Merseyside como de su domicilio, habían sido interceptadas sin habilitación legal y sin la debida autorización, agregando una segunda pretensión a la anterior relativa a que no disponía en el Derecho Interno de su país de ningún recurso efectivo para impugnarlas.

En concreto, los principales hechos que se recogen en la sentencia aluden a que la requirente había sido nombrada Inspectora General de la Policía de la localidad británica de Merseyside siendo la mujer que más alta graduación había alcanzado en la organización policial de dicho país. Con posterioridad, solicitó un nuevo ascenso que le fue denegado, por lo que en 1990 presentó una demanda por discriminación de sexo contra el Ministro del Interior y contra el Comité de Control de la Policía de dicha localidad.

Pues bien, a raíz del planteamiento de dicha reclamación judicial la requirente adujo que, como consecuencia de la misma, tanto el teléfono con línea privada que le había sido asignado a su despacho oficial como el instalado en su domicilio había sido interceptado con objeto de recoger información que pudiera ser utilizada en defensa de las pretensiones de los superiores de la actora en el proceso que ésta había iniciado.

El Gobierno Británico, por su parte, antes de la presentación de la demanda había reconocido que existían bastantes probabilidades de que varias de las conversaciones

respecto con apoyo en las exigencias de previsión legislativa, racionalidad en la adopción de la medida y control por las Autoridades Públicas correspondientes, tanto de su decisión de adoptarlas como del ulterior control de su ejecución.

Por último, para completar este apartado hay que aludir necesariamente a los terceros interlocutores, que no siendo imputados por cuanto no son objeto de investigación, se ven, también, afectados en su derecho fundamental por haber participado en un acto de comunicación utilizando un aparato o servicio de correspondencia que haya sido intervenido a los efectos de la investigación.

Lógicamente y con carácter general la eventual intromisión ilegítima en su derecho les confiere legitimación para invocar dichos derechos en amparo. Particular mención hace a este respecto la STC 165/2005 (FJ 2) cuando destaca que están legitimados (los recurrentes) para alegar vulneración de su derecho al secreto de las comunicaciones porque aunque no son titulares de los teléfonos intervenidos ni éstos se puedan encontrar en los domicilios de los imputados (y recurrentes en dicho procedimiento de amparo), ellos han sido interlocutores de las comunicaciones intervenidas y estas comunicaciones han sido utilizadas como pruebas para fundar su responsabilidad penal.

El problema, sin embargo, no se agota con esta legitimación general, por cuanto en determinados casos esos terceros no son personas que casualmente hayan realizado algún acto de comunicación desde o al aparato intervenido o hayan mantenido una ocasional correspondencia con los investigados, sino que pueden guardar algún tipo de relación con los sometidos a investigación como consecuencia de una relación profesional con ellos. Hemos de referirnos, en concreto, a los abogados

---

sostenidas por la Sra. Halford desde el teléfono de su despacho oficial hubieran sido intervenidas, pero rechazó que el teléfono de su domicilio particular hubiera sido también interceptado. Ahora bien, alegó como pretexto respecto del reconocimiento de dichas interceptaciones que se trataba de un teléfono integrado dentro de un sistema de red interna que, por razones de seguridad, permitía que las llamadas entrantes en el mismo podían ser interceptadas y que, por otra parte, se trataba de un supuesto no contemplado en la normativa británica de 1985 reguladora del sistema de escuchas telefónicas, por lo que no se precisaba de autorización previa para dicha intervención. La Sra. Halford sostendría posteriormente en su demanda que ella no había tenido conocimiento previo de tal posibilidad pues no se le había comunicado que dicho servicio interno de escuchas estuviere instalado. El Tribunal dio la razón a la requirente y apreció violación del art. 8 en este punto, por cuanto se trataba de un supuesto no previsto en la Ley y, por tanto, la interceptación no debería de haberse llevado a efecto. En relación con las supuestas escuchas de conversaciones sostenidas desde el teléfono del domicilio particular de la demandante, no quedó acreditado que las mismas se hubieren producido, por lo que el Tribunal desestimó la pretensión de la actora.

que, además, tengan a su cargo la defensa de los derechos e intereses de aquellas personas que, por otro lado no ha de olvidarse que no saben que están siendo investigados. Este problema, no resuelto por la normativa legal española, tiene que ser reinterpretado a la luz de la eficacia directa que tienen los derechos fundamentales y su aplicación directa por los Tribunales, siguiendo en este sentido toda la doctrina constitucional elaborada por el TC respecto de aquellos[23], toda vez que en este caso se verá afectado, no sólo el derecho al secreto de las comunicaciones de ambos interlocutores, el imputado y su letrado defensor, sino también el derecho de defensa del primero, que puede verse comprometido seriamente[24].

En tales supuestos, entiendo que sería procedente la legitimación para invocar la vulneración del derecho al secreto de las comunicaciones y del derecho de defensa. Se trata, en todo caso, de un tema espinoso que, como se ha indicado, carece de toda cobertura legal en nuestro ordenamiento.

Para finalizar este apartado y en relación con el derecho al secreto de la correspondencia es evidente que, en principio, son titulares de este derecho los dos interlocutores, esto es el remitente y el destinatario[25], cuyos conceptos vienen establecidos en el art. 3 del Reglamento del Servicio Postal de 1999 que hemos citado anteriormente[26]. Además, el art. 8 de este Reglamento regula la propiedad de los envíos postales, destacando que los envíos postales serán de la propiedad del remitente en tanto no lleguen a poder del destinatario, lo que es importante a los efectos de la investigación penal.

Ahora bien, cuando se produce una intervención judicial de la comunicación, en este caso de la correspondencia, para que ésta sea legítima,

---

[23] Así lo puso ya de manifiesto la añeja STC 15/1982, (FJ 8) cuando afirmó que «los principios constitucionales y los derechos y libertades fundamentales vinculan a todos los poderes públicos (artículos 9.1 y 53.1 de la Constitución) y son origen inmediato de derechos y obligaciones y no meros principios programáticos».

[24] Pensemos, por ejemplo, en la grabación de una conversación telefónica sostenida entre una persona imputada en un delito que no es objeto de la investigación sometida a la intervención, en la que revela a su abogado defensor determinados datos de aquel delito con objeto de que éste pueda articular mejor su defensa en ese proceso separado.

[25] Como sostiene la doctrina italiana (De Cupis, A.: *I diritti della personalitá*. Giuffrè, Milano, 1950), en la correspondencia epistolar se distinguen tres derechos: a) El derecho a la propiedad material, que corresponde al destinatario; b) el derecho de autor, que es propio del remitente; c) el derecho al secreto, que corresponde tanto al remitente como al destinatario.

[26] El art. 3 de este Reglamento dispone que se entiende por remitente la persona física o jurídica de quien procede el envío postal. Mientras que el destinatario será también aquella persona, física o jurídica, a la que va dirigido dicho envío.

es necesario que se encuentre incurso el afectado en un procedimiento penal, recayendo, al menos, sobre el mismo indicios racionales de criminalidad, cuando no procesado en la causa. Pero esta intervención repercutirá también en la otra persona destinataria de la correspondencia, si es que no ha mediado concierto previo y no se encuentra asimismo implicada en el procedimiento, e incluso, determinados terceros, citados en las cartas o paquetes postales intervenidos, que pueden, igualmente, verse afectados por dicha intervención.

En efecto, puede ocurrir que las manifestaciones de una carta intervenida judicialmente afecten a un tercero que ni siquiera sea el destinatario de la misma, por lo que no cabe duda de que este tercero, aunque extraño a la relación epistolar, tiene un derecho a la intimidad que es necesario proteger contra los actos de divulgación del contenido de la carta.

A estas terceras personas intermedias parece referirse el art. 579, apartado 3.º in fine de la LECrim cuando permite la observación judicial de las comunicaciones postales de las personas sobre las que existan indicios de responsabilidad criminal «así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos».

El derecho al secreto de las comunicaciones abarcará, por tanto, no sólo ya a los directamente vinculados por la correspondencia, esto es a los que aparecieren formalmente como remitente y destinatario en la carta o paquete postal girado, sino que también habrá de extenderse a aquellos terceros a los que se hiciere referencia en la correspondencia remitida o de los que se valieren, como dice el precepto citado, para la realización del hecho delictivo.

La delimitación de quiénes puedan ser los titulares de los derechos fundamentales afectados adquiere especial relieve a la hora de acordar alguna medida judicial restrictiva de este derecho.

4. *Su delimitación con el derecho a la intimidad*

Como ya hemos anticipado en otro apartado de este trabajo, tradicionalmente se ha incluido el derecho fundamental que estudiamos dentro del contexto de la «privacy» anglosajona, conceptuándolo, por tanto, como un derecho englobado dentro del derecho de toda persona a disponer de un círculo privado, de una privacidad en el ámbito de sus relaciones sociales, de tal modo que el derecho al secreto de las comunicaciones no vendría a resultar sino como una extensión más de ese derecho a lo privado.

Sin embargo, tanto la Constitución como la doctrina del TC se han encargado de otorgar sustantividad propia a este derecho, inclu-

yéndolo sistemáticamente dentro del artículo 18, pero en un apartado distinto del que recoge los derechos al honor, intimidad y propia imagen, pretendiendo de este modo darle una singularidad propia. Igualmente, el Alto Tribunal ha destacado las importantes diferencias que delimitan el ámbito de uno y otro derecho, poniéndolas de manifiesto, entre otras, en la importante STC 281/2006, FJ 3, en la que, aún con referencia al derecho al secreto de la correspondencia, es perfectamente ampliable al genérico de las comunicaciones, en la medida en que aquélla en cuanto modalidad de comunicación, se incluye también dentro de ese ámbito.

Pues bien, el Alto Tribunal se ha encargado de señalar hasta cuatro diferencias que sustancialmente sirven para distinguir con rotundidad el ámbito de uno y otro derecho:

1.ª En primer lugar, que el derecho al secreto de las comunicaciones exige resolución judicial para su limitación, mientras que en el caso del derecho a la intimidad personal, excepcionalmente la policía judicial, con habilitación legal, puede realizar determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que sean respetadas las exigencias derivadas del principio de proporcionalidad. El ámbito de protección, por tanto, de uno y otro derecho, son muy diferentes, toda vez que las garantías constitucionales y procesales exigidas para la limitación del derecho al secreto de las comunicaciones son muchísimo mayores que el establecido para la intimidad, pues, en este último caso, únicamente el requisito de la proporcionalidad es el que condiciona la injerencia, sin que sea precisa la previa autorización judicial para su limitación, excepción hecha, lógicamente, de los supuestos en que quede afecta la intimidad corporal que, por las propias exigencias del principio de proporcionalidad, que no por mandato constitucional expreso, precisan de autorización judicial para llevar a efecto la limitación del derecho (SSTC 37/1989, 207/1996 y 25/2005, entre otras).
2.ª En segundo término, el objeto directo de protección es el secreto de la comunicación, que se proyecta tanto sobre el proceso de comunicación como sobre el contenido de lo comunicado, con indiferencia de si este contenido tiene o no carácter íntimo. Por tanto, lo realmente relevante en este derecho, a diferencia del que afecta a la intimidad, es que se establece una cobertura de su contenido esencial, no sólo en el aspecto formal, esto es en lo relativo a la libertad de comunicación, sino también en su vertiente material, protegiendo el contenido de lo comunicado con

independencia de cuál sea dicho contenido. En el derecho a la intimidad, en cambio, la protección incide exclusivamente sobre el ámbito de lo material, esto es se protege en cuanto que forma parte del círculo privado del titular del derecho y todo lo demás queda fuera de dicho círculo de protección.

3.ª En tercer lugar, el Tribunal entiende que sólo se produce la injerencia en el secreto de las comunicaciones mientras que la comunicación tenga lugar. Una vez que se haya producido la misma, estaremos ante una limitación del derecho a la intimidad.

4.ª Finalmente, en cuarto lugar, la protección constitucional de este de derecho se limita a los terceros ajenos a los dos comunicantes, es decir, que únicamente opera cuando un tercero incide en el ámbito de la privacidad de la comunicación sostenida entre dos interlocutores, ya sea a través de cualesquiera aparatos o mecanismos de comunicación, como del uso de los servicios postales. En cambio, la protección del derecho a la intimidad opera frente a todos los demás, incluida la persona con la que se pueda realizar un determinado contacto, si el titular del derecho no permite su acceso a ese círculo privado de su propia esfera personal.

Por tanto, como puede advertirse, se trata de dos derechos fundamentales que tienen una sustantividad propia y que, aunque tangencialmente presentan linderos comunes que puedan inducir, a veces, a confusión, sin embargo mantienen su propia entidad, esencia y naturaleza dentro del ordenamiento constitucional español, aunque no así en el ámbito del Convenio de Roma, en que sus contornos no han sido precisados con tanta claridad por el TEDH, que ha incluido a ambos derechos dentro del más genérico derecho a la vida privada personal y familiar (art. 8.1 CEDH)[27].

III. **La limitación del derecho al secreto de las comunicaciones**

1. *Consideraciones previas: concepto y notas características*

El derecho al secreto de las comunicaciones, como cualesquiera otros derechos fundamentales a excepción del derecho a la vida y a la integridad física y moral, no son ilimitados, sino que, por el contrario pueden ser objeto de injerencia o limitación a su ejercicio en aras de la

[27] P. ej. SSTEDH de 18 de febrero de 2003, caso PRADO BUGALLO contra España (ap. 29 a 32) y 20 de diciembre de 2005, caso WISE contra Francia (ap. 29 a 34).

preservación de una serie de intereses generales que en el proceso penal se circunscriben a la investigación del delito, como lesión de bienes jurídicos colectivos o individuales que han de ser expresamente preservados, y a la determinación de los partícipes en el mismo, como respuesta social al injusto típico inferido.

GIMENO SENDRA[28] ha definido las intervenciones telefónicas como «todo acto de investigación, limitativo del derecho fundamental al secreto de las comunicaciones, por las que el Juez de Instrucción, en relación con un hecho punible de especial gravedad en el curso de un procedimiento penal, decide, mediante auto especialmente motivado, que por la policía judicial se proceda al registro de llamadas y/o a efectuar la grabación magnetofónica de las conversaciones telefónicas del imputado durante el tiempo imprescindible para poder preconstituir la prueba del hecho punible y la participación de su autor». El concepto también es aplicable, con las lógicas particularidades propias del tipo de comunicación de que se trata, a los supuestos de limitación de la correspondencia.

En todo caso y respecto de las mismas como se ha encargado de señalar el TEDH, existen hasta siete formas de injerencia en la correspondencia privada que es necesario matizar:

—Impedimento de iniciar la correspondencia[29].
—Apertura y lectura de la correspondencia[30].
—Interceptación, que supone el impedimento de remitir la correspondencia[31].
—Restricción, que supone la prohibición total durante un período de tiempo de remitir o recibir correspondencia[32].
—Retraso en el envío o en la recepción de la correspondencia[33].
—Aprehensión y examen tras un registro domiciliario de la correspondencia[34].

---

[28] GIMENO SENDRA, V.: «Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo». *Revista La Ley*, n.º 4024, 26 de abril de 1996, p. 2.

[29] En la STEDH ded 21 de febrero de 1975, caso GOLDER, decía el TEDH que «un obstáculo en la posibilidad misma de iniciar la correspondencia representa la forma más radical de injerencia» en el ejercicio del «derecho al respeto a la correspondencia». En el mismo sentido, por ejemplo, STEDH de 25 de febrero de 1992, caso MARGARETTA y ROGER ANDERSSON.

[30] STEDH de 25 de febrero de 1992, caso CAMPBELL.

[31] SSTEDH de 25 de marzo de 1983, caso SILVER, de 30 de agosto de 1990, caso MCCALLUM, de 27 de abril de 1988, caso BOYLE y RICE, de 24 de septiembre de 1992, caso HERCZEGFALVY.

[32] Informe de la Comisión relativo al caso MCCALLUM ya citado.

[33] Caso SILVER ya citado.

[34] SSTEDH de 16 de diciembre de 1992, caso NIEMIETZ, de 25 de febrero de 1993, casos FUNKE, CRÉMIEUX y MIIAILHE.

—Censura, que supone la eliminación de determinados pasajes de una carta[35].

Por consiguiente, la cuestión a resolver estriba en determinar si todas ellas o algunas, tan sólo, de las mismas son permitidas en nuestro ordenamiento jurídico.

El art. 579 de la LECrim parece referirse exclusivamente a algunos de estos supuestos de injerencia, en concreto a los de detención de la correspondencia, apertura y lectura de la misma.

A tales supuestos de injerencia también alude la Jurisprudencia[36] cuando indica que es permitida la interferencia de la autoridad pública en el ejercicio de este derecho fundamental, al contemplar en este precepto «la detención de la correspondencia privada, postal o telegráfica y su apertura y examen…».

Por consiguiente, no toda forma de injerencia realizada en el devenir normal de los envíos postales es permitida en nuestro ordenamiento, ni siquiera para la investigación de hechos delictivos.

El derecho a realizar envíos postales, por ejemplo, no puede ser restringido, como tampoco la censura de determinados pasajes de una correspondencia epistolar. La Autoridad Judicial únicamente puede interferir en el curso de los envíos realizados a través de las actuaciones ya citadas, pero en ningún caso, impedir la realización de tales actos, en cuanto manifestación del derecho a la libertad de comunicaciones que consagra el art. 18, 3.º de la CE.

De todo lo expuesto y tratando de establecer unos contenidos comunes mínimos a todas las manifestaciones de limitación del derecho, podemos afirmar que la intervención de cualesquiera comunicaciones viene, por tanto, delimitada por las siguientes notas características:

1.ª En primer lugar, la limitación del derecho fundamental tiene sentido únicamente cuando se realiza en el seno de una investigación criminal por delito, para determinar el hecho típico correspondiente y sus partícipes.
2.ª En segundo término, corresponde de manera exclusiva a la autoridad judicial, en el curso del proceso penal y en el cauce de un procedimiento por delito, la autorización motivada correspondiente para poder acordar la limitación del derecho y el control, tanto de la ejecución como de la conservación ulterior de lo obtenido con la intervención, en la medida en que se trata de un material preconstituido de imposible reproducción.

---

[35] STEDH de 25 de febrero de 1992, caso Pfeifer y Plank.
[36] Por ejemplo, STS de 5 de octubre de 1996 (RJ 7144).

3.ª Y, en tercer lugar, debe determinarse con antelación la duración de la medida limitativa del derecho que, en todo caso debe ser el tiempo imprescindible para la consecución de los fines constitucionalmente legítimos que se han expuesto.

2. *Presupuestos*

Siguiendo las directrices del TEDH, el TC ha puesto de manifiesto que son tres los presupuestos o exigencias previas que debe cumplir toda medida limitativa de este derecho fundamental cualquiera que sea el tipo de intervención de acto comunicativo de que se trate.

A) Cobertura legal

Es decir, que la medida limitativa del derecho esté «prevista por la ley». Como requisito expreso del art. 8.2 del CEDH la injerencia en la esfera privada de las personas mediante la intervención telefónica supone que la misma deba estar legalmente prevista, es decir contemplada por el Derecho Interno. Aún cuando el término «ley» ha sido interpretado por el TEDH con un criterio muy flexible, pues lo utiliza en sentido material y no formal[37], es decir que no exige el rango normativo de ley, sino que admite incluso que se trate de una disposición general de rango infralegislativo[38], lo que interesa fundamentalmente es que exista una norma de carácter general en el ordenamiento estatal que contemple, regule y establezca los límites y garantías para la adopción, ejecución y control de la medida. Tampoco importa al TEDH que la norma aparezca escrita o sea consuetudinaria[39], pues no puede olvidar que su doctrina ha de resultar aplicable tanto en los estados con ordenamientos que siguen los principios del sistema continental, como en aquellos otros, de raíz anglosajona, que han optado preponderantemente por el derecho consuetudinario[40].

---

[37] Así se expresan las SSTEDH de 24 de abril de 1990, casos Kruslin y Huvig contra Francia.

[38] STEDH de 18 de junio de 1971, caso De Wilde contra el Reino Unido.

[39] Así lo pone de manifiesto, también, en las SSTEDH de 26 de abril de 1979, caso Sunday Times, 22 de octubre de 1981, caso Dudgeon y 30 de marzo de 1989, caso Chappel, todos ellos contra el Reino Unido.

[40] En las dos SSTEDH de 24 de abril de 1990, casos Kruslin y Huvig contra Francia, que tienen el mismo texto en lo que se refiere a los fundamentos jurídicos se destaca muy expresivamente por el Tribunal que «… Ciertamente, las Sentencias en los casos Sunday Times, Dudgeon y Chappel se referían al Reino Unido; pero, sería un error exagerar la diferencia entre países de Common Law y "continentales", como con razón lo subraya el Gobierno. La ley escrita ("statute law") tiene también su importancia en los primeros. Y a la inversa,

Por tanto, de la doctrina del TEDH ahora resumida lo que más importa no es tanto la previa constatación de que la medida limitativa del derecho fundamental venga prevista en una norma de Derecho Interno, cuanto que dicha norma alcance una «calidad» determinada. Entiendo que la verdadera esencia de este presupuesto habilitante de la injerencia radica precisamente en la «calidad de la ley». A ello es a lo que dedica mayor atención el citado Tribunal a la hora de valorar la norma interna aplicable al caso.

Pues bien, la exigencia «calidad de la ley» presupone, a su vez, la necesaria constatación de que la norma cumpla tres requisitos básicos:

1.º En primer lugar, que sea accesible a todos los ciudadanos, es decir, que los términos de la ley sean lo suficientemente claros como para que aquéllos puedan comprender sin mayores dificultades los supuestos en que su derecho a la privacidad puede quedar limitado.
2.º En segundo término, que las consecuencias que puedan derivarse de las medidas limitativas del derecho fundamental sean «previsibles» para el sujeto afectado.
3.º Y, finalmente, en tercer lugar, que tales limitaciones o injerencias, tal como se prevén en la Ley, «sean compatibles con la preeminencia del derecho», es decir que la norma establezca las garantías necesarias para controlar el ámbito y aplicación de la medida de intervención.

Veamos cada una de estas exigencias por separado:

1.ª Accesibilidad de la ley: Se trata del requisito menos elaborado por la doctrina del TEDH, pues se limita a exigir que la Ley que prevea las medidas restrictivas de este derecho sea «accesible» para los sujetos afectados por las mismas[41].

---

la jurisprudencia desempeña tradicionalmente un papel destacado en los segundos, hasta el punto de que todas las ramas del Derecho positivo son resultado, en buena parte, de las resoluciones de los Jueces y Tribunales. Por lo demás, así lo ha tenido en cuenta el Tribunal en más de una ocasión para estos países (véanse, entre otras, las Sentencias Müller y otros de 24 mayo 1988, Salabiaku de 7 octubre 1988 y Markt Intem Verlag GmbH y K. Beemann, de 20 noviembre 1989). Si el Tribunal hubiera prescindido de la jurisprudencia habría socavado el régimen jurídico de los Estados "continentales" casi tanto como lo habría hecho su fallo en el caso Sunday Times de 26 abril 1979 con el del Reino Unido si hubiera excluido el Common Law del concepto de "ley"). En un ámbito amparado por el derecho escrito, la "ley" es el texto en vigor tal como los tribunales competentes lo han interpretado teniendo en cuenta, en su caso, la constante evolución jurídica».

[41] SSTEDH de 25 de marzo de 1998, caso Kopp contra Suiza (ap. 55 y 27), de abril de 2004, caso Doerga contra Países Bajos (ap. 45).

Así, en el caso MALONE contra el Reino Unido sí destaca con claridad esta exigencia y, haciéndose eco de la doctrina que había establecido ya con anterioridad para las injerencias en otros derechos de naturaleza pareja al que estudiamos, venía a declarar que «el ciudadano debe poder disponer de suficiente información, según las circunstancias, sobre las normas jurídicas aplicables a determinado caso». Además, agregaba, en segundo término, que «sólo se puede considerar como ley la norma que se expresa con la suficiente precisión para permitir al ciudadano que ajuste su conducta, y que pueda, en su caso con los adecuados asesoramientos, prever razonablemente las circunstancias que pueda ocasionar una acción determinada»[42].

De los términos recogidos en la sentencia parece deducirse que la nota esencial de esta exigencia radica en la necesidad de que los ciudadanos destinatarios de la norma tengan garantizado el acceso a su conocimiento mediante los correspondientes sistemas de publicación de la misma, circunstancia que, como indica DE LLERA SUÁREZ-BÁRCENA[43], ocurre con mayor facilidad en los sistemas jurídicos continentales que en los del Common Law, porque, lógicamente, en aquéllos predomina el Derecho escrito y publicado en los Boletines Oficiales correspondientes, mientras que en los segundos deviene de una tradición consuetudinaria no escrita y por ello de mayor dificultad en su conocimiento.

2.ª Previsibilidad de sus consecuencias: Con este requisito el TEDH pone de manifiesto que la ley que habilite las limitaciones o injerencias al derecho fundamental debe además ser muy clara y precisa en la fijación del ámbito y límites de tales medidas, de tal manera que debe expresarse, también, en unos términos tan claros y precisos que el ciudadano pueda conocer de manera suficiente en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas[44].

---

[42] El Tribunal lo que hizo fue reproducir en este caso su anterior doctrina contenida en sus sentencias relativas a los casos THE SUNDAY TIMES y SILVER.

[43] DE LLERA SUÁREZ-BÁRCENA, E.: *La observación o escucha de las comunicaciones telefónicas*. Estudios Jurídicos del Ministerio Fiscal. Tomo VI. Centro de Estudios Jurídicos de la Administración de Justicia. 1997, p. 471.

[44] Las SSTEDH de 24 de abril de 1990, casos KRUSLIN y HUVIG contra Francia fueron las primeras que aludieron precisamente a este sustancial requisito. Posteriormente, las SSTEDH de 25 de junio de 1997, caso HALFORD contra el Reino Unido, 25 de marzo de 1998, caso KOPP contra Suiza, 30 de julio de 1998, caso VALENZUELA CONTRERAS contra España y de 16 de febrero de 2000, caso AMANN contra Suiza han continuado insistiendo en el cumplimiento de esta exigencia para que la norma resulte compatible con el art. 8 del Convenio. En los dos primeros casos el Tribunal claramente destacaba que «el requisito de que sea previsible *no significa que el individuo pueda prever cuándo sus comunicaciones están expuestas a ser interceptadas por las autoridades para que pueda ajustar su proceder a este riesgo. No obstante, la ley debe ser lo suficientemente clara para señalar a todos las circunstancias y*

3.ª Compatibilidad de las medidas con la preeminencia del derecho: Con esta rúbrica tan llamativa y altisonante el TEDH llama la atención a los ordenamientos jurídicos internos sobre la exigencia que, a su juicio, contiene el núcleo más sustancial de este primer presupuesto de admisibilidad de una medida restrictiva del derecho fundamental.

Alude con este requisito a la necesidad de que la norma habilitante delimite con precisión las facultades de los poderes públicos a los que se les haya atribuido la potestad de acordar tales medidas limitativas del derecho de la manera necesaria y bastante como para garantizar la interdicción de la arbitrariedad.

En realidad, se trataría de dos requisitos englobados en uno sólo: De una parte, la ley debe indicar cuáles han de ser los extremos y circunstancias que permitan el establecimiento de la medida, es decir, lo que el TEDH denomina «garantías mínimas» que sean necesarias para evitar los abusos y arbitrariedades de los poderes públicos. Y de otra parte, se refiere también a la exigencia de que los Ordenamientos Internos establezcan sistemas de control eficaz y de impugnación de todas las fases en que se estructure la aplicación de la medida, es decir, en la fase inicial de su adopción, en la intermedia de ejecución y en la posterior de incorporación de lo obtenido como prueba al procedimiento penal abierto al efecto.

En lo que se refiere a la primera de estas condiciones o garantías mínimas que debe reunir la Ley habilitante de la limitación del derecho aparecen especificadas con toda claridad en la doctrina del TEDH. Así, por citar las que han afectado a nuestro País, las SSTEDH de 30 de julio de 1998, caso VALENZUELA CONTRERAS, y de 18 de febrero de 2003, caso PRADO BUGALLO, destacan las siguientes:

> «La definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial; la naturaleza de las infracciones a que puedan dar lugar; la fijación de un límite a la duración de la ejecución de la medida; las condiciones de establecimiento de los atestados que consignen las conversaciones interceptadas; las precauciones que se deben tomar para comunicar, intactas y completas, las grabaciones realizadas, con el fin de ser controladas eventualmente por el Juez y la defensa; las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de dichas cintas, sobre todo tras un sobreseimiento o una absolución».

---

*condiciones en que autoriza a los Poderes públicos a recurrir a una injerencia así***,** secreta y posiblemente peligrosa, en el derecho al respeto de la vida privada y de la correspondencia». Como veremos más adelante la STEDH de 18 de febrero de 2003, caso PRADO BURGALLO contra España, precisamente estima la vulneración del derecho del art. 8.1º del CEDH porque, como indica la STC 184/2003, «el actual art. 579 LECrim no cumple con las exigencias requeridas por dicho precepto relativas a la previsión legal de la injerencia».

Pues bien, llegados a este punto, hay que poner esta doctrina en relación con el Ordenamiento Jurídico español que regula el régimen de las intervenciones de los diferentes modos de comunicación porque, a mi entender, es aquí dónde se encuentra el verdadero «talón de Aquiles» de nuestro sistema jurídico en lo que se refiere a la limitación del derecho fundamental del art. 18.3 CE. El notable cúmulo de carencias normativas ya ha sido puesto de manifiesto por el TC en su STC 184/2003 (FJ 5) al haber declarado textualmente que: «el art. 579 LECrim adolece de vaguedad e indeterminación en aspectos esenciales, por lo que no satisface los requisitos necesarios exigidos por el art. 18.3 CE para la protección del derecho al secreto de las comunicaciones, interpretado, como establece el art. 10.2 CE, de acuerdo con el art. 8.1 y 2 CEDH».

De esta manera, haciéndose, eco de lo que ya mencionó en otra anterior, la STC 49/1999[45], ha destacado que las exigencias que debe reunir la regulación legal del régimen de las intervención de las comunicaciones se concretan en: La definición de las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; la descripción regulada del procedimiento de trascripción de las conversaciones interceptadas; las precauciones a observar, para comunicar intactas y completas las grabaciones realizadas a los fines de control eventual por el Juez y por la defensa y las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad.

Frente a ello, como destaca de manera textual la primera de las Sentencias citadas, en referencia al artículo 579 LECrim, «… resulta la insuficiencia de su regulación sobre el plazo máximo de duración de las intervenciones, puesto que no existe un límite de las prórrogas que se pueden acordar; la delimitación de la naturaleza y gravedad de los hechos en virtud de cuya investigación pueden acordarse; el control del resultado de las intervenciones telefónicas y de los soportes en los que conste dicho resultado, es decir, las condiciones de grabación, y custodia, utilización y borrado de las grabaciones, y las condiciones de incorporación a los atestados y al proceso de las conversaciones intervenidas». A lo que añade que «el art. 579 LECrim no es por sí mismo

[45] Sobre esta sentencia pueden ser consultados, entre otros, los siguientes estudios: ETXEBERRIA GURIDI, F., «La previsión legal y las diligencias de investigación restrictivas de derechos fundamentales (a propósito de la STC. 49/1999, de 5 de abril)», *Revista La Ley*, Jurisprudencia, T. 6, 1999, pp. 1717 y ss.; y NARVÁEZ RODRÍGUEZ, A., «Intervenciones telefónicas: Comentarios a la STC. 49/99, de 5 de abril», *Repertorio Aranzadi del Tribunal Constitucional*, T. II, 1999, pp. 1757 y ss.

norma de cobertura adecuada, atendiendo a las garantías de certeza y seguridad jurídica, para la restricción del derecho fundamental al secreto de las comunicaciones telefónicas (art. 18.3 CE)».

Y, por si ello no bastara para afirmar la insuficiente regulación de la medida limitativa, añade:

> «tampoco regula expresamente y, por tanto, con la precisión requerida por las exigencias de previsibilidad de la injerencia en un derecho fundamental las condiciones de grabación, custodia y utilización frente a ellos en el proceso penal como prueba de las conversaciones grabadas de los destinatarios de la comunicación intervenida, pues el art. 579 LECrim sólo habilita específicamente para afectar el derecho al secreto de las comunicaciones de las personas sobre las que existan indicios de responsabilidad criminal en el momento de acordar la intervención de las comunicaciones telefónicas de las que sean titulares o de las que se sirvan para realizar sus fines delictivos, pero no habilita expresamente la afectación del derecho al secreto de las comunicaciones de los terceros con quienes aquéllos se comunican. A estos efectos resulta conveniente señalar que al legislador corresponde ponderar la proporcionalidad de la exclusión, o inclusión, y en su caso bajo qué requisitos, de círculos determinados de personas en atención a la eventual afección de otros derechos fundamentales o bienes constitucionales concurrentes al intervenirse sus comunicaciones, o las de otros con quienes se comunican, como en el caso de Abogados o profesionales de la información el derecho al secreto profesional (arts. 24.2, párrafo 2, y 20.1.d CE), o en el caso de Diputados o Senadores el derecho al ejercicio de su cargo de representación política (art. 23.2 CE), su inmunidad parlamentaria y la prohibición de ser inculpados o procesados sin previa autorización de la Cámara respectiva (art. 71.2 CE)».

Como puede observarse de lo expuesto, el primero de los presupuestos que exigen, tanto el Convenio de Roma como la doctrina del TEDH en relación con la limitación de este derecho fundamental, no se cumple debidamente, a pesar de que, por vía jurisprudencial, se hayan tratado de superar las graves deficiencias legislativas que arrastra nuestra normativa procesal, pero que no garantizan con criterios de legalidad y de seguridad jurídica la aplicación de la misma.

A todas las graves deficiencias legales advertidas por el TC en su jurisprudencia habría que añadir algunas que también deben quedar incorporadas legislativamente para garantizar un mínimo de seguridad jurídica en la aplicación de la medida limitativa. Me refiero, en concreto, al hecho de que se aprecie también un notable vacío legal en lo que se refiere a la naturaleza jurídica y la entidad de los hechos punibles en los que sea posible la intervención telefónica, es decir de aquellos delitos

que, por su gravedad o trascendencia social, justifiquen razonadamente la adopción de la medida para su investigación; que no se establezca tampoco ninguna previsión legal sobre los denominados «descubrimientos casuales», es decir, aquellos no previstos en el momento de autorizarse la limitación del derecho, pero que se pueden producir en el transcurso de su ejecución; tampoco se detalla cómo debe articularse el procedimiento de la práctica y, sobre todo, el control *a posteriori* de las grabaciones obtenidas, en la línea de lo que ha establecido el Tribunal en las dos Sentencias reseñadas y, finalmente, el problema de la destrucción de aquellas grabaciones de conversaciones telefónicas sobre las que se haya articulado una prueba declarada posteriormente nula al amparo del art. 11.1 de la LOPJ. o, simplemente, porque el procedimiento penal haya sido archivado o sobreseído.

Como se ve, hay tal cantidad de aspectos de sustancial relevancia que para nada están previstos en la ley y que nuestro TC ha tenido que suplir con una jurisprudencia[46], apoyada en la doctrina del TEDH, que, pone de manifiesto una vez sí y otra también la deficiente normativa cada vez más necesitada de una novedosa, que no reformada, legislación orgánica que regule toda la materia de medidas cautelares y diligencias de investigación que puedan quedar incorporadas como

---

[46] Resulta significativo en este sentido el texto del FJ 6 c) de la STC 184/2003, donde el Tribunal trata de suplir la insuficiencia legislativa con el desarrollo de una jurisprudencia apoyada en la doctrina del TEDH y afirma: «si en el tiempo en que se llevaron a cabo las intervenciones telefónicas denunciadas la cobertura legal era insuficiente desde la perspectiva del art. 18.3 CE, hemos de reconocer, al igual que hicimos en la STC 49/1999, de 5 de abril, F. 5, que "la situación del Ordenamiento jurídico español, puesta de manifiesto en la concreta actuación que aquí se examina, y sufrida por los recurrentes, ha de estimarse contraria a lo dispuesto en el art. 18.3 CE". Pero, ahora como entonces, debemos aclarar "el alcance de la estimación de tal vulneración", pues, si bien "estamos en presencia de una vulneración del art. 18.3 CE, autónoma e independiente de cualquier otra: la insuficiencia de la Ley, que sólo el legislador puede remediar y que constituye, por sí sola, una vulneración del derecho fundamental", *para que dicha vulneración pueda tener efectos sobre las resoluciones judiciales impugnadas en amparo es preciso, en primer lugar, que la actuación de los órganos judiciales, que autorizaron las intervenciones, haya sido constitucionalmente ilegítima; esto es, que a ellas sea imputable de forma directa e inmediata la vulneración del derecho fundamental* (art. 44.1.b LOTC). Y a estos efectos, *"si, pese a la inexistencia de una Ley que satisficiera las genéricas exigencias constitucionales de seguridad jurídica, los órganos judiciales, a los que el art. 18.3 de la Constitución se remite, hubieran actuado en el marco de la investigación de una infracción grave, para la que de modo patente hubiera sido necesaria, adecuada y proporcionada la intervención telefónica y la hubiesen acordado respecto de personas presuntamente implicadas en el mismo, respetando, además, las exigencias constitucionales dimanantes del principio de proporcionalidad, no cabría entender que el Juez hubiese vulnerado, por la sola ausencia de dicha Ley, el derecho al secreto de las comunicaciones telefónicas"*» (STC 49/1999, de 5 de abril, FJ 5; «mutatis mutandis» STC 47/2000, de 17 de febrero, FJ 5).

prueba preconstituida al plenario. La LECrim, como en tantas otras ocasiones, no cumple las exigencias de previsibilidad y certeza que impone la interpretación de las garantías propias de la limitación de este derecho, en sintonía con lo que dispone el CEDH. En todo caso, hay que tener en cuenta que la STC 26/2006, (FJ 5) ha señalado al respecto que «no puede afirmarse, en el momento actual, que el Derecho interno no respete las exigencias derivadas del art. 8 CEDH, sino que a este Tribunal le corresponde suplir las insuficiencias apreciadas en el precepto legal citado hasta que se produzca la necesaria intervención del legislador… Conforme señala el art. 5.1 LOPJ, las resoluciones de este Tribunal en todo tipo de procesos vinculan a todos los Jueces y Tribunales, quienes han de interpretar y aplicar las leyes y reglamentos según los preceptos y principios constitucionales interpretados por este Tribunal».

Desde luego, la advertencia formal que el TC hace al legislador reclamando, de una vez por todas, la aprobación de una norma procesal que, a semejanza de otras que desde hace ya años tutelan la actuación de los Tribunales de otros países de nuestro entorno[47], debieran acrecentar la

---

[47] Piénsese que, sobre este extremo, y a nivel del Derecho Comparado la normativa de los países más próximos a nuestro entorno y de mayor influencia en el ordenamiento procesal español establecen una pormenorizada regulación de un medio de investigación como el que estudiamos.

Por exponer algunos ejemplos, pueden citarse, entre otros, la regulación contenida en la *Ordenanza Procesal Alemana*, la StPO de 7 de enero de 1975, en cuyos § 100 a) y b) se establece que el control y grabación de las conversaciones telefónicas puede adoptarse, tanto por el Juez como, en caso de peligro de retraso por el Fiscal (aunque supeditado a la ulterior aprobación judicial en el plazo de tres días), cuando concurran los siguientes presupuestos:

—La comisión de determinados hechos que puedan fundar la sospecha de que alguien, como autor o partícipe, ha cometido algunos de los delitos muy graves que aparecen especificados taxativamente en el § 100 a) (hechos punibles contra la defensa del Estado, orden público, falsificación de moneda, contra la vida, libertad personal, robo, etc.).

—Se establece, además, la indispensabilidad de la medida, esto es que dicha medida tendrá carácter subsidiario de tal manera que no podrá ser utilizada si existen otros medios de investigación alternativos para llegar al descubrimiento del hecho delictivo.

—Se dispone cuál ha de ser el contenido de la autorización debiéndose describir los datos identificativos del interesado contra el que se dirija, la clase, extensión y duración de la medida (con un plazo máximo de tres meses, susceptible de prórroga por semejante período y de cesar ya los presupuestos que determinaron su adopción, el cese inmediato de la intervención).

La introducción posterior en el proceso de dicho material, no regulado por la Ley ha sido explicada, como nos indica GÓMEZ COLOMER, J. L., *El proceso penal alemán, introducción y normas básicas.* Editorial Bosch, Barcelona, 1985, pp. 123 y ss., por la Jurisprudencia (SBGH de 3 de mayo de 1977), en el sentido de que, o bien se reproduce la cinta magnetofónica ante el Juez, como medio de prueba de inspección ocular, o bien se transcribe su contenido y se introduce como prueba documental.

sensibilidad del Parlamento Español hacia estos temas, so pena de que por falta de cobertura legal, llegue un momento en que, con fundamento en el derecho al secreto de las comunicaciones, conectado con el derecho a un proceso con todas las garantías, no puedan llevarse a efecto por estar viciadas de nulidad al no encontrar suficiente apoyo legal.

También, el *Código de Procedimiento Penal italiano*, aprobado por Decreto del Presidente de la República de 22 de septiembre de 1988, dedica, dentro del Título destinado a los medios de investigación, todo el capítulo IV (arts. 266 a 271) a la *intervención de conversaciones y comunicaciones*. La prolífica como detallada regulación italiana, destaca, por un lado los delitos que en catálogo cerrado son susceptibles de investigación mediante esta medida (delitos muy graves o graves castigados con penas superiores en el máximo a cinco años, también los de tráfico de estupefacientes, contrabando, tráfico de armas y explosivos, injurias, amenazas o perturbaciones en las personas cometidos por el teléfono, etc.), determina, igualmente, los presupuestos en los que es posible su utilización, encomendando al Juez de garantías (esto es el de las investigaciones preliminares), siempre a petición del Fiscal, la autorización necesaria, aunque también el propio Fiscal en caso de urgencia puede autorizar la intervención (aunque entonces debe comunicarlo al Juez en el plazo máximo de veinticuatro horas, para que en otro término de cuarenta y ocho horas convalide la autorización inicial), establece un procedimiento detallado, tanto de la grabación de las conversaciones, como de la trascripción en acta de las mismas, su conservación, y su ulterior comunicación a las defensas de los inculpados, una vez finalizadas las operaciones correspondientes, del contenido de las mismas; su audiencia por el juez, así como la posterior selección de aquellas conversaciones que se consideren relevantes a los efectos de la investigación, debiendo oírse sobre dicha selección, tanto al Fiscal como a las partes, a las que ha de entregárseles, además, una copia de las transcripciones y una reproducción de las grabaciones efectuadas. Por último, se completa la regulación con la normativa destinada a la conservación hasta el momento de haber recaído sentencia firme del material probatorio seleccionado.

Finalmente, en el *Derecho Francés*, la Ley 91-646, de 10 de julio, que aprobó el Código de Procedimiento Penal, establece, también, una regulación detallada sobre la limitación del derecho a la libre comunicación. En concreto el art. 100 del mismo, contempla que la medida sólo podrá acordarse para delitos castigados con pena igual o superior a dos años de prisión, debiendo acordar el Juez de Instrucción, por escrito, la orden de intervención, que no tiene carácter jurisdiccional ni tampoco es recurrible. En dicha orden deben constar todos los elementos de identificación de la conexión a intervenir, el delito que motiva la intervención y el tiempo de duración de la medida que será como máximo de cuatro meses, pudiendo quedar prorrogada la aplicación de la medida en las mismas condiciones de forma y duración.

Además, el Juez de Instrucción o el oficial de policía nombrado por él deberá levantar acta de cada una de las operaciones de intervención y de registro que se realicen, con mención de la fecha y hora en que la operación comience y termine. Finalmente, por lo que atañe a las escuchas telefónicas grabadas, dispone que las cintas que las contengan serán destruidas a instancia del Fiscal de la República o del Fiscal del Tribunal de casación, al vencer el plazo de prescripción de la acción pública, levantándose acta de dicha destrucción. Finalmente, se prohíbe la instalación de escuchas en las líneas telefónicas de los Diputados o Senadores, así como de las instaladas en los despachos de abogados, sin que el Presidente de la Asamblea correspondiente o el Decano, en su caso, del Colegio de Abogados sea informado previamente por el Juez de Instrucción, bajo pena de nulidad.

Como puede advertirse, en los tres sistemas procesales las exigencias del art. 8 del CEDH. son ampliamente respetadas y cumplidas.

Para concluir el estudio de este primer requisito de previsión legal, restaría por analizar la última exigencia que se deriva de la interpretación que ha hecho el TEDH de los términos del Convenio de Roma, es decir el de la necesidad de que la ejecución de las medidas no quede sujeta a la mera arbitrariedad de las autoridades públicas y que, además, se introduzcan recursos efectivos en el Derecho interno para impugnar las que hayan podido resultar contrarias a los términos del Convenio[48].

Aunque más adelante, a la hora de estudiar las fases de que se compone la intervención de las comunicaciones, nos referiremos detalladamente a esta exigencia importante señalada por la doctrina del Tribunal Europeo, ya podemos anticipar que tampoco en este punto resulta suficientemente cubierto el requisito de la previsión legislativa, y, desde luego, ha tenido que ser primero la doctrina, más tarde la Jurisprudencia, tanto del TC[49]

---

[48] Son significativos los términos en los que se emplea el TEDH en la Sentencia de 25 de marzo de 1998, caso KOPP contra Suiza en donde recuerda que «el artículo 8.2. exige que la ley sea compatible con la preeminencia del derecho: Cuando se trata de medidas secretas de vigilancia o de interceptación de comunicaciones por las autoridades públicas, la ausencia de control público y el riesgo de abuso de poder implican que el derecho interno debe ofrecer al individuo una cierta protección contra las injerencias arbitrarias en los derechos garantizados por el art. 8». En el mismo sentido se manifiesta, también la STEDH de 25 de junio de 1997, caso HALFORD contra el Reino Unido.

[49] Pueden citarse en este sentido las SSTC 85/94, 86/95, 49/96, 121/98, 151/98, 49/99, 166/99 y 167/2002 entre otras.

En particular, la STC 166/99, declara que «la intervención de las comunicaciones telefónicas puede constituir una vulneración del derecho al secreto de las comunicaciones si no se respetan las garantías constitucionales a él inherentes en alguna de las fases diferenciables en el curso de la misma: en primer lugar, en la decisión de intervención, en segundo lugar, en su ejecución policial, y, en tercer lugar, en el control judicial de la ejecución:

a) *La decisión de intervención* puede ser ilegítima, en primer término, por no haber sido adoptada por órgano judicial (STC 86/95); en segundo lugar, por inexistencia de los presupuestos materiales que habilitan legal y constitucionalmente para la adopción de la decisión judicial de intervención, cuya ausencia convierte a la medida en desproporcionada. "Pues, de una parte, mal puede estimarse realizado ese juicio, en el momento de adopción de la medida, si no se manifiesta, al menos, que concurre efectivamente el presupuesto que la legitima. Y, de otra, sólo a través de esa expresión, podrá comprobarse ulteriormente la idoneidad y necesidad (en definitiva, la razonabilidad) de la medida limitativa del derecho fundamental (SSTC 37/89, 3/92, 12/94, 13/94, 52/95, 128/95, 181/95, 34/96 y 49/99). Estos presupuestos… residen en la existencia de una investigación en curso por un hecho constitutivo de infracción punible grave, en atención al bien jurídico protegido y a la relevancia social del mismo, y en la existencia de indicios sobre el hecho constitutivo de delito y sobre la conexión con el mismo de las personas investigadas.

En tercer lugar, afecta a la legitimidad de la decisión la falta de necesidad estricta de la medida; es decir, puede ser constitucionalmente ilegítima, dado su carácter prescindible, bien porque los conocimientos que pueden ser obtenidos carecen de relevancia respecto de la investigación del hecho delictivo o respecto de la conexión de las personas investiga-

como del TS[50], y finalmente la propia Fiscalía General del Estado[51], las que, con inspiración en las tesis seguidas por el TEDH, han tenido que suplir las deficiencias legales sobre este extremo.

B) Fines legítimos

Bajo esta terminología engloba el art. 8.2. del CEDH un conjunto de finalidades que legitiman las injerencias de toda índole en el derecho al secreto de las comunicaciones.

En el ámbito del Derecho Español, la Jurisprudencia, que no el art. 579 de la LECrim, es la que se ha encargado de incorporar al sistema jurídico esta exigencia del Convenio Europeo, utilizando para ello la regla de la proporcionalidad. Así, por ejemplo, la STC 261/2005 (FJ 2) destaca: «en relación a este principio, la medida autorizada tiene que ser necesaria para alcanzar un fin constitucionalmente legítimo. La desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a su enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que la Constitución garantiza», agregando a lo

---

das, o bien porque pudieran obtenerse a través de otras medidas menos gravosas de los derechos fundamentales en litigio (SSTC 54/96 y 49/99).

Por último, incide en la legitimidad de la medida la falta de expresión o exteriorización, tanto de la existencia de los presupuestos materiales de la intervención -investigación, delito grave, conexión de las personas con los hechos- como de la necesidad y adecuación de la medida, razones y finalidad perseguida (STC 54/96), y todo ello es exigible, asimismo, respecto de las decisiones de mantenimiento de la medida, en cuyo caso, además, deben ponderarse las concretas circunstancias concurrentes en cada momento y el conocimiento adquirido a través de la ejecución de la medida inicialmente prevista (SSTC 181/95 y 49/99).

b) *La ejecución policial* puede resultar constitucionalmente ilegítima en la medida en que se verifique al margen de la cobertura judicial de la misma, es decir excediéndose de los límites temporales —se mantiene la intervención más tiempo del habilitado—, personales —se investigan personas distintas de las autorizadas— materiales —hechos diferentes—, u otros que constituyan condiciones judicialmente impuestas de la autorización (SSTC 85/94, 86/95, 49/96 y 121/98).

c) *El control judicial* puede resultar ausente o deficiente en caso de falta de fijación judicial de los períodos en los que debe darse cuenta al juez de los resultados de la restricción, así como en caso de su incumplimiento por la Policía; igualmente, queda afectada la constitucionalidad de la medida si, por otras razones, el Juez no efectúa un seguimiento de las vicisitudes del desarrollo y cese de la intervención telefónica, y si no conoce el resultado obtenido en la investigación (STC 49/99)».

[50] Por citar de las más recientes, destacaremos las SSTS de 26 de mayo de 1997 (RJ 4133), 15 de octubre de 1998 (RJ 9212), 18 de febrero y 11 de marzo de 1999 (RJ 1920 y 2097) y 16 y 26 de febrero, 3 de marzo y 18 de abril de 2000 (RJ 2082, 2094, 1109 y 2561).

[51] La Circular 1/99, de 29 de diciembre de la Fiscalía General del Estado se hace eco, precisamente, de toda la doctrina ahora expuesta.

expuesto que «… esta intervención puede ser constitucionalmente ilegítima cuando no es imprescindible, bien porque los conocimientos que pueden ser obtenidos carecen de relevancia respecto de la investigación en curso o bien porque pudieran obtenerse a través de otras medidas menos gravosas de los derechos fundamentales».[52]

Es evidente que en el marco del proceso penal, la única razón que puede justificar la adopción de esta medida limitativa del derecho fundamental es la de la existencia de un fin constitucionalmente legítimo como es el que representa el interés general que subyace en el descubrimiento del delito y en la determinación de sus partícipes. Pero en todo caso y para que esté justificada la restricción de la medida con los criterios de proporcionalidad que posteriormente estudiaremos, sólo puede justificarse desde el mandato contenido en el art. 8.2 CEDH, la injerencia en el derecho fundamental para la investigación de aquellos delitos que, por su gravedad o trascendencia social, justifiquen razonadamente el sacrificio que supone la limitación del derecho.

El problema está en que, como ya hemos anticipado, nuestra legislación no establece un catálogo de delitos o de penas en los que sería posible acordar la intervención, aunque la jurisprudencia, sobre todo a partir del conocido ATS de 18 de junio de 1992, ha reconocido la procedencia de la medida tanto en la investigación de los delitos graves[53], como en aquellos menos graves que revistan trascendencia social. La cuestión, por tanto, se localiza en que, a falta de una normativa legal al respecto, la inseguridad jurídica causada por la falta de previsión legal puede generar notables problemas con su adecuación a los términos del art. 8.2 del CEDH.

C) Medida necesaria en una sociedad democrática

Es el último pero no por ello el menos importante de los requisitos que ha destacado la doctrina del TEDH cuando le es sometido a su conocimiento una denuncia del art. 8 del Convenio[54].

---

[52] En el mismo sentido las SSTC 166/1999 (FJ 3) y 126/2000 (FJ 6).

[53] SSTC 166/1999, FJ 1 y 2; 171/1999, FJ 5; 126/2000, FJ 2; 299/2000, FJ 2; 14/2001, FJ 2, 138/2001, FJ 3, y 202/2001. Entre las sentencias del TS más recientes podemos señalar las SSTS. de 7 de diciembre de 2004 (RJ 469 de 2005) y 13 de abril y 7 de septiembre de 2005 (RJ 5182 y 6827).

[54] En el caso Klass y otros contra Alemania, el TEDH señalaba que «las sociedades democráticas se encuentran amenazadas en nuestros días por formas muy complejas de espionaje y por el terrorismo, de suerte que el Estado debe ser capaz, para combatir eficazmente estas amenazas, de vigilar en secreto los elementos subversivos que operan en su territorio. El Tribunal debe, pues, admitir que la existencia de disposiciones legislativas

A este respecto y para adentrarnos más adelante en la asimilación de su doctrina por el TC español, el TEDH en el caso MALONE advertía ya del peligro que puede comportar la utilización abusiva de tales medidas restrictivas del derecho fundamental por parte de las autoridades públicas, si se dejare a la libre discrecionalidad de aquéllas su adopción. De ahí que en su STEDH de 25 de marzo de 1983, caso SILVER contra el Reino Unido, el Tribunal indicara ya, con carácter general, un conjunto de principios sobre los que puede construirse la idea de «necesidad» a que se refiere el art. 8.2 del Convenio. Tales principios son los siguientes:

1.º En primer lugar, los términos «necesario en una sociedad democrática» no son sinónimos de indispensable, ni tampoco tiene la flexibilidad de términos como admisible, normal, útil, razonable u oportuno.
2.º En segundo término, el Convenio permite a los Estados signatarios un cierto margen de apreciación, aunque limitado, a la hora de establecer restricciones al derecho fundamental, pero la resolución final sobre la compatibilidad y adecuación de las normativas internas de dichos Estados al Convenio corresponde al Tribunal.
3.º En tercer lugar, los artículo del Convenio que establecen una excepción al derecho garantizado deben ser interpretados restrictivamente.
4.º En todo caso, para que legalmente sea posible la injerencia en el derecho fundamental que estudiamos tiene que ser posible su control.
5.º Finalmente, el que considero que es el principio que aglutina a todos los anteriores, «necesario en una sociedad democrática», significa que la intervención debe corresponder especialmente a una necesidad social imperiosa y resultar proporcionada a la finalidad legítima perseguida.

La idea de «necesidad», pues, que utiliza el art. 8.2 ha resultado interpretada por el TEDH poniéndola en relación con el criterio de la proporcionalidad[55], de tal manera que la autoridad pública que acuerde

---

acordando los poderes de vigilancia secreta de la correspondencia, de los envíos postales y de las telecomunicaciones son, ante una situación excepcional, necesarias en una sociedad democrática y/o en la defensa del orden y en la prevención de infracciones penales». (Ap. 48, STEDH de 6 de septiembre de 1978).

[55] En la STEDH de 20 de junio de 1988, caso SHÖNENBERGER y DURMAZ contra Suiza, el Tribunal destacaba textualmente que «para revestir un carácter necesario en una sociedad democrática, una injerencia debe basarse sobre una necesidad social imperiosa y especialmente ser proporcionada a la finalidad legítima perseguida…».

la medida restrictiva del derecho fundamental deberá adoptarla siempre que repute proporcionado al sacrificio del derecho fundamental consagrado en el art. 8, la obtención del superior fin legítimo que, en el caso del proceso penal, será el interés general en la averiguación del delito y en la identificación de sus autores. Lógicamente esta decisión de la Autoridad no puede reputarse en términos voluntaristas porque incurriría en la arbitrariedad que se encuentra también prohibida por el Convenio de Roma, por resultar contraria a las necesidades propias de una sociedad democrática. De ahí que la decisión de la autoridad deba explicitarse por escrito y además justificarse razonadamente por qué es adoptada y en base a qué aquélla reputa proporcionada la medida. Surge así, pues, el requisito de la motivación, que se erige en pieza angular sobre la que debe pivotar todo el proceso de decisión previa relativo a la adopción de la medida restrictiva.

Las ideas de motivación y proporcionalidad aparecen, por consiguiente, parejas y conectadas entre sí y corresponderá a la Autoridad Pública competente para acordarla el tomar una decisión fundada en los fines legítimos que postula el art. 8.2 del Convenio y con estricta observancia de tales requisitos de motivación y proporcionalidad, que son los que han servido de pilares para la elaboración de la doctrina del TC sobre los requisitos exigidos para la limitación del derecho fundamental que estudiamos.

3. *Requisitos*

La importancia de la determinación de los requisitos que, conforme a la doctrina del TEDH que hemos comentado anteriormente, ha establecido el TC para la debida limitación del derecho al secreto de las comunicaciones, radica no tanto en que la vulneración de este derecho fundamental supone en sí misma la quiebra de la debida observancia de un derecho de alcance constitucional por parte de los poderes públicos, sino que, además, como es bien sabido, si tal vulneración se produce en el marco del proceso penal, aparecerá íntimamente conectada con el derecho fundamental a un proceso con todas las garantías, esto es al proceso justo y equitativo en los términos en que se manifiesta el art. 6 CEDH, y puede acarrear como consecuencia ineludible la vulneración del derecho a la presunción de inocencia si el pronunciamiento condenatorio se apoyó exclusivamente en aquella diligencia de investigación obtenida de la limitación del derecho y convertida en una prueba preconstituida ilícita, así como de todas aquellas otras derivadas que estuvieran en íntima conexión con aquella, en cuanto vulneradora de derechos fundamentales.

Por todo ello, la doctrina del TC ha establecido todo un cuerpo de doctrina que determina el ámbito en que es susceptible de limitación el derecho al secreto de las comunicaciones. Hay que tener en cuenta, a este respecto, que la doctrina constitucional distingue, con un criterio cronológico, tres fases en la limitación de este derecho:

1.ª Una fase antecedente a la limitación del derecho, que se hace pivotar en torno a la necesaria intervención del Juez de Instrucción que autorice mediante resolución motivada la aplicación de la medida limitativa.
2.ª Una segunda fase que coincide con la ejecución de la medida limitativa del derecho y en la que también se establecen un conjunto de requisitos esenciales, tendentes básicamente a garantizar la regularidad del procedimiento.
3.ª Y, finalmente, una tercera fase de control judicial de la fuente de prueba obtenida, que el TC asocia propiamente al derecho a un proceso con todas las garantías y no al derecho fundamental que estamos estudiando.

Veamos, pues, cada una de las fases por separado y poniéndolas en relación con los requisitos esenciales que exige la doctrina constitucional en cada una de ellas.

A) Fase previa a la ejecución: La autorización judicial

Hay que comenzar el estudio de esta primera fase con una obviedad que, sin embargo, resulta relevante a la hora de establecer la doctrina constitucional al respecto. Que compete en exclusiva al órgano judicial la resolución que limite este derecho fundamental, de tal modo que al hablar de autorización judicial hay que referirla a la idea de que la autoridad administrativa que actúe en este ámbito no tendrá ninguna otra atribución que la de la mera ejecución material de la intervención de la comunicación, pero sin que disponga de potestad alguna para ejecutar la limitación en otros términos que no sean los que haya señalado el órgano judicial encargado de la investigación.

Partiendo, pues, de esta premisa la doctrina del TC ha establecido en esta primera fase un conjunto de requisitos que han de ser observados.

a) El cauce procesal adecuado

En primer lugar, la medida limitativa del derecho debe ser realizada en el ámbito de un proceso penal y en el cauce de un procedimiento seguido por delito. No obstante, el Tribunal ha destacado que la posibili-

dad de acordar la medida en el seno de unas diligencias indeterminadas no produce *per se* la vulneración del derecho fundamental, siempre que la resolución judicial motivada que acuerde la limitación del derecho y antes de que se proceda a su ejecución con la puesta en práctica de la intervención, se notifique al Fiscal, por cuanto se entiende que la medida, al haber sido acordada, por razones obvias, sin el pleno conocimiento del imputado que va a ser objeto de la limitación, corresponde al Fiscal en este caso una responsabilidad tuitiva de la protección de los derechos fundamentales de aquél.

En este sentido la STC 126/2000 (FJ 5), recordando la anterior STC 49/1999 (FJ 6), destaca:

> «(…) aunque la naturaleza de la intervención telefónica, su finalidad y la misma lógica de la intervención requieren no solamente que la investigación y su desarrollo se lleven a cabo por el Juez de Instrucción, sino que se realicen dentro de un proceso legalmente existente, el hecho de que la decisión judicial se lleve a cabo en las denominadas "diligencias indeterminadas" no implica, "per se", la vulneración del derecho al secreto de las comunicaciones pues… lo relevante a estos efectos es la posibilidad de control. Tanto el control inicial, pues aun cuando se practiquen en esta fase sin conocimiento del interesado, que no participa en ella, aquél ha de suplirse por la intervención del Ministerio Fiscal, garante de la legalidad y de los derechos de los ciudadanos por lo dispuesto en el art. 124.1 CE, como el posterior (cuando se alza la medida) por el propio interesado que ha de poder conocerla e impugnarla. Por ello, en la citada resolución consideramos que no se había quebrado esa garantía al haberse unido las diligencias indeterminadas, sin solución de continuidad, al proceso incoado en averiguación del delito, "satisfaciendo así las exigencias de control del cese de la medida que, en otro supuesto, se mantendría en un permanente, y por ello inaceptable, secreto"»[56].

---

[56] En el mismo sentido, la STC 205/2002, FJ 5, claramente pone de manifiesto que cuando el Auto acordando la intervención tenga lugar en el seno de unas diligencias indeterminadas, es preceptiva la notificación al Fiscal, al señalar: «La conclusión de que el derecho fundamental del art. 18.3 CE fue lesionado queda reforzada al examinar el Auto que autorizó la intervención, examen que para los afectados tan sólo fue posible una vez comenzado este proceso constitucional y después que fueron halladas las anteriormente extraviadas diligencias indeterminadas núm. 180/1988. Y ello porque, de un lado, se comprueba que dicha resolución se plasmó sobre un modelo estereotipado y que contiene una errónea referencia a la investigación de un delito de tráfico de estupefacientes. Y, de otro lado**,** *no fue notificada al Ministerio Fiscal, lo que impidió el control inicial de la medida* (STC 126/2000, de 16 de mayo, F. 5) en sustitución del interesado, por el garante de los derechos de los ciudadanos (art. 124.1 CE)».

Por tanto, esta primera exigencia puede resumirse en las siguientes notas características. En primer lugar, que la medida ha de ser acordada en el seno de un procedimiento judicial, aunque también lo puede ser en diligencias indeterminadas, siempre que concurra la notificación al Ministerio Fiscal. Y, en segundo término, la notificación al Fiscal es indispensable para que no se produzca la vulneración del derecho, en la medida en que en ese momento aquél es garante de los derechos del imputado, que desconoce la aplicación y ejecución de dicha medida limitativa de su derecho.

De esta doctrina pueden extraerse diversas consecuencias prácticas. En primer lugar, que no podrá apreciarse vulneración alguna del derecho al secreto de las comunicaciones ni tampoco del derecho al proceso con todas las garantías, cuando un Juez de Instrucción en funciones de Juez de Guardia, distinto de aquel que pueda tener a su cargo la instrucción de un proceso, es requerido por la Policía Judicial para acordar una intervención telefónica, aún cuando la autorice en el seno de unas diligencias indeterminadas siempre que sea notificado el Fiscal y que, una vez practicadas las actuaciones correspondientes, sean remitidas aquellas al Juez encargado de la instrucción y sean incorporadas con el resultado de la misma al procedimiento judicial en curso.

En segundo término, entiendo que por los mismos argumentos expuestos tampoco queda afectado ningún derecho fundamental en aquel caso en que, a instancia del Fiscal, un Juzgado de Instrucción acuerde una medida de intervención de las comunicaciones de una persona sometida a investigación en el seno de unas diligencias del artículo 773.2.º LECrim, siempre que ulteriormente dichas diligencias sean remitidas al Juzgado de Instrucción correspondiente, se incoe el oportuno procedimiento penal y pueda darse vista de lo actuado al ya imputado judicialmente. Aún cuando el TC no ha tenido ocasión de abordar de manera frontal y sí sólo tangencial esta problemática las exigencias anteriormente descritas entiendo que habrán sido observadas, en primer lugar, porque ha existido un control judicial, tanto de la adopción como de la ejecución de la medida y, en segundo término, porque todo lo actuado quedará incorporado ulteriormente al proceso judicial correspondiente y con la posibilidad de acceso a todo su contenido por parte del imputado.

La posición de la jurisprudencia del TS relacionada con esta cuestión no ha sido unánime, pues en un caso ha llegado a la conclusión de que no se había producido afectación del derecho fundamental al secreto de las comunicaciones, aunque bien es cierto que con la consideración de que, incluso cuando las intervenciones telefónicas acordadas se hubieran realizado con la vulneración del derecho fundamental invocado, la existencia de otras pruebas de cargo desvinculadas de aquélla, ha-

brían conducido al mismo pronunciamiento condenatorio. No obstante, el órgano judicial primero y el TC más tarde desestimaron la pretensión de los recurrentes de que hubiera existido infracción del derecho fundamental alegado. Así lo entendió la STS de 23 de febrero de 1993 (RJ 1525)[57] que, pese a haberle sido planteada por los recurrentes la eventual vulneración del derecho por haber sido ejecutada la medida limitativa en el seno de unas diligencias de investigación del Fiscal, éstas habían sido acordadas mediante resolución judicial motivada y ulteriormente incorporadas a las Diligencias Previas que fueron incoadas cuando el Fiscal dio término a su investigación y remitió todo lo actuado con el contenido de las grabaciones telefónicas al Juzgado. Interpuesto recurso de amparo contra la misma el TC inadmitió a trámite el recurso por medio de ATC 79/1994[58].

---

[57] Se analizó en esta sentencia una resolución de la Audiencia Provincial de Valencia en el denominado caso CALPE. En síntesis las circunstancias del caso fueron las siguientes: en noviembre de 1989, el Fiscal del TSJ de Valencia solicitó de diversos Juzgados de Instrucción que estaban en funciones de guardia, varias autorizaciones para intervenir diferentes teléfonos; dichas autorizaciones le fueron concedidas por medio de resoluciones judiciales dictadas en el seno de diligencias indeterminadas. Con las citadas autorizaciones fueron realizadas intervenciones telefónicas cuyas cintas que contenían las grabaciones de las conversaciones quedaron incorporadas a las diligencias del Fiscal, que éste, cuando concluyó su investigación, remitió al Juzgado de Guardia, resultando finalmente condenados los acusados por un delito de cohecho en grado de tentativa.

[58] El tema en cuestión no es abordado frontalmente por el TC tal y como lo solicitaban en su demanda los recurrentes, pero de modo implícito, el Tribunal rechaza los planteamientos de aquéllos al decir textualmente en su FJ 2 lo siguiente*:* «Este Tribunal no desconoce (SSTC 108/1984, 176/1988, 245/1991, entre otras) los efectos de la jurisprudencia del T.E.D.H., la cual ha de presidir la interpretación de las normas tuteladoras de los derechos fundamentales (art. 10.2 C.E.). No cabe, sin embargo, apreciar la violación de dicha doctrina, ni de norma alguna de la Constitución, pues no toda irregularidad en el procedimiento de intervención telefónica conlleva la violación del art. 18.3 C.E., sino tan sólo aquellas que supongan una vulneración del derecho fundamental al secreto de las comunicaciones.

Dicha violación no se aprecia en el presente caso, ya que la intervención telefónica se efectuó, como pone de relieve la Sentencia del Tribunal Supremo impugnada, mediante resolución judicial motivada en la que se determinó el hecho punible (muy grave, dado el reproche social de la conducta) causante de la intervención, el número del teléfono intervenido y el destinatario de la intervención telefónica. Se ha observado, pues, lo preceptuado en el art. 18.3 CE.

En cualquier caso, parece obvia la falta absoluta de relevancia del presente recurso de amparo, como se infiere de la argumentación de la Sentencia del Tribunal Supremo (vid. fundamento jurídico undécimo). Efectivamente, la estimación hipotética de lo que se alega al respecto en la demanda no traería como consecuencia la anulación de las Sentencias, condenatoria, de la Audiencia, y desestimatoria, del recurso de casación, en cuanto que el fundamento de la condena viene determinado, no sólo por el resultado de las grabaciones telefónicas sino, y muy especialmente, por la declaración del testigo

Hay que destacar, no obstante, que esta posición no se ha mantenido unánime en la Jurisprudencia, pues justo meses más tarde de la citada sentencia, el TS dictó otra, la de 25 de junio de 1993 (RJ 5244), en que llegó a una solución radicalmente contraria, apoyándose para ello en la afirmación de que la adopción de toda medida limitativa de derechos fundamentales ha de ser acordada por el Juez en el seno de un proceso judicial y, por tanto, las intervenciones telefónicas, que fueron autorizadas en el seno de unas actuaciones como eran las de las diligencias de investigación del Ministerio Fiscal que no constituían un proceso judicial y sin que las denominadas «diligencias indeterminadas» abiertas por el Juzgado de Instrucción que dictó los Autos autorizando las escuchas, tampoco lo fueran[59], constituían una irregularidad motiva-

---

don Javier García Pérez, extremo que subraya la Sentencia de la Audiencia Provincial de Valencia, consignando la fuerza de convicción del testimonio en cuestión. Así pues, aunque las grabaciones telefónicas se reputaran ilícitas en razón de las irregularidades que se afirman, el pronunciamiento condenatorio mantendría su fundamento en el testimonio aludido, sobre cuya valoración no es lícito entrar a través de este recurso, testimonio que, como es evidente, se produce al margen de las grabaciones y con absoluta independencia por lo que no constituiría prueba prohibida alguna, como señala en su fundamento jurídico decimotercero la Sentencia de la Sala Segunda del Tribunal Supremo. En consecuencia, el Tribunal operó con prueba bastante para considerar enervada la presunción que el derecho fundamental ex art. 24.2 C.E. comporta».

[59] El FJ 6 de esta sentencia destaca textualmente lo siguiente*:* «Una de las cuestiones abordadas por el Ministerio Fiscal al desarrollar su motivo plantea la cuestión del ámbito en que debe producirse la interceptación de las comunicaciones telefónicas. Si ha de realizarse en un proceso penal abierto o si, por el contrario, cabe su realización en las Diligencias de Investigación que puede practicar el Ministerio Fiscal con base en el art. 875 bis de la Ley de Enjuiciamiento Criminal y en el art. 5 de su Estatuto Orgánico. La autorización para realizar investigaciones preliminares a la apertura de unas diligencias penales tiene un consistente soporte legal en las disposiciones que acabamos de citar, pero en todo caso deberán ajustarse a las previsiones establecidas por el legislador sin trasvasar sus fronteras ni adentrarse en aspectos acotados para la función judicial. Las facultades concedidas al Ministerio Fiscal pretenden ser una especie de ensayo previo para el caso de que se instaure en un futuro la investigación en manos de la acusación pública, reservando al juez las decisiones que afecten a los derechos y libertades fundamentales de la persona. De momento debemos ajustarnos a los estrictos términos contemplados en la ley que limitan las diligencias a las pertinentes para comprobar un hecho que presente caracteres delictivos, cuando tenga noticia directa o a través de la Policía Judicial de la existencia de conductas presumiblemente incursas en el Código Penal. Las facultades concedidas para llevar adelante estas investigaciones se extienden a la posibilidad de hacer comparecer ante sí a cualquier persona en los términos establecidos para la citación judicial. En el caso presente la iniciativa tomada por el Fiscal Jefe del Tribunal Superior de Justicia estaba sólidamente fundada en una abundante documentación recibida de un organismo de la Administración autonómica. Existía, por tanto, algo más que una inconcreta sospecha y la decisión respondía a una noticia avalada por indicios suficientemente documentados. *Fuera de la posibilidad de obligar a comparecer a determinadas personas todas las medidas restric-*

dora de la nulidad. Desde luego, el argumento empleado no deja de ser meramente formal, pues lo importante no es en sí el procedimiento en que haya de acordarse la medida limitativa del derecho, sino entiendo que se producirá la vulneración cuando la ejecución de la medida judicialmente acordada escape al control del Juez que la autorizó y cuando quién la padezca caiga en indefensión, es decir, cuando no pueda articular mecanismos de defensa contra ella mediante el conocimiento de la información que se haya obtenido con la limitación del derecho y con la posibilidad efectiva de contradecirla. Si ulteriormente, todo el material obtenido se incorpora al procedimiento judicial y además se da conocimiento del mismo al imputado, ninguna irregularidad con alcance constitucional se habrá producido. En todo caso, el tema está abierto a la discusión doctrinal y al análisis en profundidad por la doctrina del TC.

b) La motivación

En segundo término, es requisito imprescindible que la autorización se opere mediante una resolución judicial motivada.

Sin duda, ha sido la doctrina del TC la que en nuestro país ha marcado las pautas por las que ha de conducirse esta exigencia que encuentra su apoyo en los arts. 18.3, 24.1 y 120 de la CE.

Sobre este fundamental requisito el TC se ha pronunciado reiteradamente[60] afirmando que «toda resolución que limite o restrinja el ejerci-

---

tivas de derechos fundamentales deben solicitarse de la autoridad judicial que no podrá acordarlas si no pone en marcha, previamente, unas diligencias judiciales de investigación criminal. El párrafo último del art. 785 bis de la Ley de Enjuiciamiento Criminal pone de relieve la incompatibilidad de una investigación simultánea del Ministerio Fiscal y del Juez al establecer la cesación de las diligencias preliminares en cuanto exista un procedimiento judicial sobre los mismos hechos. De lo anteriormente expuesto se llega a la conclusión de que *el Ministerio Fiscal agota las posibilidades de investigación preliminar en el momento en que se dirige a la autoridad judicial o al órgano instructor para que adopte medidas de limitación de los derechos fundamentales poniendo en su conocimiento la existencia de unos hechos que presentan caracteres delictivos. Desde ese momento las facultades de investigación se traspasan al juez instructor que no puede ser otro que aquel que recibe la noticia del hecho criminal* y siempre que se cumplan los requisitos de competencia territorial y objetiva previstos en la Ley de Enjuiciamiento Criminal. No puede admitirse, como sucede en el caso que examinamos, que hasta cuatro juzgados de instrucción hayan intervenido durante la tramitación de las Diligencias de Investigación llevadas a cabo por el Ministerio Fiscal. La decisión de intervenir el teléfono debió solicitarse al juzgado al que por turno correspondiera vinculando este órgano jurisdiccional a la tramitación de las Diligencias previas o sumariales que debió incoar como consecuencia de la denuncia recibida y como cobertura de la interferencia en los derechos fundamentales de la persona».

[60] SSTC 26/81, 62/82, 85/94, 13/85, 86/95, 181/95, 54/96, 207/96, 123/97, 181/98, 184/98, 185/98 y 49/99 y 171/99, entre otras muchas.

cio de un derecho fundamental ha de estar motivada, de forma tal que la decisión determinante pueda ser conocida por el afectado. De otro modo, se infringe el derecho a la tutela judicial efectiva de los Jueces y Tribunales en el ejercicio de los derechos, ya que se afectaría al ejercicio del derecho a un proceso público por una resolución no fundada en Derecho, dificultando con ello gravemente las posibilidades de defensa en la vía ordinaria, en su caso, y en último extremo por la vía del recurso de amparo» (STC 85/94).

Más específicamente y en relación con el derecho al secreto de las comunicaciones, el TC, en su STC 259/2005 (FJ 2) ha destacado con claridad que «la resolución judicial en la que se acuerda la medida de intervención telefónica o su prórroga debe expresar o exteriorizar las razones fácticas y jurídicas que apoyan la necesidad de la intervención», por cuanto en estos casos, la exigencia constitucional no deriva únicamente de la tutela que han de deparar los tribunales al justiciable sino que la misma queda embebida por el derecho fundamental de naturaleza sustantiva, que es el realmente lesionado, en este caso el derecho al secreto.

Pues bien, las exigencias de motivación han sido descritas con detalle y reiteración por la doctrina del TC. Así, para que un Auto que acuerde la intervención telefónica se entienda que está suficientemente motivado, debe reunir los siguientes requisitos:

1.º En primer lugar, la resolución judicial ha de expresarse en términos concretos, es decir el auto que decrete la intervención deberá precisar claramente cuál es el objeto y la finalidad de la medida, así como el sujeto o los sujetos afectados, los números de teléfono o del medio de comunicación de que se trate y su duración. En definitiva, se trata de obligar al órgano jurisdiccional a que concrete, por razones de seguridad jurídica, cuáles han de ser los límites de la intervención.

2.º En segundo término, el Auto debe expresar por qué el Juez considera verdaderamente necesaria dicha intervención. Hay que tener en cuenta que nos hallamos ante una medida excepcional, en cuanto limitativa de un derecho fundamental, por lo que su utilización únicamente puede estar justificada en razón de la necesidad de su adopción[61]. Así lo exige el art. 579 LECrim cuando establece que es necesario que existan

[61] Resulta significativa en este punto la STS de 27 de abril de 2005 (RJ 5219) cuando destaca que «de la nota de excepcionalidad se deriva que la intervención telefónica no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria».

indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia «importante» de la causa[62]. No puede olvidarse, además, que uno de los fines legítimos que habilitan para la previsión legal y la adopción de este tipo de medidas es el de la «defensa del orden y la prevención del delito», en el que se incluye, lógicamente, la investigación de hechos delictivos graves.

No basta, pues, con que la medida de intervención vaya dirigida a esclarecer un dato simplemente interesante para la investigación penal, sino que se requiere que se trate de descubrir, a través de la práctica de la intervención, datos relevantes.

La justificación de esta necesidad constituye uno de los parámetros esenciales para determinar la procedencia o no de la restricción del derecho fundamental, por cuanto alude al principio de la proporcionalidad que estudiaremos separadamente, dada su relevancia en esta materia.

3.º El tercer requisito de motivación exigido debe hacer específica referencia al delito o delitos concretos por el que se acuerde la intervención. Si falta en el auto esa referencia a la existencia de indicios concretos de criminalidad[63] y, consiguientemente, a un ilícito penal determinado, no será posible establecer el juicio de proporcionalidad entre la medida de intervención y la gravedad de los hechos.

La resolución judicial no puede ser dictada en forma tan abstracta que simplemente haga mención a que determinada persona se encuentra cometiendo presuntas acciones delictivas, sino que debe concretarse más. Así lo exige, además, el apartado 3.º del art. 579 de la LECrim al imponer como presupuesto necesario la apreciación de «indicios de criminalidad» en el sujeto que va a ser sometido a la intervención.

---

[62] A este respecto, la STC 239/2006, FJ 2, destaca que el órgano judicial debe exteriorizar «(…) por sí mismo en la resolución judicial o por remisión a la solicitud policial, cuyo contenido puede integrar aquélla— la existencia de los presupuestos materiales de la intervención, esto es, *los hechos o datos objetivos que puedan considerarse indicios* sobre la existencia de un delito grave y sobre la conexión de los sujetos que puedan verse afectados por la medida con los hechos investigados, puesto que tales precisiones constituyen el presupuesto habilitante de la intervención y el prius lógico del juicio de proporcionalidad que ha de realizar el órgano judicial». En el mismo sentido, las SSTC 26/2006, FJ 6, y 253/2006, FJ 2.

[63] Como ya tuvo ocasión de señalar la jurisprudencia del TS —ATS de 18 de junio de 1992 (RJ 6102, caso Naseiro) y también STS de 4 de mayo de 1994— los indicios racionales de criminalidad, son indicaciones, señales, notas, datos externos que, apreciados de manera razonable, permiten descubrir o atisbar, sin la seguridad de la plenitud probatoria, pero con la firmeza que proporciona una sospecha fundada, es decir, lógica, conforme a las reglas de la experiencia, la presunta existencia de la realidad de un hecho delictivo, y la posible participación en el mismo de la persona investigada, que más adelante se confirmará o no.

Pues bien, sobre este punto, el TC ha declarado que en el Auto deberán explicitarse «los datos o hechos objetivos que puedan considerarse indicios de la existencia del delito y la conexión de la persona o personas investigadas con el mismo, indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento. Esto es, sospechas fundadas en alguna clase de dato objetivo»[64].

Más adelante, la STC 259/2005 (FJ 2) describe cómo han de ser estas sospechas fundadas destacando que «la relación entre la persona investigada y el delito se manifiesta en las sospechas que… no son tan sólo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido; en primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona». Y más adelante continúa la sentencia señalando que «… estas sospechas han de fundarse en datos fácticos o indicios que permitan suponer que alguien intenta cometer, está cometiendo o ha cometido una infracción grave o en buenas razones o fuertes presunciones de que las infracciones están a punto de cometerse… o, en los términos en los que se expresa el actual art. 579 LECrim, en «indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa» (art. 579.1 LECrim) o «indicios de responsabilidad criminal» (art. 579.3 LECrim)[65].

---

[64] STC 259/2005, FJ 2, que cita, entre otras, las siguientes: SSTC 171/1999, FJ 8; 299/2000, FJ 4; 14/2001, FJ 5; 138/2001, FJ 3; y 202/2001, FJ 4, entre otras muchas.

[65] En la Sentencia se citan otras resoluciones anteriores: SSTC 49/1999, FJ 8; 166/1999, FJ 8; 171/1999, FJ 8; 299/2000, FJ 4; 14/2001, FJ 5; 138/2001, FJ 3 y 202/2001, FJ 4). Igualmente, la STC 239/2006, FJ 2, ha precisado que «… las sospechas, para entenderse fundadas, han de hallarse apoyadas en datos objetivos, en un doble sentido: en primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona». Por ello «es necesario examinar si en el momento de pedir y acordar la medida se pusieron de manifiesto ante el Juez no meras suposiciones o conjeturas, sino datos objetivos que permitieran pensar que la línea telefónica era utilizada por personas sospechosas de la comisión del delito que se investigaba y que, por lo tanto, no se trataba de una investigación meramente prospectiva, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar sospechas sin base objetiva que surjan en la mente de los encargados de la investigación penal, pues de otro modo se desvanecería la exigencia constitucional».

El TS, por su parte, ha perfilado en un plano más práctico qué indicios son los que pueden ser incorporados por el Juez en su resolución, dictada normalmente a partir de la solicitud policial, destacando en este sentido en su STS de 15 de septiembre de 2005 (RJ 7174, FJ 2, 2.) que «no es necesario manifestar en el oficio de solicitud de la medida qué actuaciones concretas fueron éstas, aunque con frecuencia sea su expresión lo que mejor permite valorar la suficiencia de esos datos. Basta con que tal oficio exprese esos datos concretos, esas relaciones del investigado con otras personas asimismo sospechosas, esos contactos con lugares donde, por ejemplo, se trafica con drogas, viajes a sitios donde la droga se produce o se adquiere con facilidad, etc». En todo caso sí es cierto que domina la casuística y que resulta muy difícil afrontar el problema y buscar solución al mismo con ideas o criterios generales, aunque entiendo que lo aquí recogido pueda esclarecer el sentido de a qué indicios alude la Jurisprudencia para estimar cumplida esta exigencia.

El estudio de este requisito supone también hacer mención a los supuestos de remisión judicial a la solicitud policial, por cuanto en la inmensa mayoría de los casos, la decisión judicial de autorizar la limitación del derecho se apoya exclusivamente en la solicitud que le presenta la policía judicial. En este sentido, la doctrina del TC es clara al respecto, destacando, en principio, la adecuación al derecho fundamental que se limita de aquella resolución judicial que se remita a la solicitud policial cursada, siempre que en esta última se contengan todas las exigencias específicas establecidas por la doctrina del Tribunal elaborada al respecto. A título de ejemplo, la STC 165/2005 (FJ 4.) declara:

> «(…) aunque lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención quede exteriorizada directamente en la resolución judicial, ésta puede considerarse suficientemente motivada si, integrada incluso con la solicitud policial, a la que puede remitirse, contiene los elementos necesarios para considerar satisfechas las exigencias para poder llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva»[66].

Finalmente, hay que abordar en este punto la problemática que, a efectos de cumplimiento de este requisito de la motivación, supone la utilización de autos o resoluciones impresas para acordar la medida limitativa del derecho. El criterio que sigue en este sentido el Tribunal

[66] En el mismo sentido SSTC 299/2000, FJ 4; 167/2002, FJ 2; 184/2003, FJ 9 y 11. Aún más recientemente, también, la STC 205/2005, FJ 3.

es el de no estimar conveniente este tipo de prácticas, si bien ello no supone el rechazo automático de los mismos, siempre que en el impreso se exterioricen las circunstancias individualizadas que hayan motivado la limitación del derecho y las exigencias específicas que conlleva el caso concreto. Más claramente, la STC 205/2005 (FJ 3) señala al respecto que «aun utilizando la no recomendable forma del impreso, una resolución puede estar motivada si, integrada incluso con la solicitud policial a la que puede remitirse, contiene los elementos necesarios a efectos de considerar satisfechas las exigencias para poder llevar a cabo con posterioridad la ponderación de la restricción de derechos fundamentales que la proporcionalidad de la medida conlleva»[67].

4.º Además, es necesario que el delito o delitos que pretendan ser esclarecidos revistan el carácter de graves, por cuanto constituye la apreciación de esta condición otro de los parámetros precisos para establecer el juicio de proporcionalidad de la medida adoptada. Ahora bien, la gravedad de los delitos a que se refiere la doctrina constitucional no viene exclusivamente determinada por la calificación jurídica de la pena que prevea el CP como tal sino que el concepto de la gravedad, para ser valorado, ha de ser referido también a otros factores no menos relevantes. Así, la STC 299/2000 (FJ 2) señala al respecto que «la gravedad de la infracción punible no puede estar determinada únicamente por la calificación de la pena legalmente prevista, aunque indudablemente es un factor que debe de ser considerado, sino que también deben tenerse en cuenta otros factores, como los bienes jurídicos protegidos y la relevancia social de aquélla»[68], de ahí que en algunos casos, sea posible

---

[67] En el mismo sentido las SSTC 200/1997, FJ 4, 171/1999, FJ 6, y 126/2000, FJ 7, entre otras.

[68] En el mismo sentido, la STC 104/2006, FJ 3, señala de modo textual que «… es al legislador al que compete en primer término realizar el juicio de proporcionalidad efectuando "la delimitación de la naturaleza y gravedad de los hechos en virtud de cuya investigación puede acordarse" la intervención de las comunicaciones telefónicas, de modo que la ausencia de previsión expresa en la Ley de este extremo ha sido considerado por el Tribunal Europeo de Derechos Humanos y por nuestra jurisprudencia un defecto relevante de la Ley que ha de regular las condiciones de legitimidad de las intervenciones telefónicas (STEDH 18 de febrero de 2003, caso Prado Bugallo c. España, ap. 30; STC 184/2003, de 23 de octubre, F. 5)». Pero, «… hasta que la necesaria intervención del legislador se produzca, corresponde a este Tribunal suplir las insuficiencias legales precisando los requisitos que la Constitución exige para la legitimidad de las intervenciones telefónicas». Por ello, el TC continúa destacando que «… las intervenciones telefónicas respetan el principio de proporcionalidad cuando su finalidad es la investigación de una "infracción punible grave, en atención al bien jurídico protegido y a la relevancia social del mismo, de modo que *la gravedad de la "infracción punible no puede estar determinada únicamente por la calificación de la pena legalmente prevista, aunque indudablemente es un factor*

acordar la limitación del derecho para la investigación de un delito al que el CP castigue con pena inferior a los cinco años de prisión (según la clasificación tripartita del art. 33 CP) en función de la relevancia del bien jurídico protegido o teniendo en cuenta la trascendencia social que el supuesto delito investigado haya podido tener.

Además, tal requisito, en la práctica forense, puede ser *a priori* muy difícil de ponderar por parte del Juez que debe tomar un decisión respecto de la solicitud formulada cuando, por ejemplo, el hecho presuntamente delictivo no haya quedado aún perfilado ni esclarecido en su totalidad por encontrarse en la fase inicial de la investigación y, por consiguiente, resulte extraordinariamente complicado precisar la gravedad del ilícito. En tales casos, no habrá más remedio que acudir a criterios de flexibilidad, teniendo en cuenta otros parámetros como puedan ser los que aporte la trascendencia social del evento o incluso, la mayor o menor dificultad existente para investigar y acreditar su comisión, en los términos que han sido reseñados por la doctrina constitucional citada.

Quizá, como ocurre en el Derecho Comparado[69], sería conveniente que el legislador delimitara los supuestos típicos en que resulte posible acordar la medida de intervención telefónica como modo de garantizar la seguridad jurídica y evitar una excesiva discrecionalidad que pueda rayar en la arbitrariedad.

Finalmente, señalar que el requisito de la motivación no se agota con el análisis descriptivo de las exigencias concretas que ello comporta, por cuanto el Tribunal ha introducido también una línea doctrinal que marca una escala gradual cualitativa en el cumplimiento de sus requisitos, en función de que la injerencia en el derecho fundamental sea de mayor o de menor intensidad. En este sentido, y en líneas generales, podemos afirmar que, mientras que en todos los supuestos de intromisión en el derecho que se conceptúen como de mayor intensidad, como puedan ser los supuestos de interceptación o de observación en el ejercicio del derecho a comunicarse, el TC mantiene sus exigencias máximas de motivación, requiriendo para ello la formalidad del Auto autorizando la limitación, con los requisitos que acabamos de exponer. Sin embargo, en supuestos en que la injerencia es de menor intensidad —por ejemplo, en la autorización para recabar información sobre los titulares de los números telefónicos que figuren en un listín o agenda— bastará la mera

---

que debe de ser considerado, sino que también deben tenerse en cuenta otros factores, como los bienes jurídicos protegidos y la relevancia social de aquélla"».

[69] En el Derecho alemán, en el italiano o en el francés, como hemos anticipado en otros apartados de este trabajo el legislador ha precisado con mayor detenimiento los tipos delictivos que pueden ser objeto de intervención de las comunicaciones.

providencia, motivando eso sí, las razones por las que se haya acordado dicha autorización.

Resulta gráfica en este sentido la lectura de la STC 123/2002 (FJ 7) en la que se alude a supuestos de intromisión en el derecho fundamental al secreto de las comunicaciones que son calificados por el Tribunal como de «menor intensidad» y que, si bien requieren de una resolución judicial motivada, esta exigencia puede verse cumplida con una providencia en la que, con justificación de la proporcionalidad de la medida, el órgano judicial haya razonado sobre la necesariedad e idoneidad de aquella a los fines de la investigación criminal que se esté desarrollando y si la misma se integra con los datos facilitados por la solicitud policial[70]. En concreto y de modo textual, el Tribunal declara lo siguiente:

> «Sin ningún género de dudas una providencia no es, por su propia estructura, contenido y función, la forma idónea que ha de adoptar una resolución judicial que autoriza la limitación de un derecho fundamental, y, ciertamente, lo deseable, desde la perspectiva de la protección del derecho fundamental, es que la resolución judicial exprese por sí misma todos los elementos necesarios para considerar fundamentada la medida limitativa del derecho fundamental (STC 299/2000, de 11 de diciembre, F. 4). Sin embargo, hemos admitido que una resolución judicial puede considerarse motivada si, integrada con la solicitud de la autoridad a la que se remite, "contiene todos los elementos necesarios para considerar satisfechas las exigencias para poder llevar a

[70] Se está refiriendo en concreto a supuestos como, por ejemplo, en que la Policía Judicial solicite del Juez la identificación de los titulares de determinados números telefónicos que aparezcan en el teléfono móvil de un sospechoso o detenido. A este respecto, la STS de 6 de marzo de 2006 (RJ 2303) destaca textualmente lo siguiente: «*Es sustancialmente distinto la facilitación de un listado de llamadas que una intervención telefónica*, basta al respecto para esto último la sola autorización judicial en el marco de un proceso penal con un nivel de exigencia y control mucho más bajo que el de una intervención de las conversaciones porque la injerencia es mucho menor sin que exista vulneración al derecho fundamental al secreto de las conversaciones. En tal sentido SSTS 459/99 de 22 de marzo (RJ 2947) y 1086/2003 de 25 de julio (RJ 5393). Con la primera de las sentencias citadas, podemos afirmar que la petición del listado de llamadas, aunque fuese ordenada por providencia por el Juez de instrucción es diligencia que no afecta al derecho a la privacidad de las conversaciones, se trata en definitiva, de datos de carácter personal, custodiados en ficheros automatizados, a que se refiere la Ley Orgánica 5/1992, de 29 de octubre [hoy la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal], reguladora del Tratamiento de tales datos, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución; estableciéndose en la misma que el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, el cual, sin embargo, no será preciso cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas, como es el caso».

> cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva" (SSTC 200/1997, de 24 de noviembre, F. 4; 166/1999, de 27 de septiembre, F. 7; 126/2000, de 16 de mayo, F. 7; y 299/2000, de 11 de diciembre, F. 4)».

Desde esta perspectiva, y en la medida en que la exigencia de resolución judicial a efectos de limitar un derecho fundamental posee carácter material, pues han de ser los Jueces y Tribunales los que autoricen el levantamiento del secreto de las comunicaciones ponderando la proporcionalidad de las medidas que afecten a este derecho fundamental y controlen su ejecución, hemos de considerar que, aunque desde luego la resolución judicial debe adoptar la forma de auto, excepcionalmente también una providencia, integrada con la solicitud a la que se remite, puede cumplir las exigencias constitucionales en un caso como el analizado en el que se trata de autorizar el acceso a los listados telefónicos por parte de la policía. Ello sucederá si la providencia integrada con la solicitud policial a la que se remite contiene todos los elementos necesarios para poder llevar a cabo con posterioridad la ponderación de la proporcionalidad de la limitación del derecho fundamental. A los efectos del juicio de proporcionalidad resulta especialmente significativo, como hemos subrayado, el dato de la menor intensidad lesiva en el objeto de protección del derecho al secreto de las comunicaciones que el acceso a los listados comporta, de modo que este dato constituye elemento indispensable tanto de la ponderación de la necesidad de esta medida para alcanzar un fin constitucionalmente legítimo, como a los efectos de estimación de la concurrencia del presupuesto habilitante de la misma».

Como puede observarse de la lectura de este párrafo de la sentencia, el Tribunal, aún reconociendo la excepcionalidad del supuesto, establece una gradación en la injerencia de este derecho, distinguiendo entre supuestos de limitación de mayor y de menor intensidad, permitiendo para estos últimos, conforme a un criterio material, que la resolución judicial no necesariamente revista la forma de auto, sino que baste una providencia, lógicamente motivada, que cumpla las exigencias establecidas por la doctrina constitucional para que pueda ulteriormente realizarse un juicio de proporcionalidad sobre los razonamientos esgrimidos por la misma. Creo que esta dual distinción puede generar problemas desde el punto de vista de las garantías, al distinguir donde no lo hace ni la Constitución ni tampoco la doctrina del TEDH, entre lo que podríamos denominar injerencias en el derecho fundamental de primera categoría, las de mayor intensidad, y de segundo grado, las de menor, cuando el derecho fundamental, en su contenido, es único y, por tanto, toda

limitación exige una intervención judicial motivada con cumplimiento de todos los requisitos que hemos analizado. Pero es que, además, puede ocasionar un factor de inseguridad jurídica, por cuanto que, si bien el Tribunal apunta la excepcionalidad del caso —solicitud de un listado telefónico—, qué duda cabe de que la práctica forense diaria es rica en supuestos singulares y en matices y en algún caso podrá surgir la duda de si la formalidad del auto es requerida para cumplir la exigencia de motivación o, por el contrario, bastará una mera providencia para cubrir aquélla. Es evidente que el problema tiene mayor calado teórico que práctico, pues en la realidad de los Tribunales, la duda debe ser resuelta tal y como reconoce también el Tribunal en su sentencia, por la opción del auto, pero también puede llevar a la consideración por parte del Juez de que baste una mera providencia, en muchos casos impresa, para entender cubierto el requisito de la motivación, lo que llevará consigo la vulneración del derecho fundamental y la nulidad de todo lo investigado a su resulta.

c) La proporcionalidad

El siguiente requisito es el de la proporcionalidad. En el Auto debe realizarse una ponderación con apoyo en el principio de proporcionalidad, inherente al valor justicia, de la razonabilidad de la medida a adoptar[71].

Antes de ello, el Juez, para apreciar si la resolución que acuerde la intervención telefónica es proporcionada al hecho que pretende investigarse, deberá tener en cuenta un conjunto de dos circunstancias[72] que

[71] Como ha señalado el ATS de 24 de enero de 1996 (RJ 275), «el principio de proporcionalidad en la práctica de una diligencia de investigación de un delito se rige por la relación o contraposición de dos parámetros: La gravedad o trascendencia social del hecho a investigar y las molestias o invasión de los derechos del sujeto sometido a aquélla».

[72] La doctrina del Tribunal Constitucional y la Jurisprudencia del TS han señalado, sin embargo, sobre el particular que la comprobación de proporcionalidad se mide en función de tres parámetros (STC 66/1995, 56 y 207/1996, 205/2002 y STS 15 de febrero de 1997 (RJ 1178), referida a la inviolabilidad del domicilio, pero de perfecta aplicación, también, a esta materia):

1. La aptitud de la medida para la consecución del objetivo propuesto (juicio de idoneidad).

2. La exclusión del empleo de otra medida más moderada para la consecución del fin perseguido con igual eficacia (juicio de necesidad).

La necesidad en este caso, implica que sólo cabe acudir a la medida si es realmente imprescindible tanto desde la perspectiva de la probable utilidad, como de la cualidad de insustituible, porque si no es probable que se obtengan datos esenciales, o si estos se pueden lograr por otros medios menos gravosos, estaría vetada la intervención (STC de 31 de enero de 1985 y SSTS de 24 de junio y 18 de julio de 1996 —RJ 4728 y 6069—).

operan como verdaderos presupuestos previos a la propia ponderación de esa proporcionalidad:

1.ª La de la indispensabilidad de dicha medida, de tal manera que no disponga de otro medio de investigación alternativo con el que poder llegar al mismo resultado esclarecedor.
2.ª El principio de mínima intervención, que en este caso consistirá en que la injerencia que autorice resulte lo menos gravosa posible para la persona o personas afectadas, procurando en este sentido limitar la ejecución de la medida a aquellos aspectos (números telefónicos, o modalidades de correspondencia postal) sobre los que existan sospechas fundadas de que son utilizados habitualmente por las personas sujetas a dicha medida, teniendo en cuenta que, a veces, la escucha o la intervención de la correspondencia se establece, no sobre los teléfonos o sobre el correo de que son titulares los investigados, sino sobre los de un tercero ajeno a la investigación[73].

En relación con este principio, la STC 261/2005 (FJ2) viene a sintetizar muy gráficamente los dos postulados que requiere el juicio de proporcionalidad, al señalar:

> «… la medida autorizada tiene que ser necesaria para alcanzar un fin constitucionalmente legítimo. La desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a su enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que la Constitución garantiza. Así, hemos mantenido que esta intervención puede ser constitucionalmente ilegítima cuando no es imprescindible, bien porque los conocimientos que pueden ser obtenidos carecen de relevancia respecto de la investigación en curso o bien porque pudieran obtenerse a través de otras medidas menos gravosas de los derechos fundamentales».

En realidad, este exigencia de la proporcionalidad guarda una íntima relación con el requisito anterior de la motivación, pues éste se configura

---

3. El equilibrio entre los beneficios y ventajas de los valores, como pueden ser la gravedad del ilícito, su trascendencia social y las sospechas existentes, excluyéndose cualquier autorización judicial en blanco, sin especificación delictiva pues ello supondría la imposibilidad de valorar aquel «juicio de equilibrio y ponderación» (juicio de proporcionalidad en sentido estricto).

[73] Tal es el caso contemplado, por ejemplo, en la STEDH de 24 de agosto de 1998, caso LAMBERT contra Francia.

como un *prius* del examen de aquélla. Así lo ha entendido la doctrina del TC y lo refleja la propia STC 261/2005 citada, al añadir a lo anteriormente expuesto:

> «la obligación de motivar la resolución por la que se acuerda una intervención telefónica constituye una exigencia previa al examen del principio de proporcionalidad, por cuanto toda disposición limitativa de un derecho fundamental ha de ser convenientemente razonada a fin de que, en ella, se plasme el pertinente juicio de ponderación sobre su necesidad. Así, la expresión del presupuesto habilitante de la intervención telefónica constituye un prius lógico de este juicio de proporcionalidad, pues, de una parte, mal puede estimarse realizado ese juicio, en el momento de la adopción de la medida, si no se manifiesta, al menos, que concurre el presupuesto que la legitima y, por otra parte, sólo a través de esa expresión, podría comprobarse posteriormente su idoneidad y necesidad, es decir, la razonabilidad de la medida limitativa del derecho fundamental…».

Una vez apreciada dicha necesidad y resuelto a acordarla en su mínima intervención, debe entonces realizar el Juez el juicio de proporcionalidad apreciando si el hecho a investigar alcanza la suficiente gravedad, entraña la notable trascendencia social, o reviste la extraordinaria dificultad de esclarecimiento, que exige el sacrificio del derecho fundamental correspondiente, y en tal caso, si llega a la conclusión de que sí es necesaria la limitación, en aras del interés público, proceder a autorizar la medida de intervención.

d) La duración

Como cualquier otra medida limitativa de derechos fundamentales, la resolución que acuerde la intervención de la comunicación debe señalar el tiempo en que operará la ejecución de la medida limitativa, partiendo siempre de que éste ha de ser el indispensable para la obtención de los fines constitucionales que persigue.

Lógicamente, el planteamiento de este requisito es muy diverso según el tipo de intervención de que se trate, pues si es de una escucha telefónica, la duración podrá prolongarse hasta un máximo de tres meses prorrogables, según dispone el art. 579. 3 LECrim, mientras que si se trata de una medida de interceptación de la correspondencia las posibilidades de duración en el tiempo suelen ser, por su propia naturaleza, de una duración inferior, circunscrita a veces a la mera recepción de un paquete o envío postal.

El TC ha destacado el requisito de la duración temporal como fundamental para la regularidad constitucional de la medida limitativa, siendo

ejes esenciales de su doctrina, además de la exigencia de que en la propia resolución se fije un plazo[74], los siguientes:

1.º En primer lugar, que el plazo de duración de la medida habrá de computarse a partir de la fecha en que haya sido dictado el Auto. Según la STC 205/2005 (FJ 5) varias son las razones que llevan a esta conclusión, frente al planteamiento de la jurisprudencia del TS, que fija el inicio del cómputo a la fecha en que la ejecución de la medida pudiera ser efectiva, es decir, desde el día en que se inicie en la práctica la escucha telefónica o la interceptación de la correspondencia.

Las razones que avalan este argumento son las siguientes.

a) En primer lugar, acoger la tesis de que el cómputo del plazo de duración de la medida limitativa del derecho empiece a correr desde la fecha en que es puesta en práctica y se ejecuta de modo efectivo «supone aceptar que se ha producido una suspensión individualizada del derecho fundamental al secreto de las comunicaciones, que tiene lugar desde el día en que se acuerda la resolución judicial hasta aquel en el que la intervención telefónica empieza a producirse» lo que es absolutamente intolerable desde la perspectiva de la efectividad del derecho fundamental, por cuanto sería sustraer al control judicial el tiempo que transcurriera entre un acto y otro, con la posibilidad de que se produjeran injerencias intolerables en el derecho.
b) Los preceptos de la normativa legal que regulen la aplicación y ejecución de una medida limitativa del derecho fundamental deben ser interpretados «en el sentido más favorable a la efectividad de los derechos fundamentales, lo que no es sino consecuencia de la especial relevancia y posición que en nuestro sistema tienen los derechos fundamentales y libertades públicas»[75], por lo que, como destaca el Tribunal, «la lectura más garantista, desde la

---

[74] STC 170/1996 y ATC 54/1999, por todos; la primera de las indicadas resoluciones (FJ 2) destaca que «el Tribunal ha venido exigiendo que al adoptarse la medida intervención de las comunicaciones se determine el período temporal de su vigencia, aunque para ello no sea estrictamente necesario fijar una fecha concreta de finalización, sino que ésta puede hacerse depender de la desaparición de la condición o circunstancia concreta que justifica la intervención». De este criterio es también la doctrina del TEDH, básicamente y por lo que se refiere a los intereses españoles, las SSTEDH de los casos Valenzuela Contreras y Prado Bugallo de 30 de julio de 1998 y de 18 de febrero de 2003, que coinciden en la necesidad de que las resoluciones motivadas dictadas por la autoridad pública competente fijen un plazo máximo de duración de la medida, que puede ser reducido cuando la misma haya alcanzado los fines para los que fue acordada.

[75] STC 133/2001, FJ 5.

perspectiva del secreto de las comunicaciones, es la que entiende que el plazo de intervención posible en el mentado derecho fundamental comienza a correr desde el momento en que la misma ha sido autorizada».

c) Finalmente, que la interpretación de que el plazo de duración de la medida deba empezar a computarse desde la fecha en que la intervención sea efectiva y comience a ejecutarse compromete gravemente la seguridad jurídica, pues hace depender de terceros ajenos al órgano judicial la duración de la misma. Así, el Tribunal señala textualmente que esta interpretación, además de afectar a la seguridad jurídica en los términos que acabamos de exponer, «consagra una lesión en el derecho fundamental, que tiene su origen en que sobre el afectado pesa una eventual restricción que, en puridad, no tiene un alcance temporal limitado, ya que todo dependerá del momento inicial en que la intervención tenga lugar»[76].

2.º Y, en segundo término que, si bien, transcurrido el plazo de duración inicial de la limitación del derecho, pueden ser acordadas sucesivas prórrogas al mismo, la resolución judicial que la acuerde deberá cumplir dos exigencias en cada ocasión:

a) La propia de la motivación en los mismos términos que se han exigido para la resolución inicial que acordó la medida, esto es justificando las razones de su adopción con apoyo en las circunstancias que concurran al momento en que la prórroga haya de ser adoptada. Así lo destaca la doctrina del TC, por ejemplo, en su STC 202/2001 (FJ 6) cuando dispone que

> «las condiciones de legitimidad de la limitación del derecho al secreto de las comunicaciones afectan también a las resoluciones de prórroga, y, respecto de ellas, además debe tenerse en cuenta que la motivación ha de atender a las circunstancias concretas concurrentes en cada momento que legitiman la restricción del derecho, aun cuando sólo sea para poner de manifiesto la persistencia de las razones que, en su

[76] Continúa diciendo en este sentido el FJ 5 de la STC 205/2005 que «es así posible, por ejemplo, que la restricción del derecho se produzca meses después de que fuera autorizada, o que la autorización quede conferida sin que la misma tenga lugar ni sea formalmente cancelada por parte del órgano judicial. En definitiva, la Constitución solamente permite —con excepción de las previsiones del art. 55 CE— que el secreto de las comunicaciones pueda verse lícitamente restringido mediante resolución judicial (art. 18.3 CE), sin que la intervención de terceros pueda alterar el *dies a quo* determinado por aquélla».

> día, determinaron la inicial decisión de intervenir las comunicaciones del sujeto investigado, pues sólo así dichas razones pueden ser conocidas y supervisadas (STC 181/1995, F. 6), sin que a estos efectos sea suficiente "una motivación tácita o una integración de la motivación de la prórroga por aquella que se ofreció en el momento inicial. La necesidad de control judicial de la limitación del derecho fundamental exige aquí, cuando menos, que el Juez conozca los resultados de la intervención acordada para, a su vista, ratificar o alzar el medio de investigación utilizado»[77].

En este punto también es relevante destacar que, para acordar la prórroga de la limitación del derecho, no es necesario que el Juez reciba todo el material de investigación obtenido en el período que ya finaliza, ni tampoco que haya de revisarlo en su totalidad, pues bastará con que haya sido informado puntualmente del estado de las investigaciones. Este es el criterio que establece la STC 205/2005 (FJ 4) cuando afirma que

> «la argumentación que se desarrolla en la demanda, según la cual el órgano judicial sólo podría acordar una prórroga de una intervención telefónica tras examinar, personalmente, los resultados de la diligencia en su día acordada, se separa manifiestamente de nuestra jurisprudencia en la materia. En efecto, si bien es cierto que hemos declarado que la autorización de prórroga de la medida debe tener en cuenta los resultados obtenidos previamente (SSTC 49/1999, F. 11; y 171/1999, F. 8)… a tal fin no resulta necesario… que se entreguen las cintas en ese momento por la autoridad que lleve a cabo la medida, pues el Juez puede tener puntual información de los resultados de la intervención telefónica a través de los informes de quien la lleva a cabo»[78].

b) Y, en segundo término, que en todo caso la prórroga ha de ser acordada antes del vencimiento del plazo inicialmente concedi-

---

[77] En esta sentencia se analiza el supuesto de que el auto que autorizó la prórroga se limitó a destacar que se estaban realizando activas gestiones para la el esclarecimiento de los hechos y la intervención de sus partícipes considerándose por el TC que tales argumentos no cumplen el requisito de la motivación. En concreto, el FJ 6 de la sentencia pone de manifiesto que «La sola referencia a que *"se están practicando activas diligencias policiales"* contenida en los Autos de prórroga no es motivación suficiente para legitimar el mantenimiento de la medida de intervención, pues en estos casos deben explicitarse y ponderarse las concretas circunstancias concurrentes en cada momento, así como el conocimiento adquirido a través de la ejecución de la medida inicialmente prevista».

[78] En el mismo sentido las SSTC 82/2002, FJ 5. y ATC 225/2004, FJ 2, que se citan expresamente en esta sentencia y con posterioridad se recoge también esta doctrina en las SSTC 26/2006, FJ 8, y 239/2006, FJ4.

do. Si la prórroga fuera acordada con posterioridad a dicho vencimiento se habrá producido la vulneración del derecho fundamental, por cuanto, si ha persistido la ejecución de la intervención en el ínterin entre la finalización del plazo de la anterior limitación y la del nuevo plazo, se habrán efectuado intervenciones de la comunicación sin autorización ni control judicial.

e) La notificación al Ministerio Fiscal

Tanto el auto que inicialmente acuerde la medida limitativa del derecho fundamental como los sucesivos que prorroguen esta situación deben ser notificados al Fiscal, toda vez que constituyen una medida de control de la legitimidad de la actuación investigadora.

Así lo ha señalado el TC en su STC 146/2006 (FJ 4), destacando al respecto que «también ha de considerarse como un defecto constitucional en el control de la intervención la falta de notificación de los Autos de intervención al Ministerio Fiscal, que impide "el control inicial de la medida… en sustitución del interesado, por el garante de los derechos de los ciudadanos (art. 124.1 CE)»[79].

B) Fase de ejecución

En esta segunda fase de la limitación del derecho fundamental tiene lugar la puesta en práctica efectiva de la intervención de la comunicación correspondiente.

En este sentido, el artículo 579 LECrim, que es el que habilita legalmente para la intervención de los medios de comunicación verbal y de la correspondencia escrita, distingue dos modalidades de ejecución: La observación y la intervención propiamente dicha, pareciendo establecer, en consecuencia, dos formas de ejecución de la medida limitativa de diferente intensidad, pues mientras que la primera aludiría a aquella injerencia que se limita simplemente a tomar un conocimiento externo de la existencia del acto de comunicación[80] pero sin acceder al contenido de lo comunicado, la segunda representaría la modalidad más profunda de la intromisión en el derecho de los interlocutores, toda vez que habilitaría para conocer el contenido de lo comunicado. La distinción

[79] En el mismo sentido las SSTC 205/2002, FJ 5, 165/2005, FJ 7, y 259/2005, FJ 5, que cita la STC 146/2006 que hemos recogido.

[80] Esto es que la comunicación existió, que la misma tuvo lugar en una fecha y hora determinada, que, en su caso, se operó desde un determinado lugar a otro y de quiénes fueron los comunicantes, así como de otros datos periféricos del acto comunicativo.

es importante a los efectos del juicio de proporcionalidad que hemos destacado anteriormente, toda vez que, si para la consecución de los fines perseguidos por la investigación criminal en un asunto determinado, bastara la mera observación, es evidente que quedaría afectado el derecho fundamental por desproporcionada limitación del mismo si se autorizara la intervención. O lo que es lo mismo, si se acordara la interceptación de un teléfono o de un envío postal cuando, para los fines de la investigación que se lleva a cabo, hubiera bastado la mera constancia del acto de comunicación sin reportar una mayor utilidad para la investigación el contenido de aquél, el exceso en la injerencia resultaría desproporcionado, por cuanto faltaría el requisito de la necesariedad de la medida, que exige que, de haber existido otra medida menos gravosa para el derecho fundamental, se hubiera que tenido que aplicar ésta en lugar de aquélla.

Durante la fase de ejecución de la medida, en la que la Autoridad Judicial delega en la Policía Judicial la realización de las tareas materiales propias para llevar a efecto la intervención de los actos de comunicación, la doctrina constitucional ha establecido también una serie de exigencias que pretenden fundamentalmente garantizar, de una parte, el control judicial de la medida y, de otro lado, preservar la autenticidad de las fuentes de prueba.

Tales requisitos son los siguientes:

1.º En primer lugar y sin ninguna duda, el control judicial de la ejecución de la medida. Como pone de relieve la STC 166/1999 (FJ 3c) «el control judicial puede resultar ausente o deficiente en caso de falta de fijación judicial de los períodos en los que debe darse cuenta al juez de los resultados de la restricción, así como en caso de su incumplimiento por la Policía; igualmente, queda afectada la constitucionalidad de la medida si, por otras razones, el Juez no efectúa un seguimiento de las vicisitudes del desarrollo y cese de la intervención telefónica, y si no conoce el resultado obtenido en la investigación». Durante esta fase, el Juez debe estar expectante a las diversas vicisitudes que tenga el curso de la intervención y, desde luego, tratándose de supuestos de intervención de las comunicaciones orales, controlar que la labor policial se ejecute de conformidad con lo acordado en el auto que autorizó las escuchas. Si se tratare de intervención de la correspondencia escrita, lógicamente, velar por que los agentes de policía que actúen por su delegación se limiten también a interceptar o a tomar nota de los envíos postales correspondientes a las personas sujetas a investigación.

2.º Y, en segundo término, por lo que se refiere a los agentes de la Policía Judicial que hayan de llevar a efecto de modo material la ejecución de la medida, les corresponderá, si se trata de intervenciones de medios de comunicación oral o electrónica, grabar en los correspondientes soportes magnéticos que hayan sido autenticados bajo la fe del Secretario Judicial correspondiente, la totalidad de las conversaciones o actos de comunicación que se realicen desde o a los aparatos cuya intervención haya sido acordada. Lógicamente si se trata de una mera observación, el acceso al contenido de lo comunicado queda vedado para los policías, que únicamente podrán hacer labores de seguimiento de tales actos de comunicación producidos en los términos y con los límites que haya establecido la autorización judicial. Igualmente, si se trata de una intervención de la correspondencia se retendrán los envíos postales que correspondan a los interesados sujetos a la investigación o que guarden relación con la misma.

Como señala la misma STC 166/1999 (FJ 3b) antes citada «la ejecución policial puede resultar constitucionalmente ilegítima en la medida en que se verifique al margen de la cobertura judicial de la misma, es decir excediéndose de los límites temporales —se mantiene la intervención más tiempo del habilitado—, personales —se investigan personas distintas de las autorizadas— materiales —hechos diferentes—, u otros que constituyan condiciones judicialmente impuestas de la autorización»[81].

Además, los funcionarios policiales, si se trata de intervenciones telefónicas, deberán ir remitiendo con la periodicidad que indique el Juzgado los soportes originales que contengan en su integridad los actos de comunicación realizados desde o al aparato de comunicación intervenido, con una trascripción literal del contenido de las conversaciones —lógicamente si fue autorizada la intervención en su manifestación más intensa—. Y si la medida afectó al secreto de la correspondencia, deberán proceder en la oficina de correos o lugar de recepción del envío postal, a la interceptación de todos o sólo de aquellos envíos postales en la forma en que se haya determinado en la resolución judicial autorizante, entregando inmediatamente dichos envíos postales en el Juzgado correspondiente.

Particular importancia cobran en esta fase las diferentes vicisitudes que pueden ocurrir durante la ejecución de la medida, tales como la

[81] En el mismo sentido SSTC 85/1994, FJ 3, 86/1995, FJ 3, 49/1996, FJ 3 y 121/1998, FJ 5.).

aparición de nuevas personas que pueden ser imputadas por los delitos investigados, el surgimiento de nuevos hechos presuntamente delictivos que hayan de ser objeto de investigación o el descubrimiento de nuevos aparatos de comunicación o de teléfonos que se hayan venido utilizando para la comisión de tales hechos, es decir, los avatares propios de unas diligencias de investigación que pueden perseguir el descubrimiento de nuevos factores criminógenos. En tales casos nos hallamos ante circunstancias totalmente imprevistas e imprevisibles en el momento en que fue dictada la resolución judicial autorizante y que de forma sobrevenida han ido apareciendo.

En este sentido, la doctrina reiterada del Tribunal se puede concretar en dos ideas básicas. De una parte, los denominados hallazgos casuales surgidos al amparo de una resolución judicial habilitante quedan totalmente cubiertos por la protección constitucional del auto anteriormente dictado, de tal manera que se considerarán como diligencias de prueba preconstituida perfectamente válidas para ser valoradas por el órgano de enjuiciamiento. De otro lado, también es indispensable que los funcionarios policiales encargados de ejecutar la medida, comuniquen inmediatamente al Juez de Instrucción la existencia de tales hallazgos, con objeto de que éste pueda ampliar, si lo estima procedente, la autorización judicial en aquellos extremos que requieran las circunstancias del caso, esto es la ampliación de la medida para la intervención de nuevos aparatos de comunicación, la extensión de la limitación a otras personas que hasta ese momento no aparecían implicadas en la investigación o la apertura de nuevas líneas de investigación para esclarecer los hechos presuntamente delictivos descubiertos en el curso de las que ya se estén realizando.

Precisamente, a los denominados «hallazgos casuales» se refirió el ATC 400/2004 (FJ 2) cuando acordó la inadmisión de un recurso de amparo porque los funcionarios policiales dieron cuenta inmediata al Juzgado del descubrimiento de nuevos hechos delictivos que requerían de la ampliación de la investigación[82]. En el apartado relativo a la valoración

[82] En concreto, el citado Fundamento destaca textualmente lo siguiente: «Por lo que respecta a la exigencia de nueva autorización judicial tras haberse descubierto en las escuchas la existencia de un delito distinto de aquel para cuya investigación se habían autorizado, ha de destacarse que los órganos judiciales a quo han examinado el problema y concluido, en resoluciones que no pueden considerarse manifiestamente irrazonables (Auto de la Audiencia Provincial de Pontevedra de 29 de diciembre de 2000, razonamiento jurídico segundo y tercero, y Sentencia de la Sala Segunda del Tribunal Supremo de 20 de junio de 2003 [RJ 4359], fundamento de Derecho segundo), que pueden ser utilizados los hallazgos casuales producto de escuchas para deducir actuaciones contra los que resultaren implicados en delito grave por las mismas, interpretación,

de la prueba de este trabajo se analiza con mayor detalle esta problemática.

C) Fase posterior a la ejecución

Constituye la tercera y última de las fases del procedimiento de limitación de este derecho fundamental. El TC ha destacado con toda rotundidad que cualquier irregularidad de alcance constitucional que cause indefensión en esta última fase no afecta propiamente al derecho al secreto de las comunicaciones sino al proceso debido, es decir al derecho a un proceso con todas las garantías.

Resulta significativo en este punto el ATC 5/2001 cuando afirma que «no constituye vulneración del derecho al secreto de las comunicaciones, sino del derecho a un proceso con todas las garantías, la utilización como prueba del contenido de las conversaciones intervenidas, pero con respecto a las cuales las irregularidades, que implican ausencia o deficiente control judicial de la medida, no tienen lugar durante la ejecución del acto limitativo, sino en la incorporación de su resultado a las actuaciones sumariales». Agregando, a este respecto, la STC 202/2001 (FJ 7) que «todo lo que respecta a la entrega y selección de las cintas grabadas, a la custodia de los originales y a la trascripción de su contenido no forma parte de las garantías derivadas del art. 18.3 CE, sin perjuicio de su relevancia a efectos probatorios, pues es posible que la defectuosa incorporación a las actuaciones del resultado de una intervención telefónica legítimamente autorizada no reúna las garantías de control judicial y contradicción suficientes como para convertir la grabación de las escuchas en una prueba válida para desvirtuar la presunción de inocencia»[83].

En efecto, en esta última fase del procedimiento cobra especial relevancia el control judicial de todo el material de investigación que haya sido obtenido como consecuencia de la limitación del derecho erigién-

---

convalidada por la jurisprudencia del Tribunal Supremo y experiencias extranjeras, que no corresponde a este Tribunal revisar dado que, en ningún caso, viene a contradecir el texto constitucional ni nuestra doctrina sobre el mismo. Por otra parte, la utilización en este caso del hallazgo casual ha resultado plenamente respetuosa con las exigencias que pudieran derivarse del reconocimiento constitucional del derecho al secreto de las comunicaciones, puesto que *aquél ha sido utilizado como mera notitia criminis que se ha hecho llegar inmediatamente al órgano judicial competente*, sin que se haya procedido a continuar con unas escuchas que ya entonces no hubiesen tenido cobertura en el Auto de intervención citado».

[83] En el mismo sentido las SSTC 49/1999, FJ 5, 166/1999, FJ 2, 236/1999, FJ 4, 126/2000, FJ 9, 14/2001, FJ 4, 202/2001, FJ 7, y 167/2002, entre otras.

dose en verdadera prueba preconstituida que ha de llegar, previo cumplimiento de los requisitos que, a continuación expondremos, incólume al juicio oral y a la disponibilidad del órgano de enjuiciamiento y de las partes. Además, la garantía de la contradicción, como veremos a continuación, exige el conocimiento por parte del imputado en la fase de instrucción del material probatorio obtenido[84].

Para que este control sea efectivo es necesario que la autoridad judicial encargada de ello, en primer lugar, asegure la autenticidad de la fuente de prueba, es decir, que si las intervenciones de los teléfonos o de cualesquiera otros aparatos que permitan la comunicación a distancia han sido intervenidos y el contenido de lo comunicado grabado, o en su caso, la correspondencia intervenida, que tanto las cintas que contengan las grabaciones originales en su integridad como los envíos postales intervenidos sean controlados directamente por dicha autoridad, o lo que es lo mismo que a ella corresponda su audición y selección de tal manera que lo que interese al buen fin del proceso quede preservado en autenticidad e integridad hasta el momento en que deba ser incorporado como verdadera prueba al plenario. Es decir, compete al Juez la selección de las conversaciones y de la correspondencia que pueda ser de interés al proceso, al tiempo que al Secretario adverar con la fe pública la autenticidad de las grabaciones o de los envíos postales intervenidos y, en su caso, del contenido de los mismos, cotejando las trascripciones que le hayan sido facilitadas por la Policía Judicial y su coincidencia con las conversaciones grabadas[85].

---

[84] Resultan significativas en este sentido las SSTC 171/1999, FJ 13, y 205/2002, FJ 7. Esta última sentencia destaca en concreto lo siguiente: «Los imputados nunca tuvieron la oportunidad de conocer los términos de las grabaciones desechadas, quedando así en una situación de desequilibrio procesal, de manera que resultaron afectadas de forma definitiva y relevante, esto es, materialmente, las elementales exigencias del derecho de defensa y contradicción que imponen que con intervención de los afectados se incorporen a las actuaciones como elemento de debate y eventualmente de prueba, todos aquellos pasajes que se consideren precisos para sustentar las diversas hipótesis —acusatorias, de defensa— que se contraponen en la investigación para así posibilitar equitativamente el debate previo a la apertura del juicio oral y finalmente el desarrollo del propio juicio».

[85] Precisamente, la STC 205/2002, FJ 7, destaca las irregularidades de alcance constitucional afectantes al derecho al proceso con todas las garantías cuando señala, en relación con el supuesto de autos resuelto, que «en el presente caso las grabaciones resultantes de la intervención de las comunicaciones telefónicas se incorporaron al proceso por medio de su trascripción mecanográfica y de la audición de ciertos fragmentos en el acto de la vista oral. Sin embargo, dicha prueba de cargo no puede tenerse como prueba constitucionalmente lícita. Conclusión a la que debemos llegar no sólo desde la perspectiva ya examinada de actuación procesal vulneradora del derecho del art. 18.3 CE, sino también en cuanto lesiva del derecho a un proceso con todas las garantías (art. 24.2 CE). Así resulta del testimonio de las actuaciones, en las que se comprueba que

En segundo término, es preciso que, finalizada la ejecución de la medida, el sometido a ella pueda tomar conocimiento[86], no sólo de que fue adoptada respecto del mismo toda vez que por razones obvias la finalidad que aquélla persigue ha de permanecer durante su ejecución oculta al sometido a la misma[87], sino también conocer el contenido de lo grabado y poder declarar sobre las conversaciones que se escuchen, proponiendo a la autoridad encargada de su control que incluya en la selección de las conversaciones aquellos extremos que considere nece-

---

la Guardia Civil se limitó a entregar al Juzgado de Instrucción núm. 1 de Pamplona *dos cintas magnetofónicas grabadas desde las originales que reproducían las conversaciones intervenidas,* así *como una trascripción escrita de las mismas en los pasajes que el instructor policial consideró "implican los hechos investigados". Por tanto no se presentaron en el Juzgado las cintas originales. A lo que hay que añadir que el texto incorporado a las actuaciones, además de parcial, careció de la adveración del Secretario Judicial*. Tales circunstancias son suficientemente expresivas del deficiente control judicial de la prueba, pues por ninguno de los dos Jueces intervinientes en la instrucción se llegó a comprobar cuál era el contenido íntegro de las grabaciones, delegándose la selección de los pasajes relevantes, así como su trascripción, a los agentes actuantes de la Guardia Civil».

[86] En las SSTEDH de 6 de agosto de 1978, caso KLASS, y de 16 de febrero de 2000, caso AMANN, precisamente se instaba del Tribunal por los requirientes respectivos la omisión de la posible comunicación *a posteriori* a los interesados de la adopción de la medida y de lo grabado como consecuencia de la escucha realizada. El Tribunal en el primero de los casos no apreció la vulneración del art. 8, pero sí en el segundo.

[87] Sobre este punto una STS de 3 de diciembre de 1999 (RJ 9696) en la que se invocaba la vulneración del art. 18.3 de la CE con apoyo en el cauce del art. 5.4 de la LOPJ planteaba el problema de la necesaria simultaneidad de la ejecución de la medida de intervención telefónica con la de la previa resolución judicial motivada acordando el secreto de las actuaciones al amparo del art. 302 de la LECrim suscitando la parte recurrente la cuestión de que el Juez había acordado la intervención telefónica sin que previamente se hubiera declarado secreto el sumario. En respuesta a la cuestión suscitada el TS destaca lo siguiente: «La doctrina de esta Sala, recogida en las Sentencias de 5 de mayo de 1997 (RJ 3625) y 25 de septiembre de 1999 (RJ 7391), entre otras estima que en los supuestos de intervenciones telefónicas "la necesidad de no frustrar la efectividad de la medida adoptada impone la declaración de secreto desde el comienzo de las actuaciones, pues de otro modo habría de ponerse el procedimiento en conocimiento del imputado, según dispone el art. 118 de la LECrim, no siendo admisible la tesis sostenida por un sector de la práctica y la doctrina, de que la resolución por la que se acuerde la intervención telefónica lleva implícita, por su especial naturaleza, la declaración de secreto, sino que es necesario un pronunciamiento expreso. Ahora bien estas mismas Sentencias 288/1996 y 1778/1998 señalan que la infracción procesal en que se incurre por no efectuar de inmediato la declaración formal de secreto, y sin embargo mantener reservada la medida no determina por sí misma la nulidad por inconstitucionalidad de las intervenciones telefónicas, pues no conlleva necesariamente indefensión material para los imputados, siempre que éstos, como sucedió en el supuesto actual, cuando tomaron posteriormente contacto con las actuaciones pudieran conocer el alcance y resultados de la medida, adoptada en su momento del modo reservado acorde con su naturaleza, y dispusieran de la oportunidad de solicitar al respecto lo que considerasen conveniente en defensa de sus intereses».

sarios a su defensa, así como los elementos de prueba de descargo que, de alguna manera, puedan suscitar dudas al órgano de enjuiciamiento sobre la verdadera identidad del interlocutor que se escuche en la cinta obtenida.

En tercer lugar, ha de garantizarse que las grabaciones así seleccionadas queden a disposición del Tribunal que haya de enjuiciar el proceso para que, bien a solicitud de alguna de las partes, bien por propia iniciativa del mismo, se pueda en cualquier momento del plenario examinar todo o parte de lo grabado, sometiéndolo, por consiguiente, a contradicción. De todos modos, como veremos en el apartado de la valoración de la prueba, la audición de las cintas grabadas en el juicio oral no es requisito imprescindible para su ponderación como medio de prueba por parte del Tribunal de enjuiciamiento, siempre que se hayan llevado a efecto la selección y adveración en la fase de instrucción y en los términos en que han quedado indicados. Tampoco se entiende que tenga alcance constitucional el retraso en la entrega en el Juzgado de los soportes magnéticos que contengan las grabaciones de los actos de comunicación, si el imputado tiene efectiva posibilidad de su conocimiento en el trámite de instrucción y de que el Juzgado realice la selección de las que tengan relevancia de cara al proceso. Se trataría de una mera irregularidad que, por no generar indefensión material, no ocasiona vulneración de derecho fundamental alguna.

Por último, apreciada la eventual existencia de una vulneración del derecho fundamental, bien en la adopción, bien la ejecución de la medida, y, por consiguiente, declarada nula la prueba, la Ley debe establecer los mecanismos necesarios para asegurar la destrucción de todas las grabaciones así obtenidas. Lo mismo debe acontecer en aquellos supuestos en que el proceso iniciado concluya con el archivo o sobreseimiento definitivo[88] del proceso.

Hemos de referirnos, finalmente, a la exigencia de que la Ley establezca, también, unos mecanismos procesales de impugnación de la medida restrictiva del derecho[89], exigencia ésta que conecta la eventual

---

[88] STEDH de 30 de julio de 1998, caso VALENZUELA CONTRERAS contra España. En su ap. 46 IV, destaca textualmente, al referirse a las garantías mínimas para evitar el abuso en la aplicación de las medidas restrictivas del derecho señala que la Ley también deberá contener «… las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de dichas cintas, sobre todo tras un sobreseimiento o una absolución».

[89] Sobre los medios de impugnación con que puede hacerse frente a al eventual ejecución de medidas restrictivas del derecho fundamental, resulta muy importante la observancia de las instrucciones impartidas al Ministerio Fiscal por la Circular 1/99, de 29 de diciembre, Apartado V, que realiza un desarrollado estudio de la intervención del Fiscal en las diferentes fases del procedimiento.

vulneración de dicho derecho con otros como el derecho de defensa y el más amplio a un proceso con todas las garantías.

4. *Valoración como prueba*

A la hora de comenzar el estudio de este último apartado no puede olvidarse que el derecho fundamental que estudiamos se conecta con otros derechos de no menor trascendencia e importancia para el proceso penal como son los que integran en su conjunto el derecho a un proceso con todas las garantías, una de cuyas manifestaciones más relevantes, aunque no la única, es la del derecho de defensa que ha de ser respetado mediante el establecimiento de los cauces adecuados para que la persona sometida a la medida tenga la posibilidad efectiva de contradecir e impugnar *a posteriori* mediante su intervención en el proceso, la validez y eficacia de lo obtenido con las escuchas telefónicas. Y, por supuesto, el derecho a la presunción de inocencia como corolario final de todo este haz de derechos fundamentales que se conectan al secreto de las comunicaciones.

Forzosamente, no podremos detenernos en el análisis del derecho a un proceso con todas las garantías y de la presunción de inocencia[90] porque el estudio de tales temas podría ser motivo de otros trabajos igual de importantes que el que ahora se analiza. Sin embargo, tampoco podemos dejar de abordar aunque sea desde la concreta perspectiva del derecho fundamental que nos ha correspondido el análisis

---

Igualmente, resultan de interés en este punto los estudios realizados por MONTERO AROCA, J.: *La intervención de las comunicaciones telefónicas en el proceso penal*, Tirant lo Blanch, Valencia, 1999, pp. 313 y ss; TORRES MORATO, M. A.: *La Prueba ilícita penal. Estudio jurisprudencial.* Aranzadi, Pamplona, 2000, pp. 226 y ss., y, en relación con la prueba ilícita, destacar la monografía de MIRANDA ESTRAMPES, M.: *El concepto de prueba ilícita y su tratamiento en el proceso penal*, J.M. Bosch, Barcelona, 1999, pp. 123 y ss.

[90] Una de las cuestiones que suscita el tema que estudiamos y que tiene una clara incidencia en el ámbito del derecho a la presunción de inocencia alude a la negativa de los imputados a reconocer que las voces contenidas en una grabación son las suyas, así como también a la circunstancia de que las defensas de los inculpados no solicitan la prueba pericial de identificación de voces. Pues bien, a este respecto, la STS de 6 de junio de 2006 (RJ 5949) destaca textualmente que «no se trata su práctica de una exigencia de orden constitucional, sino una mera cuestión de legalidad ordinaria, que, en su caso, únicamente afectaría a la validez procesal de las pruebas obtenidas con las intervenciones intachables desde el punto de vista constitucional». Agregando más adelante a lo expuesto «que la Sala puede acudir a otros medios probatorios, distintos del reclamado, como el testimonio de los funcionarios de Policía que llevaron a cabo las observaciones telefónicas, o la percepción directa de las voces de las grabaciones y su comparación con las emitidas por los acusados en su presencia».

de dos cuestiones, a mi modo de ver, relevantes para el desarrollo completo de la materia, como son, de una parte, la conexión entre el derecho al secreto de las comunicaciones telefónicas con el derecho a un proceso justo y equitativo, y de otro las importantes consecuencias que de aquélla se pueden derivar para el derecho a la presunción de inocencia del inculpado en un proceso penal, sobre todo cuando la prueba de cargo obtenida como consecuencia directa o indirecta de las escuchas telefónicas realizadas a aquél haya sido declarada nula por vulneración de sus derechos fundamentales, con especial atención a dos cuestiones acuñadas por la Jurisprudencia Constitucional, como son, de una parte, la aceptación por parte del TC de la denominada doctrina de la «conexión de antijuridicidad» y de otro lado, el hallazgo o «descubrimiento inevitable».

A) El derecho al secreto de las comunicaciones y el derecho a un proceso justo

Desde luego, hay que partir de la idea de que con la invocación directa de los derechos fundamentales contenidos en los arts. 18.3 y 24.2 de la Constitución, junto con la norma legal contenida en el art. 11.1 de la LOPJ es evidente que, en ningún caso, una prueba declarada ilícita por haber menoscabado alguno de los derechos fundamentales ahora puestos de manifiesto debería ser admitida por cualquier Tribunal no reconociéndole eficacia alguna como tal medio de prueba, ni siquiera para servir de cobertura o apoyo a otros medios de prueba, sobre los cuáles construir después la convicción judicial para un pronunciamiento condenatorio, y todo ello por muy desvinculados que los mismos estuvieren con aquélla. Como el TC destacó en su conocida STC 114/84[91], las pruebas obtenidas violentando un derecho o libertad fundamental, no pueden ser admitidas como tales medios de prueba en el proceso penal, acarreando como consecuencia «la nulidad radical de todo acto… violatorio de las situaciones jurídicas reconocidas en la Sección Primera del Capítulo Segundo del Título I de la Constitución y de la necesidad institucional por no confirmar, reconociéndolas efectivas, las contravenciones de los mismos derechos fundamentales…». El fundamento de esta posición, como sostiene Miranda Estrampes[92] con

[91] FJ 4. Luego ha sido continuada por otras muchas posteriores, tales como las SSTC 107/85, 64/86, 80/91, 85/94, 86/95, 181/95, 49/96, 54/96, 81/98, 49/99, 167/2002, 259/05 y 261/05.

[92] Miranda Estrampes, M., *ob. cit.,* p. 63. En dicha obra cita como apoyo de su afirmación la STC 127/96, FJ 3, y la STS de 28 de octubre de 1997 (RJ 7843).

cita en la referida sentencia, no descansa en el efecto disuasor de las conductas ilegales de los agentes policiales *(deterrance effect)*, acuñada por la jurisprudencia del Tribunal Supremo Federal de los EEUU, sino en la posición preeminente que tales derechos ocupan en nuestro Ordenamiento Jurídico, según se ha encargado de reiterar el TC español en su doctrina.

De ahí que el TC agregara, a continuación, que «constatada la inadmisibilidad de las pruebas obtenidas con violación de derechos fundamentales, su recepción procesal implica una ignorancia de las garantías propias al proceso, implicando también una inaceptable confirmación institucional de la desigualdad entre las partes en el juicio, desigualdad que se ha procurado antijurídicamente en su provecho quien ha recabado instrumentos probatorios en desprecio a los derechos fundamentales de otro…»[93]

Sin embargo, se ha ido abriendo paso en nuestra Jurisprudencia, siguiendo en este sentido, a la doctrina norteamericana, determinadas matizaciones a la inicial tesis de los frutos del árbol envenenado que nuestro TC y TS habían aceptado inicialmente como instrumento sustancial en la defensa de los derechos fundamentales reconocidos por nuestra Constitución, al haber restringido las consecuencias de la ilicitud de la prueba limitándola únicamente a aquellas otras derivadas de la anterior pero unidas a ésta por una «conexión de antijuridicidad» que estudiaremos a continuación.

B) La conexión de antijuridicidad y el hallazgo inevitable

Son, como hemos anticipado, dos matizaciones a la doctrina de los frutos del árbol envenenado[94] que, primeramente, acogió el TC y posteriormente halló su plasmación legal en el vigente art. 11.1 de la LOPJ.

En materia de intervención de las comunicaciones en cuanto medida restrictiva del derecho fundamental, la doctrina del TC vino a introducir con recientes pronunciamientos[95] un conjunto de matizaciones a la inicial tesis de la nulidad radical de todo lo derivado, directa o indirectamente, de la prueba ilícita.

---

[93] FJ 5.

[94] «*The tainted fruit*» o más genéricamente, doctrina de los frutos del árbol envenenado «*the fruit of the poisonous tree doctrine*».

[95] El primero de ellos se produjo en la importante STC 81/98 y ha tenido su continuación, en lo que se atañe a los supuestos de intervención de las comunicaciones telefónicas, en las posteriores SSTC 49/99, 166/99, 171/99, 50/00, 138/01, 167/02, 184/03, 259/05 y 261/05.

Pues bien, en su STC 81/98[96], el Tribunal se plantea si los elementos de prueba en los que el órgano judicial basó su convicción acerca de la culpabilidad del recurrente, pueden ser tenidos en cuenta por ser jurídicamente independientes de la intervención telefónica declarada nula, pese a hallarse causalmente conectados con ella, o, por el contrario, ello no es posible, dada su derivación e íntima conexión causal con la escucha ilícita.

En supuestos como el examinado en la citada sentencia, es decir, en los casos en que se plantea la dependencia o independencia de determinada actividad probatoria respecto de la previa vulneración de un derecho fundamental, el Tribunal señala que, para determinar cuándo ciertas pruebas que pueden guardar una conexión causal con otra declarada ilícita, por haberse obtenido con vulneración de derechos fundamentales, deben reputarse también como ilícitas, han de observarse las siguientes exigencias:

1.ª En primer lugar, constatar si desde una perspectiva natural las pruebas de que se trate guardan o no relación alguna con el hecho constitutivo de la vulneración del derecho fundamental sustantivo, es decir, si tienen o no una causa real diferente y totalmente ajena al mismo. Pues bien, si tales medios probatorios han sido practicados al margen de toda relación natural con la prueba declarada nula y tienen una causa totalmente ajena a aquélla, los mismos tienen validez y permiten al órgano jurisdiccional la consiguiente posibilidad de valoración a efectos de enervar la presunción de inocencia.

2.ª Ahora bien, el problema surge cuando, tomando en consideración el suceso tal y como ha transcurrido de manera efectiva, la prueba enjuiciada se halla unida a la que vulneró el derecho, porque se ha obtenido a partir del conocimiento derivado de ella.

En tales casos, a la regla general de que todo elemento probatorio que pretenda deducirse a partir de un hecho vulnerador del derecho fundamental al secreto de las comunicaciones telefónicas se halla incurso en la prohibición de valoración *ex* art. 24.2 de la Constitución Española, puede admitirse la excepción de que, pese a que las pruebas de cargo se hallaren naturalmente enlazadas con el hecho constitutivo de la vulneración del derecho fundamental por derivar del conocimiento adquirido a partir del mismo, pudieran ser consideradas jurídicamente independientes de él y, en consecuencia, reconocidas por el Tribunal como válidas y aptas para enervar la presunción de inocencia. Siendo,

[96] Con anterioridad a esta STS ya se había pronunciado, en cierto modo, sobre la doctrina que ha establecido el TC. Ejemplo de ello son las SSTS 25 de enero, 18 de abril o 26 de mayo de 1997 (RJ 109, 2992 y 4133).

por ello, tales pruebas reflejas, desde un punto de vista intrínseco, constitucionalmente legítimas, porque no existe lo que el Tribunal ha dado en conocer como «conexión de antijuridicidad»[97]. En la presencia o ausencia de esa conexión reside, pues, la *ratio* de la interdicción de valoración de las pruebas obtenidas a partir del conocimiento derivado de otras que vulneran el derecho al secreto de las comunicaciones[98].

Tal conexión de antijuridicidad presupone:

> «—En primer lugar un juicio de antijuridicidad *interno*, pues, a fin de apreciar si existe o no conexión de antijuridicidad, habrán de tenerse en cuenta cuáles han sido los aspectos y características de la vulneración del derecho fundamental que determinó la declaración de ilicitud.
>
> Es decir, el juicio interno de antijuridicidad lo que debe hacer es indagar cuál de las garantías de las que se compone el derecho fundamental, en este caso el derecho al secreto de las comunicaciones, ha

---

[97] Ver sobre este particular la Circular 1/99, de 29 de diciembre de la Fiscalía General del Estado. Pueden consultarse también los interesantes trabajos sobre la misma de JUANES PECES, A.*:* «La prueba prohibida (Análisis de la STC. 49/99, de 7 de abril)», *Repertorio Aranzadi del Tribunal Constitucional*, Pamplona, 1999, Tomo II, pp. 1681 y ss.; TORRES MORATO, M. A., *ob. cit.*, pp. 213 y ss.; MONTAÑÉS PARDO, M. A.: *La presunción de inocencia. Análisis doctrinal y jurisprudencial*. Aranzadi, Pamplona, 1999, pp. 109-110; PAZ RUBIO, J. M.: *La prueba en el proceso penal. Su práctica ante los Tribunales*. COLEX, Madrid, 1999, pp. 250 y ss.

[98] En la STC 167/2002, FJ 8, se descarta, por ejemplo, que las declaraciones espontáneas de los recurrentes ante la Policía y luego ratificadas ante el Juzgado, tengan conexión de antijuridicidad con las escuchas telefónicas declaradas ilícitas, a pesar de que derivan naturalmente de éstas. Dice, a este respecto, el Tribunal lo siguiente: «La existencia de una conexión causal entre la ilícita intervención telefónica y las declaraciones prestadas con las debidas garantías por los demandantes de amparo ante la policía, y ratificadas ante el Juez de Instrucción, no impide reconocer la inexistencia de una conexión de antijuridicidad entre ambos medios de prueba, pues *tales declaraciones son jurídicamente independientes*, como ha tenido ocasión de declarar este Tribunal Constitucional en supuestos similares en relación con denunciadas infracciones del derecho a la inviolabilidad del domicilio, del acto lesivo del derecho al secreto de las comunicaciones telefónicas. *La independencia jurídica de este medio de prueba se sustenta, de un lado, en las propias garantías constitucionales que rodean su práctica* —derecho a no declarar contra sí mismo, a no confesarse culpable y a la asistencia letrada— y constituyen un medio eficaz de protección frente a cualquier tipo de coerción o compulsión ilegítima; *de otro lado, en que el respeto de dichas garantías permite afirmar la espontaneidad y voluntariedad de las declaraciones,* de forma que la libre decisión del imputado o acusado a declarar sobre los hechos que se le imputan o de los que se le *acusa permite dar por rota jurídicamente cualquier conexión causal con el acto ilícito desde una perspectiva interna**;** y desde una perspectiva externa, esta separación entre el acto ilícito y la voluntaria declaración por la libre decisión del imputado o acusado atenúa, hasta su desaparición, las necesidades de tutela del derecho material que justificaría su exclusión probatoria*, ya que la admisión voluntaria de los hechos no puede considerarse un aprovechamiento de la lesión del derecho fundamental». En el mismo sentido, las SSTC 161/1999, FJ 4, 8/2000, FJ 3, o 136/2000, FJ 8.

sido menoscabada y en qué forma[99]. Y, en función de la gravedad de tales infracciones habrá de determinarse si las pruebas derivadas de una intervención telefónica declarada nula, obligan también a declarar la nulidad de dichas pruebas derivadas.

—Y, en segundo término, ha de llevarse a efecto también un juicio *externo* de antijuridicidad que ha de constatar si las necesidades esenciales de tutela que exige el derecho fundamental vulnerado por la práctica de la prueba ilícita conllevan o no también que la declaración de nulidad se extienda o no a las pruebas derivadas. Es decir, que en ocasiones aún cuando no pudiera apreciarse la existencia de una conexión causal entre la prueba ilícita y la prueba derivada, la infracción del derecho al secreto de las comunicaciones es de tal entidad que la necesidad de tutelarlo impone indefectiblemente la nulidad de la prueba derivada.

Ambas perspectivas, interna y externa —como sostiene el TC— son complementarias, pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo cabrá entender que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los aspectos que configuran el contenido del derecho fundamental sustantivo»[100].

Concluye, finalmente, su doctrina el Tribunal indicando que la determinación de la existencia del nexo de antijuridicidad entre la prueba declarada ilícita y la derivada constituye «un juicio de experiencia» que corresponde emitir en exclusiva a los Tribunales ordinarios, sin perjuicio del control que sobre la razonabilidad del mismo pueda efectuar el propio TC.

Desde luego, esta doctrina[101] no ha dejado de plantear dudas e interrogantes que, en definitiva, podrían afectar a la virtualidad y eficacia de los derechos fundamentales puestos en juego, pues todas las cuestiones pueden resumirse en una sola: ¿Hasta qué punto puede no considerarse, por ejemplo, una prueba derivada causalmente de la intervención telefónica previa el seguimiento policial efectuado a un sujeto al que, en un momento determinado se le detiene y se le ocupa la droga que se sabía se encontraba en aquel momento en su poder porque había sido

---

[99] Es decir, se trata de constatar si lo que se infringieron fueron los presupuestos exigidos para la adopción de la medida (carencia de autorización judicial, etc.), el control judicial de la misma o las exigencias de proporcionalidad en los términos que hemos estudiado anteriormente.

[100] STC 49/99,. FJ 14.

[101] Pueden consultarse, en este sentido, los atinados comentarios que realiza Miranda Estrampes, M., *ob. cit.*, pp. 119 y ss.

objeto de seguimiento precedente y había tenido intervenido el teléfono que utilizaba habitualmente? Tal caso que no es hipotético sino que, muy resumidamente, es objeto de enjuiciamiento por el Tribunal en su STC 171/99, fue resuelto en el sentido de que, si bien el Tribunal apreció la vulneración del derecho al secreto de las comunicaciones, no estimó vulnerado, en cambio, ni los derechos a un proceso con todas las garantías y a la presunción de inocencia, porque consideró que el acto de la aprehensión de la droga era jurídicamente independiente de la escucha telefónica a la que había sido sometido el sujeto.

Finalmente, una vertiente de la doctrina ahora afirmada sobre la eventual validez y eficacia de los medios probatorios derivados aunque no conectados con la prueba originaria ilícita es la del denominado por la jurisprudencia americana «*hallazgo inevitable*»[102], esto es aquél elemento probatorio que se habría obtenido indefectiblemente aún cuando no se hubiere llevado a cabo la intervención telefónica ilegal, por no hallarse conectado causalmente con aquélla o porque dicho medio de prueba habría iniciado su andadura procesal con anterioridad a la intervención.

Fue el TS el que inicialmente abordó esta última cuestión en diversas resoluciones[103] relacionadas la gran mayoría de ellas con delitos contra la salud pública en los que la detención de los autores y la aprehensión de la droga, tuvieron lugar al margen de la intervención telefónica declarada nula y posteriormente también el TC a partir de la ya citada STC 81/98, aunque explícitamente no ha aludido al mismo.

En los casos en que el TS ha tenido ocasión de abordar esta cuestión se parte de una absoluta certeza «presumida» de que la averiguación de los hechos se produjo al margen de lo obtenido de las escuchas telefónicas. En algún caso[104] conecta el descubrimiento inevitable con la exigencia de que las actuaciones policiales hayan sido realizadas de buena fe por parte de los agentes, tesis ésta que, como sostiene, a mi entender con toda razón, Miranda Estrampes[105], no se compadece con

---

[102] Analizado, también, con detenimiento por Miranda Estrampes, M., *ob. cit.,* pp. 119 y ss. respecto del que no ahorra tampoco comentarios críticos a su admisión dentro del proceso penal español, por sus eventuales contradicciones con la posición de preeminencia que los derechos fundamentales tienen en nuestro ordenamiento jurídico y por sus más que probables vulneraciones del derecho a la presunción de inocencia. Puede consultarse también a Martín Pallín, J. A.: «Escuchas telefónicas», *Homenaje a D. Enrique Ruiz Vadillo*. COLEX, Madrid, 1999, pp. 394 y ss., y Paz Rubio, J. M., *ob. cit.,* pp. 249 y ss.

[103] SSTS de 18 de febrero de 1994 (RJ 2314), 5 de junio de 1995 (RJ 4538), 26 de mayo, 4 de julio y 23 de septiembre de 1997 (RJ 4133, 6008 y 7259) y de 24 de enero y 20 de febrero de 1998 (RJ 88 y 1181).

[104] Como así lo pone de manifiesto la STS de 4 de julio de 1997 (RJ 6008).

[105] Miranda Estrampes, M., *ob. cit*., p. 120.

el fundamento que sí existe en la jurisprudencia americana del efecto disuasor de las conductas ilegales de los agentes policiales[106], pero sobre el que no reposa, según la jurisprudencia del TC, la doctrina de los derechos fundamentales reconocidos por nuestra Constitución, a los que aquélla les ha otorgado un lugar preferente dentro del ordenamiento jurídico. Además, la construcción se apoya sobre verdaderas «aguas movedizas», porque únicamente puede contar con los juicios hipotéticos, las meras suposiciones o las conjeturas difícilmente conciliables con el derecho a la presunción de inocencia. Yo añadiría aún más, también resulta contradictorio con el concepto del derecho al proceso justo que señala el art. 6.1 del CEDH y, por ende, con el derecho a un proceso con todas las garantías, generador de verdadera indefensión para el inculpado, pues en la práctica construye auténticas presunciones judiciales *iuris et de iure* que no responden a ningún fundamento racional ni lógico.

IV. **El secreto de las comunicaciones en el ámbito penitenciario**

Aunque muy brevemente, el estudio del derecho al secreto de las comunicaciones y la posición doctrinal que el TC ha establecido para el mismo quedaría huérfano si no se dedicara este último capítulo a reflejar la jurisprudencia acuñada por el Tribunal en relación con el derecho al secreto de las comunicaciones de los ciudadanos recluidos en un centro penitenciario y los requisitos que deben cumplir los acuerdos o medidas de intervención de las mismas.

Hay que decir, al respecto, que el Tribunal ha creado un cuerpo de doctrina uniforme[107] sobre el reconocimiento de este derecho y su limitación dentro de los centros penitenciarios, siendo las notas características de esta doctrina las siguientes:

1.ª En primer lugar, el marco normativo constitucional del derecho al secreto de las comunicaciones de que puede gozar una persona interna en un centro penitenciario viene determinado, no sólo por lo dispuesto en el art. 18.3 CE —que garantiza el derecho al secreto de las comunicaciones, salvo resolución judicial—, sino también y primordialmente por el art. 25.2 CE, precepto que en su inciso segundo establece que «el

---

[106] *Deterrence effect.*

[107] Pueden consultarse en este sentido las SSTC 183/1994, 127/1996, 170/1996, 128/1997, 175/1997, 200/1997, 58/1998, 141/1999, 188/1999, 175/2000, 106/2001, 193/2002, 194/2002 y 169/2003, así como el ATC 54/1999, entre otras resoluciones.

condenado a pena de prisión que estuviera cumpliendo la misma gozará de los derechos fundamentales de este Capítulo, a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria». Así pues, el Tribunal ha destacado que «la persona recluida en un centro penitenciario goza, en principio, del derecho al secreto de las comunicaciones, aunque puede verse afectada por las limitaciones expresamente mencionadas en el art. 25.2 CE»[108], refiriéndose, en concreto, a tres tipos de limitaciones: En primer lugar, las que provengan del propio fallo condenatorio, es decir del sentido en que se haya manifestado el Tribunal sentenciador teniendo en cuenta el delito que haya sido cometido por el interno. En segundo lugar, las propias limitaciones derivadas de la pena que tenga que cumplir y que en determinados casos puede acarrear la prohibición de comunicarse con determinadas personas. Y, por último, las propiamente derivadas de la legislación penitenciaria como consecuencia de la relación de sujeción especial que une a todo interno con la Administración Penitenciaria.

2.º En segundo término, el art. 51 LOGP reconoce el derecho de los reclusos a las comunicaciones, diferenciando el propio precepto, en cuanto al ejercicio de tal derecho, entre varias modalidades de comunicación, que son de muy diferente naturaleza y vienen, por ello, sometidas a regímenes legales claramente diferenciados. Por lo que se refiere a las limitaciones que pueden experimentar las denominadas comunicaciones genéricas que regulan los arts. 51.1 LOPG y concordantes del Reglamento Penitenciario de 1996 (art. 47), esto es, las que los internos pueden celebrar con sus familiares, amigos y representantes de organismos internacionales e instituciones de cooperación penitenciaria, el citado art. 51.1 LOGP, además de mencionar los casos de incomunicación judicial, impone que tales comunicaciones se celebren de manera que se respete al máximo la intimidad, pero autoriza que sean restringidas por razones de seguridad, de interés del tratamiento y del buen orden del establecimiento, permitiendo el art. 51.5 LOGP que tales comunicaciones sean intervenidas motivadamente por el Director del centro penitenciario, dando cuenta a la autoridad judicial competente.

Por tanto, como destaca el Tribunal, «el citado precepto legal permite la intervención de las denominadas comunicaciones genéricas por razones de seguridad, interés del tratamiento y del buen orden del establecimiento, configurándose tales supuestos, por lo tanto, como cau-

[108] SSTC 170/1996, FJ 4, 175/1997, FJ 2, 200/1997, FJ 2, 175/2000, FJ 2 y 3, y 106/2001, FJ 6.

sas legítimas para ordenar la intervención de las comunicaciones de un interno».

Quedan excluidas, sin embargo de este régimen, no sólo por así establecerlo expresamente el apartado 2.º del art. 51 LOGP y el art. 48 del RP que ahora estudiamos, sino también por interpretación que ha hecho del mismo la doctrina constitucional las comunicaciones orales, escritas o por medio de aparatos de telefonía entre un interno y su letrado defensor o aquél que sea expresamente llamado por el mismo en relación con asuntos penales, en cuyo caso, sólo es posible la limitación del derecho cuando se den acumulativamente dos requisitos: Autorización judicial motivada, con una motivación especialmente reforzada, y cuando además se persiga un delito de terrorismo. Ambos requisitos tienen que darse para que pueda autorizarse esta limitación, pues en estos casos, como ha destacado el Tribunal, está en juego no sólo el derecho al secreto de las comunicaciones sino también el ejercicio efectivo del derecho de defensa[109].

---

[109] La STC 183/1994 (FJ 5) es muy gráfica y clara al respecto: «El art. 51 de la LOGP, distingue entre las comunicaciones, que podemos calificar de generales, entre el interno con determinada clase de personas —art. 51.1— y las comunicaciones específicas, que aquél tenga con su Abogado defensor o con el Abogado expresamente llamado en relación con asuntos penales (art. 51.2); la primera clase de comunicaciones viene sometida al régimen general del art. 51.5, que autoriza al Director del Centro a suspenderlas o intervenirlas "por razones de seguridad, de interés del tratamiento y del buen orden del establecimiento", según precisa el art. 51.1, mientras que las segundas son sometidas al régimen especial del art. 51.2, cuya justificación es necesario encontrar en las exigencias y necesidades de la instrucción penal, a las cuales es totalmente ajena la Administración Penitenciaria que no tiene posibilidad alguna de ponderar circunstancias procesales que se producen al margen del ámbito penitenciario.Este carácter de régimen singular, que para las comunicaciones con el Letrado establece el art. 51.2, se prolonga más allá de la Ley,… en el que las comunicaciones orales con el Abogado se regulan en Sección distinta de la dedicada a las comunicaciones del régimen general y en el que, al tratar de las comunicaciones escritas, con el Abogado,… "no tendrán otras limitaciones que las establecidas en el punto 2 del art. 51 de la Ley General Penitenciaria". Esta diferenciación esencial que existe entre el art. 51.5 —régimen general cuya única remisión válida es al art. 51.1— y el art. 51.2, pone de manifiesto la imposibilidad constitucional de interpretar este último precepto en el sentido de considerar alternativas las dos condiciones de "orden de la autoridad judicial" y "supuestos de terrorismo", que en el mismo se contienen, así como derivar de ello la legitimidad constitucional de una intervención administrativa que es totalmente incompatible con el más intenso grado de protección que la norma legal confiere al derecho de defensa en los procesos penales. *Dichas condiciones habilitantes deben, por el contrario, considerarse acumulativas* y, en su consecuencia, llegarse a la conclusión que el art. 51.2 de la LOGP autoriza únicamente a la autoridad judicial para suspender o intervenir, de manera motivada y proporcionada, las comunicaciones del interno con su Abogado sin que autorice en ningún caso a la Administración Penitenciaria para interferir esas comunicaciones».

3.ª En cuanto a los requisitos que deben de cumplir los Acuerdos o medidas de intervención de las comunicaciones genéricas, junto a la exigencia de motivación y de dar cuenta a la autoridad judicial competente que impone el art. 51.5 LOGP, así como la de notificación al interno afectado que establecen los arts. 43.1 y 46.5 RP de 1996, el Tribunal ha añadido la necesidad de preestablecer un límite temporal a la medida de intervención[110].

En todo caso, en relación con este límite temporal de la medida de intervención, el TC recuerda que el mantenimiento de una medida restrictiva de derechos como la analizada, «más allá del tiempo estrictamente necesario para la consecución de los fines que la justifican podría lesionar efectivamente el derecho afectado»[111], pues los arts. 51 y 10.3 LOGP y 41 y ss. RP de 1996 llevan implícita la exigencia del levantamiento de la intervención en el momento en que deje de ser necesaria por cesación o reducción de las circunstancias que la justificaron, en cuanto se justifica exclusivamente como medida imprescindible por razones de seguridad, buen orden del establecimiento o interés del tratamiento. Por todo ello, el TC ha venido exigiendo que, «al adoptarse la medida de intervención de las comunicaciones, se determine el período de su vigencia temporal, aunque para ello no sea estrictamente necesario fijar una fecha concreta de finalización, sino que ésta puede hacerse depender de la desaparición de la condición o circunstancia concreta que justifica la intervención». El Acuerdo puede, pues, en determinados casos sustituir la fijación de la fecha por la especificación de esa circunstancia, cuya desaparición pondría de manifiesto que la medida habría dejado de ser necesaria[112].

4.ª Respecto al requisito de la doble notificación o comunicación de la medida, esto es al Juzgado de Vigilancia y al propio interno, el Tribunal ha declarado que «la notificación de su adopción al interno en nada frustra la finalidad perseguida, ya que la intervención tiene fines únicamente preventivos, no de investigación de posibles actividades delictivas para lo que se requeriría la previa autorización judicial, a la vez de que supone una garantía para el interno afectado»[113].

Además, la necesidad legal de la comunicación de la medida adoptada a la autoridad judicial competente ha de ser inmediata, con el objeto de que ésta ratifique, anule o subsane la decisión administrativa, es

---

[110] Así lo destacan en este extremo las SSTC 128/1997, FJ 4, 175/1997, FJ 3 y 4, 200/1997, FJ 3, 188/1999, FJ 5, 175/2000, FJ 3, 106/2001, FJ 6, y 194/2002, FJ 6.

[111] SSTC 206/1991, FJ 4, y 41/1996, FJ 2.

[112] Ver en este sentido las SSTC 170/1996, FJ 4, 175/1997, FJ 4, 200/1997, FJ 4, 141/1999, FJ 5, y ATC 54/1999.

[113] SSTC 200/1997, FJ 4, y 194/2002, FJ 6.

decir, ejerza con plenitud su competencia revisora sobre la restricción del derecho fundamental, articulándose, pues, como una auténtica garantía con la que se pretende que el control judicial de la intervención administrativa no dependa del eventual ejercicio por el interno de los recursos procedentes. Como dice gráficamente el Tribunal «rectamente entendida esta dación de cuentas a la autoridad judicial competente implica, no sólo la mera comunicación del órgano administrativo al órgano judicial para conocimiento de éste, sino un verdadero control jurisdiccional de la medida efectuado "a posteriori" mediante una resolución motivada»[114].

A esta solución llega, no sólo de una necesaria consideración sistemática del art. 51.5 LOGP con los arts. 76.1 y 2 g) y 94.1 de la misma, conforme a los cuales corresponde al Juez de Vigilancia Penitenciaria salvaguardar los derechos fundamentales de los internos que cumplen condena, sino, igualmente, del art. 106.1 CE, por el que la Administración Penitenciaria está sujeta al control judicial de la legalidad de su actuación. A ello hay que añadir, para valorar en toda su dimensión la importancia de esta medida, que el recluso puede ponerse en comunicación con ciudadanos libres, a los que también les afecta el acto administrativo de intervención. «Por todo ello resulta claro que, si la autoridad judicial competente se limitara a una mera recepción de la comunicación del acto administrativo en el que se acuerda intervenir las comunicaciones y adoptase una actitud meramente pasiva ante la restricción por dicho acto del derecho fundamental del recluso, no estaría dispensando la protección del derecho en la forma exigida»[115].

5.ª Por último, la exigencia de motivación de la medida no sólo se convierte *ex* art. 51.5 LOGP en presupuesto habilitante de toda restricción del derecho al secreto de las comunicaciones, sino que, aunque faltase esa precisión legal, su concurrencia vendría exigida por la propia Constitución, ya que su ausencia o insuficiencia afecta al propio derecho fundamental en la medida en que sin ella el recluso que ve limitado el ejercicio de un derecho desconoce la razón de esa restricción y los órganos judiciales encargados de efectuar el control relativo a la necesidad, idoneidad y proporcionalidad de la medida carecen de datos indispensables para llevar a cabo esta tarea, que es el objeto principal del control jurisdiccional. En este sentido, la jurisprudencia constitucional ha insistido en la importancia y necesidad de la motivación de la medida de intervención, no sólo porque ello permite acreditar las razones que justifican

[114] STC 106/2001, FJ 6.

[115] Así lo han declarado, entre otras, las SSTC 141/1999, FJ 5, y 188/1999, FJ 5, entre otras.

la medida de restricción del derecho, sino, además, porque constituye el único medio para constatar que la ya limitada esfera jurídica del ciudadano interno en un centro penitenciario no se restringe o menoscaba de forma innecesaria, inadecuada o excesiva.

El Tribunal ha señalado, además, que el contenido de la motivación ha de extenderse, primero, a la especificación de cuál de las finalidades legalmente previstas —seguridad, buen orden del establecimiento e interés del tratamiento— es la perseguida con la adopción de la medida y, segundo término, a la explicitación de las circunstancias que permiten concluir que la intervención resulta adecuada para alcanzar la finalidad perseguida.

Respecto a este último requisito, el TC ha declarado:

> «la individualización de las circunstancias del caso, e incluso de la persona del interno, no significa que dichas circunstancias deban ser predicables única y exclusivamente del interno afectado por la medida, o que si se trata de características comunes que concurren en un grupo de personas no puedan aducirse como causa justificativa de la intervención. Individualizar no significa necesariamente destacar rasgos que concurran exclusivamente en el recluso afectado. Puede tratarse de unos rasgos comunes a los pertenecientes a ese colectivo o a una organización; en estos casos lo que debe individualizarse es esa característica común que a juicio de la Administración penitenciaria justifica en el supuesto concreto la adopción de la medida»[116].

En lo referente a los aspectos formales de la motivación, cuya finalidad sigue siendo hacer posible el control jurisdiccional de la medida, el acuerdo que adopte la Administración Penitenciaria ha de contener los datos necesarios para que el afectado y posteriormente los órganos judiciales puedan llevar a cabo el juicio de idoneidad, necesidad y proporcionalidad, aunque no resulta exigible que en el mismo se exprese ese triple juicio por parte de la Administración, pues los referidos datos pueden completarse con los que de forma clara y manifiesta estén en el contexto en el que se ha dictado el acuerdo.

V. **Conclusión**

Como en tantas otras ocasiones, hay que volver a insistir en que no puede seguirse aplicando una serie de medidas limitativas de derechos fundamentales apoyándose exclusivamente en una doctrina jurispru-

[116] STC 106/2001, FJ 6.

dencial que puede ser cambiante, cuanto lo que realmente falta es que el legislador asuma su responsabilidad y establezca una normativa detallada y específica sobre los diferentes problemas que la práctica forense diaria nos depara.

Serían muchas las conclusiones a extraer de todo este trabajo, pero nos quedamos con una sola que aglutina a todas las demás, la de la necesidad de seguir sosteniendo que el principio de seguridad jurídica exige a todas luces una respuesta legislativa a esta insuficiente normativa procesal.

El levantamiento de la carga de la prueba en Internet: ¿ficción o realidad?

Carolina Sanchís Crespo
Profesora Titular de Derecho Procesal. Universidad de Valencia

Antes de comenzar

Quiero agradecer a las personas encargadas de organizar estas *IV Jornadas de Derecho Penal en homenaje a José María Lidón*, la oportunidad que me han brindado permitiéndome participar en ellas.

Me complace haber podido asistir y ser partícipe ahora en la publicación de sus resultados. Y ello por un doble motivo.

El primero y principal es rendir un pequeño tributo póstumo a un magistrado que perdió su vida, sin posibilidad de defensa ni de garantía procesal alguna a la que acogerse. No tuve la fortuna de conocerle, pero me consta que mientras vivió se ocupó de que otras personas gozaran de los beneficios que el estado de Derecho otorga a los justiciables y que a él le fueron injustamente hurtados. Celebro contribuir de esta manera a que su memoria siga viva.

En segundo lugar, la temática de las Jornadas —Delito e Informática: algunos aspectos— me permite dedicarme a un asunto que me resulta siempre gratificante: la interacción entre el Derecho Procesal y la Informática. Asimismo he podido compartir las experiencias de jueces, fiscales, policía y profesores universitarios que vienen dedicando sus esfuerzos profesionales a la aprehensión de esta poliédrica realidad.

Por todo ello quede, pues, constancia escrita de mi gratitud al profesor Dr. Norberto de la Mata y a la fiscal Ilma. Sra. D.ª Carmen Adán, codirectores de las Jornadas.

I. Planteamiento del tema

Una de las cuestiones más relevantes en la interacción entre proceso penal e informática es la relativa a la prueba. La lectura de sentencias en las que se aborda esta materia, así como las impresiones que he podido intercambiar con los operadores jurídicos, han confirmado esta apreciación personal.

La elección del tema que motiva estas páginas responde a la constatación de que en el medio informático y, especialmente en Internet, se asiste actualmente a una impunidad *de facto* de cierta clase de delincuencia, que cuando finalmente es juzgada, suele ser absuelta. De los casos que he tenido oportunidad de seguir y de las sentencias que he leído, se desprende un plus de dificultad probatoria cuando el delito se ha cometido con el concurso de la Red.

Se ha dicho autorizadamente que «se puede tener razón pero, si no se demuestra, no se alcanzará procesalmente un resultado favorable»[1].

Este resultado procesal favorable no es otro para el acusador, que la sentencia condenatoria y para ello, se hace imprescindible levantar la carga de la prueba desvirtuando la presunción de inocencia de la que goza todo acusado.

Lo relevante para el acusador no será tener razón o contar la verdad histórica, sino probar las acusaciones realizadas más allá de toda duda razonable. Ello no significa que a través del proceso no pueda satisfacerse la legítima aspiración a la justicia de los ciudadanos. Lo que pretendo poner de manifiesto es la falibilidad del juicio humano, que ante la imposibilidad material de saber qué es lo que realmente sucedió, debe conformarse con el resultado que la prueba arroje sin confundirlo con la verdad histórica con la que puede o no coincidir[2].

Pretendo, a lo largo de las páginas que siguen, poner el acento en esa específica dificultad probatoria antes aludida y apuntar alguna posible solución en aras a conseguir un proceso penal respetuoso con la presunción de inocencia, pero también eficaz.

II. **Presunción de inocencia y carga de la prueba**

El art. 24.2 de nuestra Constitución consagra el derecho de los ciudadanos a la presunción de inocencia[3]. Partiendo de que la expresión

---

[1] MONTERO AROCA, J. en MONTERO AROCA, J. / GÓMEZ COLOMER, J.L. / MONTÓN REDONDO, A. / BARONA VILAR, S.: *Derecho Jurisdiccional II. Proceso Civil*, Tirant lo Blanch, Valencia, 2004, p. 245.

[2] En el momento de escribir estas líneas están juzgándose los hechos que dieron lugar al terrible atentando terrorista del 11 de marzo de 2004 en Madrid. En un macro juicio como ése, creo que se hace palpable la distancia que puede mediar entre la verdad histórica y su prueba.

[3] El art. 11.1 de la Declaración Universal de los Derechos Humanos de 1948, el art. 6.2 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales de 1950 y el art. 14.2 del Pacto Internacional de Derechos Civiles y Políticos de 1966, reconocen este derecho fundamental.

es poco afortunada[4], puede decirse sintéticamente que el derecho a la presunción de inocencia supone que cualquier ciudadano debe ser considerado inocente hasta que no se declare lo contrario en sentencia condenatoria y ésta devenga firme.

La presunción de inocencia supone entonces[5]:

1.º La existencia de un verdadero principio que debe conformar toda la regulación del proceso por el legislador ordinario. Ello impone que a lo largo del proceso la parte pasiva debe ser tratada y considerada como inocente.
2.º Que el acusado no necesita probar nada, siendo toda la prueba de cuenta de los acusadores, de modo que si falta la misma ha de dictarse sentencia absolutoria.
3.º Que la prueba capaz de desvirtuar la presunción ha de ser válida y de cargo. Esto es, debe ser prueba llevada a cabo en la fase de juicio oral, realizada con observancia de las normas constitucionales y legales que regulan la admisibilidad de los medios de prueba y su práctica. Finalmente, debe dar un resultado en contra del acusado.
4.º Una íntima conexión con la motivación de las sentencias, cumpliendo, así, dos finalidades complementarias; hacer públicas las razones de la decisión adoptada y permitir su posible control por medio de los recursos. La motivación supone que han de ir poniéndose en relación los medios de prueba con los hechos que en la sentencia se estiman probados, de modo que cada afirmación que por el juez sentenciador se haga con relación a éstos, cuente con el soporte de un medio concreto de prueba.

Como puede apreciarse, el derecho a la presunción de inocencia se vincula estrechamente con la normativa de carga de la prueba.

Desde el punto de vista de un proceso dispositivo es perfectamente asumible la configuración formal de que la carga de la prueba recae,

---

[4] En primer lugar, no se trata de una presunción sino más bien de una afirmación puesto que en ella no encontramos los elementos comunes a las presunciones. En segundo lugar, la expresión tradicionalmente acuñada de «presunción de inocencia» resulta en sí misma contradictoria. En efecto, si lo que intenta ponerse de relieve es la inocencia de la persona hasta que su culpabilidad no quede fehacientemente demostrada, referirse a ese estado de inocencia como presuntivo, es de entrada, restarle credibilidad, cuando de lo que se trata, precisamente, es de poner el acento en lo contrario.

[5] Montero Aroca, J.: *Principios del proceso penal, una explicación basada en la razón*. Tirant lo Blanch, Valencia, 1997, pp. 152 a 156.

como regla general, sobre el que alega[6]. Así lo establece el art. 217.2 LEC[7].

La situación en el proceso penal es distinta puesto que se rige por principios y reglas conformadoras diferentes a las del proceso civil.

No es posible hablar de reparto de papeles probatorios entre las partes en el sentido del proceso civil, aunque sí podría asumirse cierto reparto de la carga probatoria cuando la defensa alega hechos impeditivos o extintivos, de modo que la prueba del hecho criminal imputado y de la participación en él del acusado, es carga probatoria de los acusadores y «los hechos o extremos que eliminen la antijuridicidad, la culpabilidad o cualquier otro elemento excluyente de la responsabilidad por los hechos típicos que se probaren como por él cometidos», corresponden al acusado (SSTS de 4 de febrero de 1995 y 9 de febrero de 1995)[8].

Así pues, en el momento de dictar sentencia el juez valorará la prueba y se encontrará respecto a ella en una de estas cuatro situaciones:

1.º Los hechos alegados por los acusadores han sido convincentemente probados, en cuyo caso procede dictar sentencia condenatoria
2.º Concurriendo la situación anterior, la parte acusada prueba hechos impeditivos, extintivos o excluyentes. Debe dictarse, entonces, sentencia absolutoria
3.º La parte acusadora no ha probado los hechos alegados. Debe dictarse sentencia absolutoria
4.º La parte acusadora no ha probado convincentemente los hechos alegados, ni la acusada hechos impeditivos, extintivos o excluyentes.

Es en la última situación donde la aplicación del principio *in dubio pro reo*, soluciona la incertidumbre. Dado que el juez tiene la obligación de resolver, en caso de que tras la actividad probatoria conforme a ley subsista la duda, se resolverá ésta en forma de sentencia absolutoria, esto es, a favor del acusado.

El principio *in dubio pro reo* no forma parte de la presunción de inocencia, sino que debe de ser incardinado en la valoración de la prueba.

---

[6] Barona Vilar, S., en Montero Aroca, J. / Gómez Colomer, J.L. / Montón Redondo, A. / Barona Vilar, S.: *Derecho Jurisdiccional III. Proceso Penal*, Valencia, 2002, p. 293.

[7] Según este precepto «Corresponde al actor y al demandado reconviniente la carga de probar la certeza de los hechos de los que ordinariamente se desprenda, según las normas jurídicas a ellos aplicables, el efecto jurídico correspondiente a las pretensiones de la demanda y de la reconvención».

[8] Barona Vilar, *ob. cit.,* p. 294.

La presunción de inocencia como derecho fundamental, exige la existencia objetiva de actividad probatoria de cargo para que quede desvirtuada, mientras que la regla *in dubio pro reo* presupone esa actividad y atiende al problema subjetivo del juez en la valoración de la prueba, ordenándole que en caso de duda sobre la culpabilidad del acusado se incline por la absolución[9].

En cualquier caso, la interrelación entre presunción de inocencia y el *in dubio pro reo* es evidente, cuando sí haya existido actividad probatoria pero ésta haya resultado insuficiente.

III. **Dificultades probatorias en Internet**

Cuando se trata de aplicar la normativa de carga de la prueba en un proceso penal en el que la comisión de los hechos esté vinculada a la Red, hacen acto de presencia una serie de dificultades añadidas. Tanto da que se trate de delitos puramente informáticos, que serían aquéllos que sólo pueden realizarse con la concurrencia de ordenadores, como que sean delitos tradicionales en su vertiente tecnológica[10]. Lo común en ambos casos es la clase de actividad que debe desplegarse para desvirtuar la presunción de inocencia y, en concreto, para hacer creíbles los hechos de la acusación más allá de toda duda razonable.

En más de una ocasión tal actividad resultará insuficiente.

Como ejemplo de lo expuesto paso a referirme a un caso real. El juzgado en la sentencia 110/2005 del JP n.º 1 de Madrid, de 29 de julio.

1. *Sentencia 110/2005 del JP n.º 1 de Madrid, de 29 de julio*

Los hechos que dieron lugar a esta sentencia son, en esencia, los siguientes.

—Se inician unas actuaciones por atestado instruido por la Dirección General de la Guardia Civil, Departamento de Delitos de Alta Tecnología, Unidad Central Operativa en fecha 23 de mayo de 2001.

—Tras la oportuna instrucción se acusa de un delito de daños y continuado de daños y de un delito de descubrimiento y revelación de

[9] Montero Aroca, J., en Montero Aroca, J. / Gómez Colomer, J.L. / Montón Redondo, A. / Barona Vilar, S.: *Derecho Jurisdiccional I. Parte General*, Tiranr lo Blanch, Valencia, 2003, p. 371.

[10] En cualquier caso con conexión a Internet.

secretos y continuado de descubrimiento y revelación de secretos a J.C.T.

—Son parte en el juicio oral el Ministerio Fiscal y como acusación particular la Tesorería General de la Seguridad Social, el Partido Popular y la Universidad de Santiago de Compostela.

—Se declara probado expresamente que durante los meses de mayo y agosto de 2001, el acusado desde el ordenador de su propiedad e instalado en su domicilio, accedió al sistema informático de la Dirección General del Tesoro y Política Financiera del Ministerio de Economía y Hacienda y a ABC Prensa Española S.A., sin que se haya acreditado que causase daños con dicho acceso.

—En dicho ordenador personal del acusado se encontró información de distintas empresas entre las que se hallan Dun Bradstreet España, S.A, Partido Popular, Telefónica Publicidad e Información S.A., El Corte Inglés, S.A., Dirección General del Tesoro y Política Financiera del Ministerio de Trabajo y Asuntos Sociales y Universidad de Santiago de Compostela.

—No resulta probado que el acusado haya accedido a los sistemas informáticos de esas empresas para la obtención de dicha información, ni que las mismas sufriesen daños por la acción del acusado, ni que se revelase la información a terceros.

Al margen de una cuestión previa que suscita la defensa por una supuesta vulneración del derecho fundamental a la inviolabilidad de las comunicaciones que la juzgadora desestima[11], todo el entramado probatorio que la sentencia va desgranando, pone de manifiesto la volatilidad de la prueba cuando ésta se mueve en un medio como Internet.

En efecto, los hechos que se consideran probados lo son, porque el propio acusado en sucesivas declaraciones, incluida la que se efectúa

[11] Se refiere a la solicitud remitida por la Guardia Civil a la Sociedad IRC Hispano para que les transmitiesen los datos registrados en dicha sociedad y referidos al apodo y al e-mail de los que se tenía constancia, en virtud de las diligencias preliminares, que había utilizado el acusado para sus accesos a las páginas web. Los datos que proporcionó la citada sociedad fueron meramente tres reseñas de identificación de los contactos verificados al *chat*, con indicación de los días y las horas. Se trata de códigos alfanuméricos, carentes por sí mismos de virtualidad para identificar al usuario del *chat* y para identificar a las personas o titulares con los que conectó en dichas ocasiones. Concluye la Magistrado que, en definitiva, el suministro de estos datos a la Guardia Civil, no puede ser calificado de interceptación o intromisión en una comunicación, en la medida en que no proporcionan datos relativos a los sujetos que entraron en comunicación, ni a los números de teléfono que se pusieron en contacto, ni muchos menos, al contenido de lo comunicado, tratándose meramente de datos relativos a la facturación o al control del tráfico generado en dicho *chat*.

como prueba en el juicio oral, así los reconoce. El resto queda en una incertidumbre probatoria, a pesar de los esfuerzos realizados para paliar esta situación.

El acusado reconocía haber accedido a la página web del Ministerio de Economía y Hacienda y a la del periódico ABC, afirmando que dejaba una nota para que subsanaran el error, poniendo su *nick* y correo electrónico, con la idea de que se pusieran en contacto con él. Se trataba, siempre según el acusado, de demostrar que se encontraban en situación vulnerable, de modo que los encargados del servidor subsanaran el error. En ningún momento reconoció haber borrado el documento por el que se le achacan los daños. Respecto a todos los ficheros que se encontraron en su ordenador pertenecientes a las empresas *supra* citadas, el acusado afirma que los tenía porque se los había bajado de una red de *chats* internacionales.

Así las cosas, la declaración de los agentes de la Guardia Civil es, a decir de la Magistrado, enormemente esclarecedora y suministra las dudas razonables que impiden formar la convicción judicial.

Los agentes son preguntados con relación al acceso a los sistemas informáticos de las empresas y respecto a la información contenida en el ordenador del acusado. En ambos casos no puede determinarse fehacientemente. Para hacerlo sería necesario disponer de los *logs*, cosa que no sucede siempre pues se trata de archivos antiguos y tales datos habían sido borrados. Al mismo tiempo la posibilidad de que el acusado hubiera dispuesto de la información a partir de una red de *chats* internacionales es real. Obviamente no es carga del acusado justificar cómo consiguió esos datos, sino de la acusación probar que lo hizo de modo ilegal.

Respecto de los daños, no pudieron peritarse adecuadamente porque no se tuvo acceso a los ordenadores o datos informáticos. No se remitió soporte informático alguno y por ello no se analizó ningún dato digital que permitiese a los expertos referir ningún daño.

En estas condiciones, la Magistrado considera que carece de la certeza suficiente para afirmar rotundamente, y sin lugar a la duda razonable, que el acusado entró en las empresas y organismos distintos a los reconocidos por él, porque los propios agentes de la Guardia Civil no la tienen y, por tanto, no se la pueden transmitir. En cuanto a los daños resulta imposible acreditar su existencia.

Concluye la Magistrado que no ha podido llegar a la convicción judicial plena, sin lugar a razonables y razonadas dudas, de que el acusado haya cometido los hechos que se le venían imputando. Por un lado, los expertos que llevaron a cabo la investigación no han podido llegar a esas conclusiones de autoría. Por otro lado, el resto de las pruebas tampoco

han podido demostrar que concurran los requisitos penales del delito por el que se acusaba a J.C.T., pues es dudoso el acceso a los sistemas informáticos que se dicen atacados y cuando se ha reconocido, no se han probado los daños, ni que éstos tengan relevancia jurídico penal.

En lo referente al delito de descubrimiento y revelación de secretos, las conclusiones expuestas por los efectivos de la Guardia Civil no permiten declarar probado que el acusado haya accedido a sus ordenadores y mucho menos que se haya apropiado de información sobre datos reservados. Tampoco el necesario perjuicio para tercero exigido por el precepto penal.

Por todo ello se dicta sentencia absolutoria con todos los pronunciamientos favorables al respecto.

2. *La complicada enervación de la presunción de inocencia en la delincuencia informática*

La lectura de la sentencia que se describe en el apartado anterior se alinea con muchas otras en las que se pone de manifiesto lo que podríamos denominar intangibilidad de la prueba en Internet. Los datos necesarios para probar fehacientemente los hechos, han podido existir en algún momento, lo complicado es hacerse con ellos y trasmitírselos al juez de modo tal que la convicción de éste pueda formarse.

Si quien delinque a través de la Red no tiene reparos en dejar huellas de sus acciones e incluso se jacta de ellas, nos encontramos con otro tipo de supuestos en los que abunda el material probatorio. No hay obstáculos entonces para levantar la carga de la prueba. Surgen así bien sentencias de conformidad[12], bien sentencias en las que ésta no se produce. En ambos casos se llega a un resultado condenatorio.

Tras la lectura del epígrafe anterior podemos llegar a formularnos alguna de las siguientes preguntas: ¿existía algún modo convincente de probar la comisión de los hechos?, o bien, ¿tenemos que tolerar

[12] Como por ejemplo sucedió en la sentencia dictada recientemente por el JP n.º 2 de Lleida, de 16 de noviembre de 2006. En ella se alcanza un resultado condenatorio por delito contra los derechos fundamentales y las libertades públicas, tras la conformidad del acusado. Se declara probado que desde los equipos informáticos de que disponía el acusado se crea una dirección de Internet en la que desde la fecha de su creación y varias veces al día, fueron introduciéndose datos y textos de contenido xenófobo y racista, con textos e imágenes contra grupos por razón de la etnia, raza, origen nacional o condición emigrante. La dirección contenía 129 páginas. Posteriormente, el acusado crea una nueva dirección de contenido y características similares a la anterior. En ella los enlaces y documentos internos son los mismos, con excepción de pequeñas diferencias.

determinadas conductas delictivas porque los acusadores están abocados al fracaso en sus intentos probatorios y los jueces sólo pueden, en aplicación de la normativa legal, absolverlas? Situados en este aparente callejón sin salida, se ofrecen algunas posibilidades que podemos considerar.

Por un lado están aquéllas que la propia técnica nos brinda. En algunos casos resulta imprescindible para su incorporación el desarrollo de normativa legal. También existen posibilidades desde la perspectiva de *lege data*.

A) Apreciaciones de lege ferenda

El art. 12 de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, conocida como LSSICE, se refiere al deber de retención de datos de tráfico relativos a las comunicaciones electrónicas, estableciendo lo siguiente:

> «1. Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo.
>
> 2. Los datos que, en cumplimiento de lo dispuesto en el apartado anterior, deberán conservar los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.
>
> Los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.
>
> En ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones.
>
> Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos.
>
> 3. Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribu-

nales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.

4. Reglamentariamente, se determinarán las categorías de datos que deberán conservarse según el tipo de servicio prestado, el plazo durante el que deberán retenerse en cada supuesto dentro del máximo previsto en este artículo, las condiciones en que deberán almacenarse, tratarse y custodiarse y la forma en que, en su caso, deberán entregarse a los órganos autorizados para su solicitud y destruirse, transcurrido el plazo de retención que proceda, salvo que fueran necesarios para éstos u otros fines previstos en la Ley.

(…).»

No debe perderse de vista que este artículo es aplicable a las fuentes de prueba, esto es, a las realidades materiales que se incorporarán, en su caso, posteriormente al proceso a través de los medios de prueba. Esta norma no añade nada al régimen procesal de la prueba, sino que incide en la propia eficacia de la misma al hacerla posible. Ahora bien, para que ello pueda ser efectivamente real, resultaba imprescindible un desarrollo normativo del párrafo 4.º del artículo. Con él las investigaciones basadas en los datos de tráfico tendrían más probabilidades de éxito. Pues bien, en este sentido, es importante destacar la actual tramitación del Proyecto para la conservación de datos en comunicaciones electrónicas y redes públicas de comunicaciones[13]. La norma afecta a la cesión de datos de las comunicaciones electrónicas a las Fuerzas y Cuerpos de Seguridad.

El Proyecto, que ha sido aprobado a propuesta de los Ministros de Justicia, Interior, Industria, Turismo y Comercio y Defensa, incorpora al ordenamiento interno español una Directiva comunitaria sobre conservación de datos generados o tratados en comunicaciones electrónicas[14].

Se establece la obligación para los operadores de este tipo de servicios de conservar ciertos datos generados en cualquier tipo de comunicación electrónica (telefonía móvil y fija e Internet), así como de entregarlos cuando se les requiera para la investigación, detección o enjuiciamiento de delitos. Con ello se refuerzan considerablemente los

[13] El Proyecto deroga el art. 12 de la LSSICE. En el momento de escribir estas líneas se encuentra tramitándose en el Congreso de los Diputados en periodo de enmiendas.

[14] Se trata de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de los datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Su transposición a nuestro ordenamiento jurídico es el objetivo principal de la futura ley.

instrumentos disponibles para el ejercicio de las funciones de seguridad pública de los cuerpos policiales competentes (estatales y autonómicas con competencia para la protección de personas y bienes y para el mantenimiento del orden público), así como del Centro Nacional de Inteligencia y de Vigilancia Aduanera. Éstos podrán acceder a unos datos que en la actualidad, no siempre están disponibles, dificultando la averiguación de los delitos.

Se trata de mantener un imprescindible equilibrio entre los fines de seguridad pública, que justifican las medidas contenidas en el Proyecto, y el respeto de los derechos individuales que pueden verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones. En este sentido, la Exposición de Motivos, especifica que el texto es respetuoso con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido manifestando el Tribunal Constitucional. Tal respeto se articula a través de dos garantías: en primer lugar, porque los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, pero en ningún caso reveladores del contenido de ésta; y en segundo lugar, porque la cesión de tales datos, que afecten a una comunicación o comunicaciones concretas, exigirá siempre, la autorización judicial previa. El legislador ha optado por habilitar la cesión de estos datos para cualquier tipo de delito, a fin de no privar a las autoridades judiciales de un mecanismo de detección e investigación con el que actualmente cuentan, de acuerdo con la configuración constitucional del derecho al secreto de las comunicaciones.

Los datos que deben retenerse no revelarán en ningún caso el contenido de la comunicación. Sólo se conservarán los necesarios para identificar su origen y destino, la hora, fecha y duración, el tipo de servicio y el equipo de comunicación utilizado por los usuarios.

Dichos datos deberán conservarse durante doce meses desde la fecha en que se haya producido la comunicación. Se requerirá siempre autorización judicial.

Se prevén instrumentos para controlar los datos procedentes de teléfonos móviles, adquiridos mediante la modalidad de tarjetas prepago, y se establece la obligación de los operadores de dicho tipo de tarjetas de llevar un libro-registro con la identidad de los compradores.

Asimismo, deberán conservar los datos correspondientes desde la adquisición de la tarjeta, hasta que cese la obligación de conservarlos, de acuerdo con la futura Ley.

Los operadores de estos servicios han de realizar las adaptaciones precisas para el cumplimiento de sus obligaciones de conservación y cesión de datos, en un plazo de tres meses, desde que se apruebe el

procedimiento técnico para la remisión de datos, que, en principio, será también de tres meses desde que se apruebe la futura Ley.

En conclusión[15], los *obligados a la conservación* de datos son tanto los operadores de servicios de comunicaciones electrónicas disponibles al público, como los que exploten redes públicas de comunicaciones.

Mientras que *los datos a conservar* son los necesarios para:

—Rastrear e identificar el origen de una comunicación.
—Identificar el destino de una comunicación.
—Determinar la fecha, hora y duración de una comunicación.
—Identificar el tipo de comunicación.
—Identificar el equipo de comunicación de los usuarios, incluso las tarjetas prepago.
—Identificar la localización del equipo de comunicación móvil.
—Identificar llamadas infructuosas.

En cuanto a la eficacia de toda esta normativa relativa a la conservación de datos, merecen traerse a colación las palabras que RODRÍGUEZ LAINZ dedicaba hace algún tiempo al aún vigente art. 12 LSSICE. Son aplicables al nuevo escenario que dibujará la futura Ley de conservación de datos. Según este autor

> «(…) difícilmente podrá imponerse a un prestador de servicios extracomunitario un deber de retención de tanta trascendencia técnica y económica cuando el prestador de servicios no tendrá más relación con el Estado español que los cables de comunicaciones que permitan el acceso y utilización de sus servicios; por ello, ciertamente, (…) puede suponer una auténtica fuga de entidades concernidas por la obligación a auténticos *paraísos cibernéticos*, la eficacia del referido precepto si no va acompañada con una difusión o extensión en el derecho comparado o de la consecución y coordinación de esfuerzos en el panorama internacional *(sic)*, puede quedar sustancialmente mermada en cuanto a sus potencialidades de servir al fin por el que se ha establecido la obligación legal»[16].

Junto con esta necesaria previsión legal, que finalmente parece que verá la luz en breve, podemos también referirnos al Sistema de Rastreo

---

[15] Síntesis de obligados y datos, accesible en RIBAS, X.: http://xribas.typepad.com/xavier_ribas/2007/03/proyecto_de_ley.html

[16] RODRÍGUEZ LAINZ, J.L: *Intervención judicial en los datos de tráfico de las comunicaciones. La injerencia judicial en los listados de llamadas y otros elementos externos de las telecomunicaciones y comunicaciones electrónicas*. Ed. Bosch, Barcelona, 2003, p. 519.

de Explotación Infantil CETS (son las siglas en ingles de *Child Exploitation Tracking System*). Se trata de un *software* que Microsoft creó por petición de la policía canadiense y que ya ha funcionado con éxito en aquel país[17].

El sistema, según Microsoft, compara todas la investigaciones que hacen referencia a las mismas personas, correos electrónicos, apodos, sitios *web* y *chat*, y además, comparte y busca información desde el momento de la detección, fase de investigación y arresto del acusado. No persigue ni almacena datos personales de los usuarios, sino que permite a las distintas policías compartir información y crear bases de datos comunes donde cruzarla para perseguir todos los delitos relacionados con pornografía infantil y abuso a menores.

La plataforma se implementó por primera vez en 2003, en Canadá, cuyas fuerzas de seguridad están conectadas en nueve provincias. Actualmente se ha donado a varios países entre ellos a España. Con su uso no se duplican esfuerzos y se comparte el conocimiento entre los investigadores de todo el mundo a través de redes sociales específicamente creadas para combatir la pornografía infantil. Como se sabe, los delitos relacionados con esta lacra social han encontrado en Internet un campo perfecto para su distribución[18].

Iniciativas como CETS pueden ser una valiosa ayuda en la lucha contra la criminalidad que usa de la Red como medio de difusión y comisión del delito. Permiten llegar a establecer la autoría, que suele ser más difícil

---

[17] La policía canadiense anunció el 18 de octubre de 2006 la detención de un individuo de 34 años dos horas después de que transmitiese por Internet en directo la violación de una niña. El detenido transmitió por la Red las imágenes de la violación en directo a un policía (Paul Krawczyk) que actuaba encubierto. Un portavoz del cuerpo de Policía dijo que el detenido, cuya identidad no fue revelada para proteger a la niña, estaba siendo investigado desde enero de ese año cuando envió al agente una serie de fotografías pornográficas con una menor. Tan pronto como Krawczyk empezó a recibir la transmisión de las imágenes se inició el rastreo de su procedencia y en pocos minutos la policía identificó su origen en la localidad canadiense de St. Thomas, a 180 kilómetros al suroeste de Toronto. Dos horas después del inicio de la transmisión de las imágenes, la policía se encontraba en la puerta de la casa del acusado, en la que todavía se hallaba la menor. La detención fue posible gracias a la tecnología CETS, que desde 2004 ha permitido la realización de 64 arrestos sólo en Canadá. Su creación fue la respuesta directa del propio Bill Gates a un afortunado correo electrónico que Paul Gillespie, el jefe de Krawczyk, le envió directamente una noche de 2003. La orden de Gates a sus subordinados y la buena disposición de los agentes de Gillespie bastaron para poner en marcha, un año y medio después, este *software*. La noticia ha sido consultada en el diario *El País* de 3 de noviembre de 2006 y bajo el título «La herramienta que Microsoft donó a la Guardia Civil».

[18] Según la Interpol la mitad de los delitos que se cometen en Internet están relacionados con la pornografía infantil. *Idem*.

de probar que la propia existencia objetiva del delito. Como ponía de relieve recientemente MAZA MARTÍN, la Justicia tiene graves dificultades para perseguir y castigar los delitos informáticos. Sobre todo a la hora de investigarlos e identificar sus autores[19].

Finalmente, desde esta óptica de *lege ferenda*, debe señalarse la conveniencia de establecer un marco normativo europeo específico que regule la prueba electrónica. En este sentido, el primer estudio realizado en toda Europa sobre admisibilidad de la prueba electrónica revela que el 78% de los juristas consultados, entre los que se encuentran fiscales, jueces, abogados, notarios y representantes del CGPJ, reclaman ese desarrollo legislativo para ayudar a combatir los delitos. Incluso consideran necesario fijar normas internacionales que homogeneicen el tratamiento procesal de la prueba electrónica, para mejorar así la cooperación internacional entre quienes combaten el crimen[20].

B) APRECIACIONES DE LEGE DATA

Desde un planteamiento de *lege data* podría estudiarse la aplicación supletoria del art. 4 LEC a la LECrim y, en su virtud, considerar el principio de disponibilidad y facilidad probatoria al que se refiere el art. 217.6 LEC.

El primero de estos preceptos establece la supletoriedad de la LEC frente al resto de leyes procesales, de modo que en defecto de disposiciones en la LECrim, será de aplicación la normativa de la LEC al proceso penal.

Por su parte, el art. 217 LEC regula la normativa de carga de la prueba, y al hacerlo, establece en su apartado 6 que «el tribunal deberá tener presente la disponibilidad y facilidad probatoria que corresponde a cada una de las partes del litigio». En este sentido debe valorarse la proximidad real de la parte a la fuente de prueba y la alegación por el acusado de hechos impeditivos o extintivos, tal y como lo refieren las SSTS citadas *supra*[21]. En el bien entendido siempre de que la parte pasiva no tiene carga alguna de manifestarse respecto a los hechos de la acusación.

---

[19] MAZA MARTÍN, J.M. es Magistrado del Tribunal Supremo. Lo trascrito en el texto forma parte de su intervención en el primer *Congreso Iberoamericano de Seguridad y Desarrollo de la Sociedad de la Información,* celebrado en Madrid el pasado mes de diciembre de 2006.

[20] Estudio realizado por la empresa española de investigación de fraudes en entornos virtuales Cybex.

[21] En concreto se trata de las SSTS de 4 de febrero de 1995 y 9 de febrero del mismo año.

La posibilidad real de acudir a través de la supletoriedad primero (art. 4 LEC), y de la analogía después (art. 217.6 LEC), a la normativa de la Ley procesal civil, en materia de carga de la prueba merece una reflexión más detenida. Por razones de espacio no me es posible profundizar más en este momento. Sin embargo, creo que merece la pena, al menos, apuntarlo.

IV. **A modo de conclusión**

Dado el carácter y extensión de este trabajo, la conclusión a la que a continuación me refiero no puede ser más que interina, de modo que con esa limitación la planteo.

A lo largo de la lectura de las sentencias en las que concurre prueba tecnológica mediando conexión a Internet, no he podido dejar de advertir la exquisitez y prolijidad de las argumentaciones esgrimidas por los juzgadores al valorar la virtualidad de tal clase de prueba. En gran parte de los casos para terminar justificando la aplicación del principio *in dubio pro reo* por la situación de incertidumbre en que permanecían los hechos de la acusación tras la fase probatoria.

Probablemente se recurra al principio *in dubio pro reo* con más asiduidad de la que se emplea cuando los delitos suceden fuera de Internet y en esa situación me pregunto, si en la actualidad y teniendo en cuenta los graves peligros que amenazan la sociedad democrática y plural que pretendemos conservar, no debería procederse a una revisión de algunos de los pilares básicos del proceso penal, como es el derecho a la presunción de inocencia. Quizás podrían considerarse determinados supuestos en los que el principio no se interpretara en forma tan rígida que parece atentar, a veces, contra la propia lógica[22].

En la sociedad actual, mantener incólume un principio pensado para otra en la que determinadas actuaciones especialmente lesivas del ser humano eran impensables por impracticables, supone restar muchas posibilidades de actuación al proceso penal. Siempre teniendo en cuenta la vocación de *ultima ratio* de éste. Ahondando en ello, las palabras de una periodista y escritora recientemente fallecida, se revelan dolorosamente lúcidas: «Cuanto más democrática y abierta es una sociedad, tanto más

[22] No sería la primera vez y seguramente tampoco será la última. Nuestro Tribunal Constitucional lo ha hecho respecto de la doctrina en torno a la prueba ilícitamente obtenida, flexibilizando el entendimiento de preceptos tan categóricos como el art. 11.1 LOPJ «(…) No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales».

expuesta está al terrorismo. Cuanto más libre es un país, cuánto menos tolera las medidas policiales, tanto más padece o se arriesga a padecer (…) secuestros y masacres (…)»[23].

La reflexión es aplicable a otras formas de criminalidad organizada y a la delincuencia informática a través de Internet. Desvirtuar la presunción de inocencia en esa clase de delitos resulta una tarea, muchas veces agotadora y demasiadas veces improductiva.

Creo que deberíamos hacer lo posible para conjurar esos riesgos a través de instrumentos como los apuntados *supra* que, sin dejar de ser respetuosos con la presunción de inocencia, hagan más realista nuestro sistema de enjuiciamiento penal.

[23] FALLACI, O.: *La rabia y el orgullo*, Madrid, 2002, p. 64.

Anexo:
Vocabulario informático y siglas de interés

Carmen Adán del Río
Fiscal del Tribunal Superior de Justicia del País Vasco

Este pequeño vocabulario, se inició como una serie de consultas en biblioteca y en la red, siendo fundamentalmente de esta última de donde se ha extraído la mayor parte de la información. Tiene como finalidad facilitar la comprensión de algunos de los términos más habituales en lenguaje sencillo, siendo consciente de que el número de ataques y fraudes recogidos es singularmente corto con relación a los existentes.

I. **Componentes de un ordenador**

Además de los conceptos básicos: *hardware* (soporte físico, elementos electrónicos que realizan los procesos) y *software* (programas y aplicaciones informáticas), es importante tener en cuenta los siguientes:

Placa base. Unidad de control del *PC*, donde se encuentran la mayor parte de sus componentes.

Procesador. Circuito integrado en un chip que realiza los cálculos basicos. Es la parte del ordenador que hace todo el trabajo de procesamiento de datos. Se le suele llamar *CPU* (*Central Processing Unit*, unidad central de procesamiento), aunque en algunos ordenadores se utiliza este término para referirse a la caja del PC sin el monitor, o el teclado. De forma más simple sería la parte encargada de hacer las transacciones necesarias para que frente a una cuestión determinada se de un resultado.

Memoria. Lugar donde se almacenan datos. *Ram* (*Ramdom Access Memory*), memoria de acceso aleatorio, porque se pueden leer los datos de cualquier parte de la memoria en el orden que sea. La cantidad de *Ram*, como es evidente, afecta a la cantidad de programas que se pueden ejecutar en el ordenador y a su mayor velocidad. La

memoria es volátil, esto es, los datos almacenados se pierden cuando el sistema se apaga o se corta la alimentación.

Disco duro. Principal medio de almacenamiento permanente de datos de un PC.

Sistema operativo. Enlace entre el *hardware* del ordenador y los programas de aplicaciones que se usan para realizar tareas concretas. Proporciona administración de archivos, seguridad y coordinación de las aplicaciones y programas que funcionan al tiempo.

Aunque de forma en exceso simple, en ocasiones, se presentan los conceptos de ordenador, fichero, registro y campos, como similares a los de oficina, fichero, ficha y datos.

II. **Términos frecuentes**

Administrador. Aquel que tiene el poder absoluto sobre la máquina, el control sobre el funcionamiento del sistema informático. Es un concepto relacionado con *Sysop* o *Root* (ver).

Adjunto - Attachment. Fichero que se incluye en un mensaje de correo electrónico. Puede contener texto, imagenes, sonido, secuencias…

ADSL. *Asymetrical* (o en su momento *Asynchronous*) *Digital Subscriber Line*. Línea Digital Asimétrica de Abonado. Línea digital de alta velocidad. Es una tecnología de acceso a Internet de banda ancha, que supone mayor capacidad para transmitir mas datos, y en definitiva mayor velocidad. Esta tecnología se denomina asimétrica, debido a que la velocidad de descarga (desde la Red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente la velocidad de descarga es mayor que la de subida.

Adware. Modalidad de *spyware (ver)*. Programa espía que se instala al descargar un programa, añadiendo publicidad a los programas. Su finalidad suele ser, por dicha razón, meramente comercial.

Applet. Aplicación informática incluida en una página *web* programada en lenguaje *Java (ver)*, que se ejecuta en nuestro ordenador.

Ancho de banda. Tamaño de la conducción de datos.

Archivo. Tambien fichero. Forma de estructurar la información. Todos los archivos que son sólo texto, son archivos binarios. Hay que distinguir entre archivo de datos y archivo ejecutable. *Archivo de datos*, es

la fórmula simple, una especie de contenedor de información. *Archivo ejecutable*, sería en realidad un programa, puesto que siguiendo los parámetros que da, realiza unas acciones determinadas.

Arpanet. Red impulsada por la Agencia de Proyectos de Investigación Avanzada del Departamenteo de Defensa de EEUU en los años 60, que conectaba diferentes ordenadores en un sistema que permitía, que si uno de ellos era inutilizado, la información seguía fluyendo entre los demás.

AUI. Asociación de Usuarios de Internet.

Backbone. Columna vertebral. Conjunto de computadoras que transportan el flujo de datos principal en la Red.

Backdoor. Puerta trasera. Mecanismo que sustituye la forma habitual de entrada en un sistema informático. Suele aprovechar una debilidad del sistema o se crea al efecto.

Banca on line. Concepto que abarca las entidades bancarias tradicionales que ponen al servicio de su cliente las comodidades de acceder en casa a su cuenta o relizar transacciones (ej. El servicio Uno-e, ofrecido por el BBVA), como igualmente, aquelllas entidades bancarias que solo operan en Internet (ej.: ING *direct*).

Banner. Gráfico que se inserta en una página *web* con finalidad publicitaria. Suele incluir el enlace con el sitio publicitario. La posibilidad de que los móviles permitan navegar por Internet, dará lugar, y ya se ha anunciado por varias compañias para el año 2008, a la inserción de publicidad, mediante *banners*. Imágenes estáticas o dinámicas que podrán en breve permitir enlazar con la página del anunciante.

BBS. *Bulletin Board System*. Se puede traducir como Tablero de Anuncios Electrónico. Era una fórmula de conexión entre ordenadores que ofrecía muchos de los servicios que hoy presta Internet: correo, *chats*, intercambio de archivos informáticos… Existía un ordenador central al cual se conectaban los usuarios. Esto es lo que marca la diferencia respecto a Internet, lo que suponía una enorme ventaja en cuanto a garantizar la confidencialidad. Es considerado precursor de la *w.w.w*. (ver)

Binhex. Método de cifrado utilizado por *Mac*.

Biometría. Estudio mensurativo de los procesos o fenómenos biológicos. Técnica que estudia las características físicas de las personas,

tales como huellas, iris… Una de las técnicas biométricas más seguras es la identificación por iris. Ha habido experiencias piloto de entidades bancarias para incluir técnicas biométricas de seguridad, quiza la más significativa, el año pasado, fue la del *Senshu Bank of Osaka*, cuyas tarjetas de crédito incluían patrones de las palmas de las manos e información de la huella dactilar del cliente.
Otra modalidad es el *Palm Secure*, que ofrecen algunos ordenadores, en los cuales frente a los ya conocidos, de huella de la palma de la mano, ofrece la novedad de no ser preciso el contacto, bastando con abrir la mano sobre el lector sin tocarlo.

Bit. Unidad básica de datos. Nombre que se da a los dos digitos, 0 y 1, que utiliza la numeración binaria, tambien llamada lenguaje binario, lenguaje máquina o código máquina.

Blog. Publicación *on line*, en la que quien la escribe comparte su contenido, con opiniones sobre determinados hechos, narrando temas de interés. Su importancia creciente, se reconoce por periodistas, que consultan con relación a temas concretos de lugares concretos de interés, o incluso por analistas y buscadores de tendencias en ámbito comercial.

Bomba lógica. *Software (ver)*, rutina o modificación de programas que dan lugar a cambios, borrados, o alteraciones del sistema, normalmente cuando el usuario pulsa unas determinadas teclas o incluye una determinada aplicación.

Bomba de tiempo. Es uno de los tipos de bomba lógica. En ella, la alteración, cambio o borrado se produce con efecto retardado, normalmente en una fecha determinada, o a partir de una fecha concreta.

Boot. Sector de arranque. Proceso o zona del disco duro en la que se encuentran los ficheros que hacen posible que se cargue en memoria y se inicie el sistema operativo y los programas al encender el ordenador.

Bookmark. Marca o puntero de un documento electrónico, o en las páginas *web*, apuntando a una dirección de Internet, un archivo o un documento.

Bot. Diminutivo de robot. Es un programa informático que realiza en línea funciones normalmente realizadas por humanos. En un sitio de conversación, un *bot* puede simular ser una persona. Se les considera una de las herramientas favoritas de los *hackers (ver)*.

Bounce. Devolución de un mensaje de correo electrónico debido a problemas para entregarlo a su destinatario.

Boxes. Aparatos, circuitos electrónicos o eléctricos utilizados para el *phreaking (ver)*. Logran crear tonos multifrecuenciales que permiten comunicaciones telefónicas gratuitas.

—**Bluebox.** Genera tonos de llamada a larga distancia.
—**Greenbox.** Genera tonos de llamada a cobro revertido.
—**Redbox.** Genera tonos para realizar llamadas gratis.

Bps. *Bits (ver)* por segundo. Velocidad de transferencia de datos entre dos módems (ver).

Bug. Mal funcionamiento, fallo o defecto de *software* (ver) o del *hardware* (ver) que provoca un error, que hace que el ordenador o sistema en ciertas circunstancias no actúe correctamente. El término viene del inglés, *bug*, bicho, porque el primero conocido, fue una polilla real que provocaba la paralización de una computadora. Son utilizados o provocados en ocasiones por los *hackers (ver)*.

Buscador. Herramienta, página o sitio *web* que permite encontrar información en Internet, a través de una palabra o referencia. También es llamado motor de búsqueda.

Business to Business. B2B. Comercio electrónico entre empresas.

Business to Consumer. B2C. Comercio electrónico entre empresa y consumidor final del producto.

Bytes. Son las unidades que usan los ordenadores para representar una letra, un número o un símbolo. Unidad de medida informática. Un *byte* suele ser equivalente a ocho *bits (ver)*. Un *megabyte*, mil *kilobytes*… El orden sería: *byte*, *kilobyte* (*KB*), *megabyte* (*MB*) (ver), *gigabyte* (*GB*) (ver), *petabyte* (*PB*), *exabyte* (*EB*)… y aunque nos suene extraño se habla ya, en esa cadena, de *zettabyte* (*ZB*), y *yottabyte* (*YB*).

Caballo de Troya o troyanos. Programas que se ocultan dentro de otros, para no ser descubiertos, y se instalan en nuestro sistema, de forma que al actuar producen un auténtico sabotaje contra el sistema informático. Los troyanos no se replican a sí mismos lo que les diferencia de los virus puros aunque algunos sí son capaces de enviarse como adjuntos.

Cache. Copia de las páginas que se visitan en un determinado periodo de tiempo, de forma que podemos pedirlas de nuevo en nuestro ordenador sin descargarlas del ordenador remoto. Viene a

ser un almacenamiento temporal que suele proporcionar el navegador, y que permite incrementar la velocidad del sistema disminuyendo los accessos al disco duro. En el mismo sentido el término *caching*.

Carding. Falsificación y utilización de tarjetas de créditos ajenas o de sus números.

Careware. Forma de distribución de *software (ver)*, en la que el creador lo da libremente sugiriendo o indicando que se pague una cantidad a una obra de caridad. Es el mismo concepto que *donateware*, *charityware*…

Carpeta. Espacio que podemos crear en nuestro ordenador para almacenar datos. Una carpeta equivale a un directorio.

Carrier. Proveedor de telefonía local e internacional que puede proporcionar conexión a Internet de alto nivel.

CATSI. Consejo Asesor de las Telecomunicaciones y la Sociedad de la Información.

CCN. Centro Criptográfico Nacional. Depende del CNI. Actúa de oficio en ataques contra información clasificada como sensible para la seguridad nacional. Este año, ha presentado un equipo especializado en detectar amenazas o zonas vulnerables que pueden afecta a los sistemas de información de las administraciones públicas, así como en formar a los responsables de redes públicas para en caso de ataque minimizar el daño.

CEPS. Sistema de rastreo de pornografía y explotación infantil. Sistema *software (ver)* donado por *Microsoft* a varios países para su utilización con la finalidad de crear y relacionar las bases de datos sobre esta materia.

Chat. Charla. Sistema de comunicación a tiempo real, con otros usuarios conectados a la red, a través de texto, imagen o voz. El programa histórico de las chats era el *MIRC*.

Ciberespacio. Concepto que procede de la literatura de ficción, concretamente utilizado por Willian Gibson, para refererirse al mundo entre los ordenadores conectados, redes de información y medios digitales.

Ciberpunk. Se ha utilizado en ocasiones para los *hackers (ver)*, por lo que significa este movimiento social de desconfianza o ataque a las máquinas.

Cloacker. Programa encargado de borrar las huellas (*logs*) que deja la entrada no autorizada en un sistema informático. Es similar a *Zapper*.

Consumer to consumer. C2C. Transacciones comerciales entre particulares que se realizan en los tableros de anuncios de las páginas *web*, en tiendas virtuales o en grupos de noticias.

Cookies. (Galletitas). Bloques de datos que determinados sitios *web* envían a las máquinas que se conectan a ellos, quedando almacenadas en su disco duro, de forma que cuando el usuario vuelve a visitar ese sitio *web*, los datos son reenviados al servidor dando información sobre ese usuario. Su uso malintencionado más frecuente es el dirigido a controlar los hábitos de navegación de un sistema a otro, obtener la información de acceso de un usuario a un sitio *web* y enviarlo a otro, o incluso para capturar la dirección *e-mail* de un usuario y añadirla a una lista de correo sin su conocimiento.

Cracker. De forma simple, pirata informático malo. Persona que accede ilegalmente a un sistema informático ajeno con fines vandálicos o dañinos. Para otros, este aspecto queda igualmente incluido en el *hacking*. De ahí la expresión, *dark-side hacker* (*hacker* del lado oscuro). Desde este concepto restringido su objetivo sería producir daño, frente al *hacker (ver)* que busca obtener información.

Crash program. Programa de destrucción masiva.

Criptografía. Ciencia que estudia y diseña el conjunto de técnicas empleadas para cifrar la información. En España, ha de tenerse en cuenta al organismo oficial, CCN, Centro Criptológico Nacional, dependiente del CNI.

Daemon. Proceso que se está ejecutando en un segundo plano.

Data diddling. Ataque informático consistente en modificación, borrado, sustitución o manipulación en general de datos.

Debugger. Término genérico que designa un programa que permite la ejecución controlada de otros programas, mostrando simultáneamente el código que se está ejecutando. Esto posibilita el seguimiento pormenorizado de las instrucciones que el sistema informático está ejecutando, así como la realización de las modificaciones necesarias para evitar las secciones del código que no interesan al usuario o la localización de *bugs (ver)*, el diseño de *cracks*, etc. También se les conoce como programas DDT.

Denegación de servicio. Forma de ataque informático, que sin afectar a la información de un sistema, le impide prestar el servicio por saturación o bloqueo. Es tambien llamado *DoS Attack (ver)*, *Denial of Service attack*

Dirección IP. Dirección numérica separada por puntos que identifica en exclusiva a un ordenador en Internet

Dirección URL. Siglas inglesas de *Uniform Resource Locator*. Localizador Uniforme de Recursos. Conjunto de caracteres o dirección que identifica de manera inequívoca un recurso determinado en la Red; un archivo, un documento, una página *web*, etc.

Div-x. Programa destinado a la descomprensión de videos en formato *MPEG4*. *(ver)*

Dominio. Nombre único o caracteres que tiene una entidad para operar en la Red (*host*) (ver). Hay un sistema internacional de dominio *DNS (ver)*. En todo caso, la mayoría de los paises tiene un dominio propio, España (*es*), y los mas conocidos son: *com* (empresas, comercio), *gov* (gobierno), *net* (operación en la Red), *org* (organización sin fines de lucro)…

DNS. *Domain Name System* o Sistema de nombres de Dominio. Sistema que localiza la dirección IP correspondiente a un servidor.

Dos Attack. *Denial of Service Attack* (Ataque de Denegación de Servicio). Abreviatura utilizada para designar aquellos incidentes en los cuales un usuario se ve privado del acceso a un servicio que normalmente podría utilizar. Así por ejemplo, el intento de desactivar un grupo de noticias mediante el envío masivo de *spam (ver)*.

ECHELON. Nombre clave con el que se denominaba un sistema de espionaje electrónico creado por los aliados después de la II Guerra Mundial, que mediante satélites espía y programas informáticos que reconocían voces y hacían seguimientos de palabras en la mayor parte de las comunicaciones mundiales.

E-mail address. Conjunto de caracteres que identifican en exclusiva a un usuario de correo electrónico y, en consecuencia, permiten la remisión de mensajes a un destinatario concreto. Todas las direcciones de correo electrónico tienen el siguiente formato: nombre de usuario @ nombre de dominio.

E-mail. De obvio significado y uso para todos. *Electronic mail*. Correo electrónico. Servicio que permite el envío y recepción de mensajes

escritos entre usuarios de Internet. También hace referencia al mensaje transmitido a través de dicho servicio.

Emulador. *Software (ver)* o programa informático que simula el funcionamiento de un terminal central. Con él es posible usar juegos y aplicaciones diseñadas para otros sistemas (consolas, máquinas recreativas y ordenadores tipo *Spectrum*, *Amstrad*, etc.). Se ha usado para «piratear» juegos de consolas. Uno de los emuladores de terminal más conocido es *Telnet (ver)*.

Enlace. Referencia a otro documento (ver *link*).

Espejo - Mirror. Réplica de un sitio *web*. Servidor *web* cuyo contenido es una copia exacta de otro servidor; su utilidad es reducir el tiempo de acceso del usuario a servidores muy visitados, como los que descargan archivos, evitando su sobrecarga.

Esteganografía. Escritura encubierta. Método de ocultación de datos, que oculta sus contenidos y su propia existencia. Mediante su uso, se evita llamar la atención de las personas que buscan información confidencial. La mayor parte de los autores consultados, lo consideran de futuro, de uso común, dada la frecuencia de los ataques.

Exploit. (Aprovechar, explotar). Programa informático, que utiliza una parte vulnerable de un programa (*bug*) *(ver)*, para obtener acceso con fines de uso o destrucción.

Fake email. Envío de un mensaje de correo electrónico con dirección falsa.

Favoritos. Carpeta que almacena las direcciones *URL (ver)* preferidas por el usuario.

Firewall. Muro de fuego o cortafuegos. Filtro o sistema de seguridad que controla las comunicaciones que pasan de una red a otra. Los más clásicos son los llamados perimetrales, que hacen de pasarela entre una red local a Internet.

Firma digital. Datos cifrados y encriptados que identifica al autor de un mensaje y documento. Garantiza tanto la autenticidad e integridad del documento como la identidad del autor. Tiene una parte privada, propia del autor, y otra que es la que se da a conocer a terceros y entidades, que permite que se desencripte.

Freeware. *Software (ver)* libre. Aplicaciones o programas gratuitos, que pueden ser libremente copiados, distribuidos, o modificados, atendiendo a los parametros fijados por el autor. Viene a equivaler a que el autor dona el programa sin retener el *copyright*.

FTP. *File Transfer Protocol*. Protocolo de Transferencia de Ficheros. Programa o conjunto de protocolos, que permite a un usuario de Internet acceder a servidores que permiten cargar o descargar archivos informáticos en su ordenador. Al estar alojados estos ficheros en un ordenador remoto, organizados debidamente, su tiempo de descarga y copia es menor que a través de la *www*. *(ver)*

F-serve. Prestación que permite a otros el acceso al disco duro de nuestro ordenador, ya sea para ver o para lograr determinados contenidos de nuestro ordenador.

GIF. *Graphic Image File*. Formato, comprimido, gráfico y de imagen que se usa en las páginas *web*.

Gigabyte. Unidad de medida informática equivalente a mil millones de *bytes (ver)* o un millón de *kilobytes* o mil *megas (ver).* Su símbolo es *GB* o *GIB*.

Gusano. *Worn*. Programa autoreplicante que no altera los archivos sino que reside en la memoria y se duplica a sí mismo. Algunas de las fuentes consultadas lo considera un virus o equivalente, aunque la diferencia, está posiblemente en el carácter sólo autoreplicante.

Hack Tv. Forma de fraude, consistente en el empleo de tarjetas que suplantan a las tarjetas originales de una compañía, obteniendo acceso a un canal o señal de televisión codificadas, sin necesidad de abonarse.

Hacker. Pirata informático. El concepto original, *hacking*, abarcaba cualesquiera accesos no autorizados, con o sin intención dañosa, con o sin intención de lucro. Según algunas opiniones, el concepto no incluye a quien entra en el ordenador con intención criminal o vandálica, para el cual sería apropiado el término *cracker (ver)*. Según algunas fuentes, el concepto viene de *hack*, que era el sonido que se empleaba en las empresas de telefonía al golpear el aparato telefónico para que funcionara.

Hacking tool. Programa cuya finalidad es controlar un ordenador a distancia, desde otro equipo.

Hardware. Componentes físicos de un ordenador.

Header. Cabecera de un *e-mail* con el nombre y dirección del remitente, y otros datos como la fecha de envío del mensaje y los servidores por los que éste ha pasado hasta llegar a su destino.

Hijacker. Programa que secuestra al navegador, dirigiéndolo a una página de Internet.

Home page. Página inicial. La que se muestra por defecto cuando acudimos a una dirección *web* determinada.

Host. Anfitrión. Servidor. Ordenador conectado a Internet o a cualquier otra red que proporciona a otros ordenadores diferentes servicios, de archivo, de correo electrónico… En realidad puede ser un ordenador, un fichero, un servidor de archivos… Por extensión a veces también se llama *host* al dominio del equipo.

Hot chat. *Chat* con contenido sexual explícito.

HTML. *Hypertext Markup Language*. Lenguaje de Marcas de Hipertexto. Lenguaje que incluye texto, gráficos, sonido… mediante el que se escriben las páginas a las que se accede a través de navegadores *web*. Lenguaje para crear documentos en la Red.

Internet explorer. Navegador de *Microsoft*.

HTTP. *HyperText Transport Protocol*. Protocolo de Transferencia de Hipertexto. Sistema mediante el cual se envía la petición para acceder a determinada página *web*, y la respuesta, remitiendo la información que vemos en la pantalla.

Hypertexto. Documento en el que se puede saltar a otra parte haciendo *clik* en una palabra.
Término que se aplica a los enlaces o *links (ver)*, que existen en una página *web* y que son interpretados por los navegadores como accesos a otras páginas *web*.

IAP. *Internet Access Provider*. Proveedor de acceso a Internet. Entidad que proporciona acceso a Internet a través de una conexión telefónica, actuando como intermediario entre ésta y el usuario final.

ID - UserID. Conjunto de caracteres alfanuméricos que identifican a un usuario para acceder en Internet a una serie de recursos dentro de un servidor

IMAP. *Internet Messaging Acces Protocol*. Protocolo de mensajería instantánea en Internet. Facilita el acceso a los mensajes de correo electrónico almacenados en un servidor, desde cualquier equipo que tenga conexión a Internet.

INTECO. Instituto Nacional de Tecnologías de la Comunicación. Organismo del Ministerio de Industria que entre otros cometidos, contro-

la o realiza informes sobre la seguridad en la Red. Recientemente, catalogó los programas de riesgo, en tres grupos, de alto riesgo, como los troyanos, marcadores o captadores de pulsaciones, de medio como el *adware (ver)*, y de bajo riesgo, como las bromas. Según su informe, el 52 % de los equipos sufre un riesgo alto.

Interface. Programa o conjunto de programas que comunican un sistema con otro. Fase intermedia para comunicar sistemas que no se comunican directamente.

INTERNET. Red de redes de ordenadores a escala mundial con un sistema de comunicaciones común. España según varias encuestas sólo tiene un poco más del cincuenta por ciento de la población incorporada a su uso, aunque según datos objetivos, en cuanto a infraestructuras de acceso estamos en el número diecisiete de los países de la Unión Europea.

Intranet. Red de ordenadores de características y en ocasiones servicios similares a Internet**,** pero de uso interno o privado.

IP. *Internet Protocol*. Protocolo de Internet. Conjunto de normas que regulan la transmisión de paquetes de datos a través de Internet

IRC. *Internet Relay Chat*. Canal de Charla en Internet. Sistema de charlas, o protocolo mundial de comunicación en tiempo real en texto, en grupo o privado.

ISP. *Internet Service Provider*. Proveedor de servicios de Internet, también IPS. Proveedor de acceso. Entidad que proporciona acceso a Internet.

Java. Lenguaje de programación diseñado por *Sun Microsystems*.

Javascript. Aunque coincide en las cuatro primeras letras, no confundir con el anterior. Estamos ante un lenguaje de *scripting* desarrollado por *Netscape* para permitir la ejecución de códigos incluidos en las paginas *web*. Se usa para modificar tamaño de ventana del explorador, abrir y cerrar ventanas… Se considera un tipo de código que por determinados puntos débiles de los que adolece, se puede usar para realizar acciones no deseadas o incluso peligrosas en un ordenador.

Joke. Bromas. Son programas inofensivos, como por ejemplo, los que hacen que la pantalla se mueva, cambie de posición…

Joost. Programa que proporciona televisión por Internet con gran calidad de imagen, canales telemáticos, programas y series completas.

Junkmail. Envío masivo de propaganda a través del correo electrónico. Existe un gusano con este nombre. Correo basura. *Spam (ver)*.

Kazaa. Programa de intercambio de canciones. Sus creadores, los escandinavos Janus Friis y Niklas Zennstrom, usaron para ello la tecnología *P2P (ver)*.

Kernel. Núcleo o parte fundamental de un sistema operativo. Es el *software (ver)* responsable de facilitar a los distintos programas acceso seguro al *hardware (ver)* de la computadora o, en forma más sencilla, sería el encargado de gestionar recursos.

Keylogger. Programa o dispositivo físico, diseñado para registrar, sin que el usuario lo perciba, cada pulsación del teclado. Una clase es el *keycarbon*, dispositivo *USB* que registra en su memoria todo lo que el usuario teclea.

LAN. *Local Area Network*. Red de área local. Una red puede ser definida como un conjunto de ordenadores conectados entre sí con el fin de compartir recursos e información. Según el espacio que abarquen o la distancia a la que se encuentren los ordenadores que integran una red, se suele distinguir entre *LAN* (red de área local) y *WAN* (red de área amplia) *(ver)*.

Link. Enlace *(ver)*. Marcador que al hacer *click* sobre el mismo permite saltar a otra información, documento o archivo contenido en el mismo sitio *web* o en otro distinto.

Linux. Sistema operativo compatible con *Unix (ver)* totalmente gratuito y de libre distribución.

Macros. Conjunto de instrucciones que ejecutan una función automáticamente dentro de un programa.

Mailbomb. Ataque informático consistente en inundar una dirección de correo electrónico con gran número de mensajes con finalidad dañina, normalmente de colapsarla.

Mailbox. Buzón de correo. En este caso referido al directorio donde se guardan los mensajes de correo electrónico.

MailFilter. Filtro de correo. Programa usado para seleccionar los mensajes de correo electrónico según criterio que se establezca.

Malware. Programa maligno. Concepto en el que se suele incluir a los virus *(ver)*, gusanos *(ver)*…

Megabyte. (*MB*) Es una unidad de medida de cantidad de datos informáticos. Aunque anteriormente al tratar *byte (ver)* indicaba que era equivalente a mil *kilobytes*, más preciso es señalar que un *megabyte* equivale a 1024 *kilobytes*.

Mockingbird. Programa malicioso que actúa entre el servidor y sus usuarios, obteniendo información sobre identidad y contraseña del usuario.

Módem. Abreviatura de *Modulator/Demodulator* (Modulador/ Demodulador). Elemento de *hardware (ver)* o dispositivo que convierte las señales digitales en analógicas y a la inversa, y comunica dos ordenadores mediante una línea de teléfono.

Modding. Modificación estética o funcional de *software (ver)*, ordenador o de los periféricos al ordenador.

Morphing. Posibilidad que tienen algunos programas de diseño gráfico, que permite obtener una imagen a partir de otra.

MP3 - MP4. Siglas de *MPEG Audio Layer-3 o 4*. Formato de compresión de audio digital que permite reducir el tamaño de los ficheros de audio. En el caso del *MP4* cuatro incluye comprimir vídeo.

Napster. (*Napster Comunity Music*) Aplicación informática gratuita que conecta a sus usuarios entre sí, a través de un conjunto de servidores y les permite intercambiar ficheros musicales en formato *MP3 (ver)* que tengan en sus ordenadores. Tuvo su punto álgido en el año 2000. El nombre viene del pseudónimo utilizado por Shawn Fanning, su creador, «siestero», porque se decía que dormía muchas siestas.

Navegador. *Browser*. *Software (ver)* que permite visualizar los documentos *web* generados mediante *HTML (ver)*. Los dos navegadores más utilizados en la *web* son el *Netscape Navigator (ver)* y el *Microsoft Explorer*, similares aunque con algunas prestaciones diferentes.

Netscape. Navegador de la empresa del mismo nombre.

Netiquette. Conjunto de normas de comportamiento y cortesía recomendado a los usuarios de Internet.

NIC. *Network Interface Card*. Tarjeta de interfaz de red. Dispositivo de *hardware (ver)* necesario para establecer comunicación entre dos ordenadores. Hay formas de conectar ordenadores sin *NIC*, p. ej. con módem *(ver)* y una línea telefónica, o por un cable serie.

Nodo. Cualquier punto de conexión a una red, ya sea punto terminal o intersección. En una red, cada computadora puede ser un nodo.

Nukear. Ataque informático malicioso, consistente en bloquear o causar trastornos a los ordenadores de otros usuarios.

On-line. En línea. Expresión con la que se designa el hecho de estar conectado a una red. En lenguaje coloquial, la mayor red en cuestión es normalmente Internet, por lo que, la expresión en línea, describe información que es accesible a través de Internet.

Off-line. Estado de un usuario que no dispone de conexión a una red.

Overclocking. Método utilizado por *hackers (ver)* o aficionados, consistente en forzar al procesador a trabajar más rápido de su velocidad.

P2P. *Peer to peer*. Red informática entre iguales. Red que no tiene clientes y servidores fijos, sino un servidor de modo que sus clientes o servidores son nodo de otros. Es el método utilizado para intercambio gratuito de videos, música… (p. ej., *Kazaa*…).

Páginas web. Páginas en lenguaje *HTML (ver)* que ofrecen información de todo tipo, ya sea como texto, gráficos, sonido o secuencias de vídeo. Habitualmente enlazan a otras páginas con información relacionada.
El conjunto de todas las páginas *web* integradas en Internet, es la w.w.w. (*world wide web*) *(ver)*, traducido como telaraña o malla mundial.

Passpack. Aplicación que permite mantener en el anonimato a los usuarios, usando códigos de acceso.

Password. Contraseña. Es una clave formada por un conjunto de caracteres y reservada a un usuario. Para que sea relativamente segura se recomienda un mínimo de ocho caracteres, y usar los cuatro grupos de caracteres del teclado: mayúsculas, míniscula, números y símbolos.

PDF. Formato gráfico desarrollado por *Adobe*, que reproduce un documento en formato digital para su posterior transmisión electrónica.

PGP. *Pretty Good Privacy* (privacidad bastante buena). Programa de criptografía que permite el cifrado y firmado digital de ficheros y documentos, y que a la vez garantiza la autenticidad e integridad del fichero o documento.

Pharming. Modalidad de fraude *on line (ver)*. Consiste en cambiar direcciones *DNS (ver)* de cualquier página de un usuario haciendo que la página que visita no sea la original.

Phising. Modalidad de fraude *on line (ver)* en la que se crea una página falsa, por ejemplo de un banco, de forma que los usuarios al entrar en ella introducen, engañados, sus datos bancarios. En ocasiones se llega a la página por mensajes que guían hasta la misma.

Phreaking. Conjunto de técnicas empleadas para *crakear (ver)* la red telefónica para, por ejemplo, poder realizar llamadas gratuitas a larga distancia.

Plug-in. Pequeños programas que se añaden al navegador y permiten mejorar la visualización de páginas multimedia.

Portal. Espacio *web*. En él es posible utilizar *chat (ver)*, correo y otros servicios.

Postmaster. Responsable, en un proveedor de Internet, de solucionar los problemas con el correo electrónico.

Proxy. Servidor o sistema cuya misión es hacer de intermediario entre un sistema y otro a través de Internet. Al ser intermediario entre la red privada e Internet puede restringir accesos.

Puerto. Punto de conexión para unir el ordenador con diferentes dispositivos, la impresora, módem *(ver)*, *scanner*…

Rabbit. Programa malicioso que provoca procesos inútiles repetidos hasta que colapsa el ordenador.

RDSI. Red Digital de Servicios Integrados. En inglés *ISDN* (*Integrated Services Digital Network*). Es una red que procede, por evolución, de la Red Digital Integrada (RDI), que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios. Sería admisible decir que procede por evolución de la red telefónica existente, que al ofrecer conexiones digitales de extremo a extremo permite la integración de multitud de servicios en un único acceso.

Remailer. Servicio de red que hace que el envío de un correo electrónico sea anónimo. Un *remailer* permite enviar mensajes de correo electrónico sin que el receptor sepa cómo se llama el emisor o cuál es su dirección de correo electrónico.

Router. Dispositivo que dirige el tráfico entre dos redes, normalmente conecta una red local con otra remota o con Internet.

SAID. Servicio Automático de Identificación Dactilar. Recoge no sólo las huellas dactilares e identificación de las personas reseñadas en investigaciones policiales, sino también las huellas latentes, localizadas sin identificación.

Scanning. Escaneo.Técnica antivirus (*a posteriori*), consistente en revisar el código de todos los archivos contenidos en la unidad de almacenamiento en busca de alguna parte del código que pertenezca al virus *(ver)*.

Script. Grupo de caracteres programado para automatizar una tarea que se realiza de forma muy habitual, por ejemplo una conexión a Internet.

Scriptkiddie. Hay quien lo considera la forma más baja del *cracker (ver)*. Es el término con el que se conoce a los que sin muchos conocimientos técnicos, utilizan códigos escritos por otros para sembrar estragos. Este grupo y sus próximos, los *packet monkeys* (literalmente, monos de los paquetes), son los autores de las anulaciones de *Yahoo* y *eBay*, aunque precisamente por su falta de formación dejan rastro suficiente para ser localizados

Servidor. Ordenador que permite a un usuario autorizado utilizar recursos y servicios de un ordenador remoto. El término obedece a que ese ordenador presta servicios a las otras máquinas o clientes. Los servicios pueden ser de todo tipo, almacenar o acceder a archivos, aplicaciones, de correo… Se les denomina también *host (ver)* y el hecho de publicar algo en ellos (p. ej, en *blogs*) *(ver)*, se denomina *hosting*, que se podría traducir como alojar lo escrito.

Shareware. Difusión de programas en el cual el autor ofrece o comparte el programa, normalmente por un tiempo determinado. A veces los que se ofrecen para distribución gratuita pueden ser un medio de difusión de virus *(ver)*.

SICC. Sistema de Inspección Control y Consulta de la Fiscalía General del Estado. Base de datos que recibirá periódicamente los datos más importantes de la actividad global de las Fiscalías y de los Fiscales en particular. Ha sido desarrollado por la Subdirección General de Nuevas Tecnologías del Ministerio de Justicia como herramienta para la Inspección Fiscal, la Secretaría Técnica y la Unidad de Apoyo. Mediante el sistema de búsquedas permite consultar expedientes y dictámenes, obtener datos del volumen de trabajo, elaborar estadísticas, así como determinar el tiempo que un procedimiento se encuentra en tramitación en un Juzgado.

SIS. Sistema de Información de Schengen. Base de Datos definida en el Acuerdo Schengen, como sistema informático con información sobre personas, documentos de identidad, armas de fuego, vehículos… El registro o señalamiento de datos tiene un periodo tras el cual se borra

automáticamente, salvo en el caso de personas. La Base de Datos de Señalamientos Nacionales (BDSN) responde al mismo concepto pero en el ámbito nacional español.

Sistema operativo. Es el enlace entre el *hardware (ver)* del ordenador y los programas de aplicaciones. Los más utilizados son *Windows*, *Unix-Linux*, *Macintosh*.

SIRENE. Organismo que se encarga de enlazar a los diferentes países firmantes del Acuerdo Schengen y que realiza labores de intercambio de información, envio de expedientes para detención provisional, resolver consultas y comprobaciones necesarias en determinados casos.

Skinning. Clonado de tarjetas de crédito.

Skype. Programa para llamadas gratis.

Sniffer. (Husmeador). Dispositivo que busca interceptar la información que circula por una red informática buscando una cadena numérica o de caracteres en los paquetes que atraviesan un nodo. *Sniffing* es, por tanto, un tipo de ataque informático en el que el objetivo es obtener información sin manipularla.

Software. Conjunto de programas y aplicaciones informáticas que hacen funcionar a un ordenador o que se ejecutan en él.

Spam. Envio masivo de mensajes publicitarios que invaden diariamente nuestro correo electrónico. También conocido como *junk mail (ver)*. A veces vienen con virus *(ver)* dentro. A pesar de que la mayor parte de empresas y administraciones cuentan con programas de seguridad *antispam*, resulta imposible acabar con esta auténtica plaga, so pena de restringir en exceso las comunicaciones.

Spoofing. De *spoof*, broma, o *to spoof*, engañar a alguien. Ataque informático, consitente en obtener el nombre y contraseña de un usuario legítimo, introducirse en un sistema y actuar en su nombre, enviando correos, etc… Permite la simulación de direcciones para engañar a otros ordenadores y hacerles creer que un mensaje se ha originado en una dirección que no es la suya. Es posible la simulación *IP (ver)*, la simulación *web*, la simulación *ARP* (Protocolo de resolución de direcciones), la simulación de *DNS* (sistema de nombres de dominios, que es el utilizado habitualmente para que el *hacker (ver)* cree su propio sitio *web* que coloca entre el usuario y el sitio real) *(ver)*… entre otras.

Spyware. Programa espía o aplicación maliciosa que se instala sin que el usuario lo advierta, normalmente al descargar otro programa.

Superzapping. Forma maliciosa o ataque a un programa para cambiarlo, destruirlo, copiarlo, introducir datos, o impedir su uso correcto.

Surfing. Lectura del *PIN* de quien teclea, utilizando para ello cualquier tipo de medio (el término abarca incluso los medios no informáticios, como el uso de una cámara de vídeo).

Sysop. *Sytem Operating* u Operador del sistema. El que se encarga de administrar y mantener una *BBS (ver)*. Es equivalente a *system adminstrator* o administrador *(ver)*.

Tablet PC. Alternativa al ordenador tradicional en el que es posible escribir directamente en la pantalla gracias a un bolígrafo especial.

Tag. Etiqueta *HTLM (ver)*. Instrucción que combinada nos permite crear una página *web*.

Tapefailure. Programa que ayuda a mantener vigilados a todos los usuarios que dependan de una red (páginas que visitan, grabar en video el tiempo que están conectados a la red, …).

TCP/IP. *Transmission Control Protocol/Internet Protocol*. Es el conjunto de protocolos de comunicaciones estándar en los que está basado Internet, y que regula la transmisión de datos a través de Internet.

TEDIS. *Trade Electronic Data Interchange Systems*. Programa aprobado en 1987 por la UE relativo a la transferencia electrónica de datos de uso comercial utilizando redes de comunicación.

Tip. Hay quien lo define como banco de sonidos, pero puede considerarse algo más en la medida que se trata de un proyecto de transformación de los residuos sonoros digitales mediante la interacción de múltiplas usuarios.

Tel net. Abreviatura de *Tele Network*. Emulador o protocolo de comunicaciones para la emulación de terminales que permite acceder a otro ordenador de forma remota.

Touched up. Técnica o resultado de alterar digitalmente fotografías, imágenes o archivos gráficos, en ocasiones con fines pornográficos para aparentar que los intervinientes son menores de edad.

Unix. Sistema operativo multiárea y multiusuario.

Usenet. *Unix Users Network*. Servicio al que se puede acceder desde Internet o desde *BBSs (ver)*, en el que se leen y envian mensajes o artículos, grupos de noticias o foros de discusión.

Vínculo. Enlace *(ver)*. *Link (ver)*.

Virus informático. Programas creados para alterar un sístema informático. Para poder ser catalogados como virus debe compartir las siguientes características: ocultos, dañinos (nunca es inocuo o inofensivo), se autoreproducen y su finalidad principal es la propagación.Hay diferentes teorías sobre sus creadores, desde los que afirman que son los propios fabricantes de *software (ver)*, para evitar plagios sin beneficio o, bien, expertos informáticos que los sacan para luego ofrecer la solución.
Se suelen clasificar como virus de archivo, de *macro*, de *boot (ver)* o sector de arranque, virus *Bat* y virus del *MIRC*.

WAN. *Wide Area Network*. Red de área amplia.

WAP. *Wireless Application Protocol*. Protocolo de aplicaciones inalámbricas. Protocolo de comunicaciones que permiten a un usuario de teléfono móvil acceder a Internet y ver información de la Red.

War Dialer. Programa que escanea la línea telefónica en busca de módems *(ver)*.

Warez. Término que incluye la piratería, el porno y el *HCPV*, esto es, *hacking (ver)*, *cracking (ver)*, *phreaking (ver)* y *virusmaking*.

Webcam. Cámara utilizada para la transmisión de imágenes a través de la *web*.

Webmaster. Persona encargada de la gestión y el mantenimiento técnico de un servidor de páginas *web* o de una *web* determinada.

Website. Sitio *web*. Conjunto de páginas *web* que comparten una misma dirección.

Wiretapping. Pinchado de líneas. Suele incluirse como uno de los supuestos de sabotaje informático.

w.w.w. *World wide web*. Conjunto de todas las páginas *web* de Internet.

You tube. Sitio de obtención de videos. *Google* se comprometió al adquirir *You tube* a crear un filtro automático que buscara y eliminara contenidos de su base de datos que estuviera protegido por *copyright*. Ofrecimiento que tiene que ver con las demandas frecuentes de proveedores por la presencia de vídeos en esas bases de datos sin los permisos de emisión.

Cuadernos penales José María Lidón

Los *Cuadernos penales José María Lidón* tienen un doble objetivo. Pretenden mantener viva la memoria del profesor y magistrado José María Lidón, asesinado por ETA, ya que relegarlo al olvido sería tanto como permitir que la insoportable injusticia de su muerte viniera a menos y, en cierta forma, hacerse cómplice de ella. Asimismo pretenden que su memoria sea un punto de encuentro para quienes desde cualquier profesión relacionada con el Derecho penal compartan, como compartimos con él, el anhelo por un Derecho que contribuya a crear cada vez más amplios espacios de libertad e igualdad y a que éstas sean reales y efectivas para todos. De este modo su memoria será doblemente enriquecedora.

CONSEJO GENERAL
DEL PODER JUDICIAL
AGINTE JUDIZIALAREN
KONTSEILU NAGUSIA

EUSKO JAURLARITZA
GOBIERNO VASCO
JUSTIZIA, LAN ETA GIZARTE
SEGURANTZA SAILA
DEPARTAMENTO DE JUSTICIA,
EMPLEO Y SEGURIDAD SOCIAL

Universidad de
Deusto

Deustuko
Unibertsitatea