La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales

Prof. Dr. Alfonso Galán Muñoz

Profesor Titular de Derecho penal.
Universidad Pablo de Olavide

Revista Penal, n.º 24.—Julio 2009

RESUMEN: *El presente artículo analiza el modo en que la internacionalización del Derecho penal y procesal penal referido a la denominada criminalidad informática, ha incidido en el panorama normativo español relativo a dicha materia. Se presta especial atención al modo en que dicha normativa ha influido en las reformas propuestas con respecto a la posible tipificación penal de las conductas de* Hacking *y a las que se han ocupado de la investigación y persecución penal de los delitos cometidos en Internet.*

PALABRAS CLAVE: *Delincuencia informática. Derecho penal internacional.* Hacking. *Interceptación de comunicaciones. Investigación y persecución de delitos en Internet. Datos de tráfico. Proveedores de servicios.*

ABSTRACT: *In the present papers is analyzed the way in which the internationalization of criminal process and law about computer crimes has influenced on the Spanish law. Special attention is paid to investigate the way in which this law has influenced on the punishment of the Hacker´s behaviour as well as on the regulation of investigation and prosecution of the Cybercrimes.*

KEYWORDS: *Computer crimes. Internacional criminal law. Hacking. Interceptetion of Communications. Investigation and prosecution of cybercrimes. Trafic data. Server providers.*

1. Introducción

Vivimos tiempos de cambios; tiempos en los que las viejas realidades nacionales son cada vez más puestas en entredicho por fenómenos políticos, económicos y técnicos a los que no pueden hacer frente por sí solas[1].

Los enormes avances técnicos y la facilidad del transito de personas, de capitales y de información a nivel mundial han llevado a que ningún país del mundo pueda controlar todas las actividades que tienen o pueden tener efectos, incluso delictivos, dentro de sus fronteras.

Terrorismo, tráfico de drogas, blanqueo de capitales, tráfico ilegal de personas, etc. Los ejemplos de delincuencia transnacional son múltiples y cada vez más numerosos.

Sin embargo, si hay un campo en el que se ha mostrado lo inútiles que pueden resultar los esfuerzos exclusivamente nacionales por controlar los peligros que genera el uso de las nuevas tecnologías, es en el ámbito de lo que se ha venido a denominar como delincuencia o criminalidad informática[2].

Nadie discute que la implantación de los modernos sistemas de tratamiento de datos ha abierto enormes posibilidades al desarrollo del conocimiento y de las relaciones humanas en todo el mundo, pero tampoco parece que nadie puede negar que al hacerlo también se han

1. SIEBER, U., «Límites del Derecho Penal». *Revista Penal*, n.º 22, 2008, págs. 134 y ss.

2. Sobre este concepto y su evolución véase, de forma general GALÁN MUÑOZ, A., «Expansión e intensificación del Derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas en materia de criminalidad informática» en *Revista Derecho y Proceso penal,* n.º 15, 2006, pág. 14.

abierto las puertas a nuevas posibilidades de abusos y a nuevos peligros que deberían ser controlados y neutralizados por quien supuestamente ha de protegernos de ellos, el Estado.

Sin embargo, el Estado nacional, como bien señala BECK, ha perdido la completa soberanía que antes ostentaba sobre el flujo de información que se desarrollaba dentro de sus fronteras[3]. Ningún país puede controlar lo que un sujeto transmite o hace desde el territorio de otro mediante las modernas redes de comunicación y, sin embargo, dichas actividades sí pueden tener notables efectos dentro de sus fronteras[4].

La marcada transnacionalidad de los denominados delitos informáticos ha llevado a que los Estados necesiten y requieran la colaboración de otros Estados para perseguirlos y castigarlos, con lo que cada vez se producen más contactos, conflictos y fricciones entre las distintas regulaciones nacionales referidas a los mismos.

La disparidad de criterios nacionales a la hora de solucionar los problemas que plantea el mundo de las nuevas tecnologías es inmensa y así nos encontramos con que lo que en algunos países puede ser considerado como algo tan intolerable que ha de ser penalmente perseguido (p. ej., la difusión de pornografía entre adultos en Internet), en otros constituye algo no sólo permitido sino completamente lícito que da lugar a una poderosa industria generadora de cientos de millones de dólares de beneficios al año.

Realizar un cierto acercamiento o armonización entre las distintas legislaciones nacionales referidas a este nuevo mundo resulta imprescindible, ya que de lo contrario podríamos encontrarnos con que algunos países podrían convertirse en verdaderos *safe harbour* o en «paraísos de la criminalidad informática» desde los que se podrían cometer delitos con total impunidad. Este hecho ha llevado a que el denominado Derecho penal informático se nos presente como uno de los ejemplos más paradigmáticos de la internacionalización y del incremento de la «interlegalidad» que caracteriza al Derecho penal de nuestro tiempo[5].

Ahora bien, esta internacionalización del Derecho penal, difícil e incluso cuestionable en algunos aspectos[6], puede presentar dos vertientes bien diferenciadas.

Por una parte, puede ser una armonización «extensiva» que dé lugar a la incriminación de nuevas conductas y a la creación de nuevos delitos en los ordenamientos jurídicos nacionales para atender a las nuevas necesidades de protección que tienen las sociedades de la Información. Pero, por otra parte y en sentido contrario, también puede ser una armonización «limitadora» o restrictiva que venga a extender unos estándares de garantías mínimas que todos los países deberían reconocer a sus ciudadanos, con lo que limitaría el posible ejercicio del *ius puniendi* nacional en este concreto ámbito[7].

Ahora bien, pese a la existencia de esta evidente dicotomía, la realidad nos demuestra que son pocos, como veremos, los instrumentos internacionales que hablan de las garantías jurídicas que ha de tener el ciudadano frente al Estado y muchos, sin embargo, los que recomiendan o incluso obligan a los Estados a crear nuevos delitos y a articular nuevos sistemas de investigación penal para protegernos de esos enormes y, en algunos casos, casi míticos peligros que nos acechan tras las aparentemente inocentes pantallas de nuestros ordenadores.

De hecho, el aluvión de reformas legislativas referidas a la denominada «criminalidad informática» producidas en nuestro Código penal en los últimos años ha sido importante e incesante, jugando las distintas normas internacionales un papel decisivo en su proliferación. Veamos algunos de los últimos ejemplos de este fenómeno.

---

3. BECK, U., *¿Qué es la globalización?*, Ed. Paidós, Barcelona, 2008, pág. 49. En el mismo sentido SIEBER, U., quien afirma que *«... Un control estatal de los caudales de datos en los límites territoriales es difícilmente posible»*. En «Límites del Derecho penal» (...), pág. 127. En el mismo sentido, CASTELLS OLIVÁN, M., *La era de la información. Economía, sociedad y cultura: 2. El poder de la identidad,* Ed. Alianza, Madrid, 1998, pág. 287.

4. Véase sobre este carácter de la criminalidad informática, de forma más amplia GALÁN MUÑOZ, A., «Expansión e intensificación del Derecho Penal de las nuevas tecnologías: una análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», *Revista Derecho y Proceso penal,* n.º 15, 2006-1, págs. 20 y 21. MATELLANES RODRÍGUEZ, N., por su parte, llega a afirmar que *«La transnacionalidad de sus efectos es, posiblemente, el rasgo más sobresaliente de la delincuencia informática»*. En «Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)», *Revista Penal* n.º 22, 2008, pág. 55.

5. En este sentido, VOGEL, J., considera a la «interlegalidad», a los cambios e intercambios que los contactos entre los distintos ordenamientos jurídicos regionales, nacionales e internacionales, como uno de los fenómenos más característicos de nuestro tiempo, ya que, resulta evidente que todas las ramas de nuestros ordenamientos jurídicos nacionales, y la penal no es ninguna excepción, están cada vez más condicionadas e influenciadas por instrumentos jurídicos desarrollados más allá de nuestras fronteras. «La internacionalización del Derecho penal», *Revista Penal*, n.º 22, 2008, pág. 161.

6. Piénsese, por ejemplo, en los evidentes déficits democráticos que presentan muchos de los instrumentos internacionales que dan lugar a este nuevo Derecho. Sobre este problema véase de forma general, BECK, U., ¿Qué es la globalización? (...), pág. 182 y ss., o lo comentado por VOGEL, J. con respecto al Derecho penal internacional en «La internacionalización del Derecho penal» (...), pág. 167, entre otros.

7. VOGEL, J., «La internacionalización del Derecho penal» (…), pág. 163.

2. La incidencia de las normas internacionales sobre el Derecho penal español referido a las nuevas tecnologías

Resulta imposible analizar, siquiera de una forma sintética, todas las normas penales que nuestro legislador ha ido creando en materia de criminalidad en los últimos años y que tienen su origen, o se han visto marcadamente influenciadas por la normativa internacional referida a esta clase de criminalidad.

Muchos de los nuevos delitos que nuestro Código establece para reprimir conductas realizadas mediante sistemas informáticos y que supuestamente atentan contra bienes jurídicos como el patrimonio, la propiedad intelectual o incluso de la indemnidad sexual de los menores, encuentran un precedente internacional en su creación.

Parece que la alusión al origen internacional de cualquier nuevo tipo delictivo le otorga un halo de indiscutible legitimidad incriminadora, atendiendo al siguiente planteamiento: si todos o muchos países señaladamente democráticos se han puesto de acuerdo a la hora de entender que una conducta debe ser penalmente perseguida y sancionada, ¿cómo es posible que puedan haberse equivocado o que se hayan excedido al hacerlo?

Se entiende entonces por qué el legislador alude cada vez más frecuentemente en las exposiciones de motivos de sus últimas reformas a exigencias internacionales a la hora de justificar la incriminación de conductas tan alejadas de la efectiva lesión del bien jurídico que supuestamente se pretende proteger con su tipificación como la tenencia o creación de instrumentos específicamente destinados a desproteger programas de ordenador[8], el simple suministro de información sobre el modo de conseguir el acceso no autorizado a un medio de acceso condicional[9], la posesión de pornografía infantil para el propio consumo o las referidas a la producción de pornografía en la que no interviniendo realmente menores se utilice su imagen o su voz alterada o modificada[10], entre otras.

No importa que algunos de estos delitos resulten difícilmente compatibles con las más básicas exigencias derivadas de principios penales tan esenciales como el de intervención mínima o el de subsidiaridad, ni con las derivadas de otros más generales como el de proporcionalidad. Todo parece quedar olvidado desde el mismo momento en que se alude a su ascendiente u origen internacional.

Así, por ejemplo, ¿cómo se puede justificar que quien se limita a tener un instrumento destinado a desproteger programas informáticos pueda ser sancionado con la misma pena que a aquel que lo usa y con ello ocasiona una efectiva lesión patrimonial al titular de los derechos de explotación que recaen sobre el mismo? ¿No se encuentra dicha conducta tan alejada de la efectiva lesión patrimonial que debería ser considerada como un mero acto preparatorio de los delitos que castigan esta última afección?

¿Por qué razón defraudar a una compañía que suministre los modernos servicios de acceso condicional (p. ej., servicios televisivos de pago por visión) se castiga como delito con independencia de la cuantía de la defraudación producida, y defraudar a compañías que prestan otros servicios más tradicionales (p. ej., suministro de agua o de luz) sólo constituye delito si se demuestra que el perjuicio que se les ha producido supera los 400 euros?

¿Realmente se afecta a la indemnidad sexual de un menor cuando se utiliza su voz o su imagen alterada sin su conocimiento en la producción de pornografía realizada con mayores de edad? ¿Éste es el bien jurídico que trata de proteger este delito? ¿O es que este delito más que proteger al menor trata de perseguir a todo aquel que tenga o que fomente o favorezca las tendencias pedófilas (que no pederastas) de terceros?

Como se puede comprobar, los problemas de legitimidad que presentan todos estos delitos, pese a su ascendiente internacional, no son pocos ni pequeños, con lo que no parece que la mera referencia del legislador español a la existencia de una obligación internacional, previamen-

8. El origen europeo de este delito contemplado en el actual art. 270.3 CP es puesto de manifiesto por GÓMEZ MARTÍN, V., «El art. 270.3: breve historia de un despropósito» en *Eguzkilore. Cuaderno de Instituto Vasco de Criminología,* n.º 21, 2007, págs. 82 y ss. MATA Y MARTÍN, R., «Protección penal de la propiedad intelectual y servicios de radiodifusión e interactivos: excesos y equívocos. Su continuación en la reforma de 25.11.03» en *Estudios penales en homenaje al profesor Cobo del Rosal,* Ed. Dykinson. Madrid, 2005, pág. 627, o DEL ROSAL, B./MIRÓ LLENARES, F., *Comentarios al Código penal*. Tomo VIII, Ed. Edersa, Madrid, 2005, pág. 911, entre otros.

9. Sobre el origen internacional, primordialmente europeo, de este delito y los problemas que el mismo plantea véase GALÁN MUÑOZ, A., «El Derecho penal español ante la piratería de los servicios de radiodifusión» en *Eguzkilore. Cuaderno del Instituto Vasco de Criminología,* n.º 21, 2007, págs. 65 y 76 y ss., o MOYA FUENTES, M., «La alteración y duplicación del número indentificativo de equipos de telecomunicaciones, su comercialización y su utilización: art. 286.2 y 4 CP», *RECPC* 11-02 (2009), pág. 02:2 (http://criminet.ugr.es/recpc (últ. vis. 12-2-2009).

10. Sobre la influencia que ha tenido la normativa internacional sobre estas incriminaciones supuestamente protectoras de la indemnidad sexual de los menores, véase, por todo, GARCÍA VALDÉS, C., «Acerca del delito de pornografía infantil» en *Estudios en Recuerdo del profesor Ruiz Antón*. Ed. Tirant lo Blanch. Valencia, 2004, págs. 411 y ss.; SANS MULAS, N., «Pornografía en Internet», *Revista Penal* n.º 23, 2009, págs. 186 y ss., o MORALES PRATS, F., «Los ilícitos en la red (II): pornografía infantil y ciberterrorismo» en *El cibercrimen: nuevos retos jurídico-penales nuevas respuestas político-criminales*. Ed. Comares, Granada, 2006, págs. 280 y ss., entre otros.

te adquirida, de crearlos pueda servir para ocultarlos ni para justificarlos.

Sin embargo, la existencia de todos estos problemas no ha supuesto óbice alguno para que nuestro legislador haya vuelto a utilizar al «legislador internacional» como justificación o coartada de la incriminación de nuevas conductas referidas al uso o al abuso de las modernas tecnologías de la información que se contienen en el último, por el momento, anteproyecto de modificación del Código Penal.

En concreto, el citado anteproyecto alude a 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, para justificar el incremento punitivo que se produce en todos los delitos referidos a la indemnidad sexual de menores, entre los que se encuentran —como no podía ser de otro modo—, uno no propiamente informático pero que cada vez está más vinculado al uso de las nuevas tecnologías de la información, como es el delito de distribución de pornografía infantil del art. 189 CP.

Pero también y por otra parte, la citada Exposición de Motivos alude a la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información para justificar una reforma del delito de daños informáticos que distanciará a este delito aún más, y sin motivo aparente, del resto de los delitos de daños[11] y, sobre todo, para legitimar el castigo de una conducta que hasta el momento se ha mantenido en el ámbito de lo atípico y sobre cuyo merecimiento y necesidad de pena la doctrina patria no ha llegado a ponerse de acuerdo, la referida a los accesos no autorizados a sistemas informáticos ajenos.

Para algunos autores, la incriminación de estas conductas resulta necesaria, ya que, a pesar de que muchas de ellas no ocultan sino verdaderos actos ejecutivos de delitos contra la intimidad o contra el patrimonio, pueden llegar a quedar impunes al ser difícil de probar que se realizaron con la concurrencia de los elementos subjetivos que permitirían castigarlos como tentativas de alguno de dichos delitos (p. ej., la intención de descubrir secretos o el dolo de dañar o perjudicar, etc.)[12].

Por el contrario, y frente a esta postura, se alzan las voces de quienes entienden que muchas de estas intromisiones no se realizan con dichas intencionalidades delictivas, sino por el mero reto intelectual de demostrar que se está capacitado para vulnerar las posibles medidas de seguridad que el titular del sistema informático hubiese establecido para evitar que se pudiese acceder al mismo[13]. De hecho, se señala que muchas de ellas ni siquiera presentan dañosidad objetiva alguna que pueda justificar su castigo conforme a los referidos tipos delictivos, por cuanto ni ponen en peligro el patrimonio del dueño del sistema informático vulnerado, ni inciden sobre ordenadores que contengan informaciones que puedan ser consideradas como datos personales o secretos de carácter personal o de

11. En concreto, ha de señalarse que si la actual regulación del delito de daños ya da lugar a que se pueda pensar que los daños que consistan en la destrucción o alteración de los elementos lógicos de un sistema informático son castigados por un delito (el contenido en el actual art. 264.2 CP), completamente autónomo y diferente del contemplado en el tipo básico del delito de daños del art. 263 CP, parece que la regulación propuesta confirmará definitivamente dicha impresión al exigir tan sólo que el daño informático producido se realice de forma «grave» para poder considerarlo como delito. Parece que así se quiere desvincular definitivamente al injusto propio de este nuevo delito de la efectiva constatación y valoración de la lesión patrimonial ocasionada con su realización. El valor de la merma patrimonial producida podrá y deberá ser tenido en cuenta a la hora de valorar la gravedad de la conducta típica realizada, pero no tendrá la misma importancia y valor que tiene en el resto de delitos de daños, donde actúa como referente delimitador esencial del delito y la falta. La afección patrimonial no será ya el único referente de la valoración del injusto típico propio del delito de daños informáticos, y este hecho dará lugar a que recobren fuerza aquellas opiniones que defienden que este delito tendrá que entrar en concurso de delitos y no de leyes con aquel otro que valorase el daño patrimonial ocasionado a los elementos materiales o físicos del sistema informático afectado, lo que determinaría, por ejemplo, que cuando se produjese la destrucción de los datos y la del soporte físico en el que estos estaban almacenados no se pudiese apreciar un único delito de daños sino dos. Esta solución concursal resulta a nuestro modo de ver algo más que cuestionable, lo que ha llevado a algunos autores, como GONZÁLEZ RUS, J.J., a tratar de solucionarla incluyendo en los daños castigados y valorados por el art. 264.2 CP (los daños informáticos) a los que pudiesen recaer sobre los soportes en «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*. Ed. Comares, Granada, 2006, pág. 259; solución que, sin embargo, es cuestionada, a mi juicio de forma correcta, por MATA Y MARTÍN, R.M., *Delincuencia informática y Derecho penal,* Ed. Edisofer, Madrid, 2001, pág. 65 y que, además, quedará totalmente excluida si llega a entrar en vigor la comentada reforma.

12. GUTIÉRREZ FRANCÉS, María L., «El intrusismo informático (Hacking): ¿represión penal autónoma?». *Informática y derecho: Revista iberoamericana de derecho informático*, n.º 12-15, 1996, pág. 1180, y GONZÁLES RUS, J.J., quien considera que será realmente excepcional el caso en el que la intromisión ilícita no esté animada por ninguna finalidad ilícita. «Los ilícitos en la red (I): ...» (...), pág. 247.

13. ORTS BERENGUER, E./ROIG TORRES, M., «Delitos contra la intimidad, utilización fraudulenta de tarjetas de crédito y falsedad en documento electrónico»: Análisis de casos» en *Incorporación de las nuevas tecnologías en el comercio: aspectos legales, Estudios de Derecho Judicial*, 71. Madrid, 2005, pág. 92. MATELLANES RODRÍGUEZ, N. en «Vías para la tipificación del acceso ilegal...(I)» (...), págs. 63 y 64. Con mayor extensión MORÓN LERMA, E., *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red,* Ed. Aranzadi, Pamplona, 2002, págs. 55 y ss.

empresa de los que protegen los delitos de los arts. 197 y 278 del CP[14].

Este hecho, unido a la inexistencia de un tipo delictivo específico que venga a sancionar estas conductas, ha llevado a la mayoría de la doctrina española actual a entender que el ordenamiento penal español considera, por el momento, a los meros accesos no autorizados a sistemas informáticos ajenos o conductas de *Hacking blanco* como actuaciones completamente irrelevantes y atípicas a efectos penales[15]. Y digo por el momento porque evidentemente esto cambiará si se llega a aprobar, y entra en vigor, el proyecto de reforma que venimos comentando, que viene a introducir un nuevo apartado 3 en el art. 197 de nuestro Código penal, en el que se establece que:

> «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».

Como fácilmente se podrá deducir, este precepto convierte o pretende convertir en delito al mero intrusismo informático, es decir, al simple acceso no autorizado a un sistema informático ajeno, opción legislativa que se corresponde perfectamente con las tendencias internacionales contenidas no sólo en la ya citada la Decisión Marco 2005/222/JAI, cuyo art. 2 obliga a todos los Estados miembros de la Unión a sancionar penalmente los accesos ilegales a los sistemas de información[16], sino también con las contempladas en otros instrumentos internacionales, como sucede con el art. 2 del Convenio del Consejo de Europa sobre criminalidad informática, firmado en Budapest el 23 de noviembre de 2001[17] y que está abierto a la firma de cualquier país y no sólo de los países europeos[18].

Nos encontramos con un delito que castiga el acceso no autorizado aunque no se realice con ninguna finalidad añadida a la de la consecución del acceso en sí mismo. Tampoco es un delito que requiera la constatación de una puesta en peligro siquiera hipotética del patrimonio o de los secretos individuales de los titulares de los sistemas informáticos afectados para su apreciación, por lo que no debe sorprendernos que algunos autores consideren que no estamos ante un delito que castigue la puesta en peligro de un bien jurídico individual, sino ante uno que sanciona la efectiva lesión de un nuevo bien jurídico de carácter netamente informático y dotado de una naturaleza claramente colectiva: la seguridad informática[19].

En concreto, se podría considerar que este delito sería un delito de mera actividad pero también de efectiva le-

14. Entre otros, ORTS BERENGUER, E./ROIG TORRES, M., «Delitos contra la intimidad...» (...), págs. 92 y ss., o 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 *Derecho a la intimidad y nuevas tecnologías,* Cuadernos de Derecho Judicial IX, 2004, pág. 119.

15. MORÓN LERMA, E., *Internet y Derecho penal: (...),* pág. 64, GONZÁLES RUS, J.J., «Los ilícitos en la red (I):..» (...), pág. 246; GALÁN MUÑOZ, A., «Ataques contra sistemas informáticos» (...), págs. 226 y 227.

16. En concreto, el citado artículo establece que «art. 2. Acceso ilegal a los sistemas de información.

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». Un análisis más detallado de las exigencias y problemas que presenta esta normativa al ordenamiento jurídico penal español se puede encontrar en GALÁN MUÑOZ, A., «Ataques contra sistemas informáticos» (...), págs. 225 a 232.

17. «Artículo 2. Acceso ilícito. 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».

18. Véase en este sentido lo establecido por el artículo 2 del Convenio con respecto a este tipo de conductas, comentado entre otros por MORALES GARCÍA, Ó., «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-crime» en *Delincuencia informática. Problemas de responsabilidad.* Cuadernos de Derecho Judicial IX, 2002, pág. 27; LÓPEZ ORTEGA, J.J., «Intimidad informática y Derecho penal…», pág. 12; CARRASCO ANDRINO, M.M., «El acceso a un sistema informático» en *La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea,* Ed. Tirant lo Blanch, Valencia, 2009, pág. 346.

19. GUTIÉRREZ FRANCÉS, María L., «El intrusismo informático (Hacking): ...» (...), págs. 1163 y ss.; LÓPEZ ORTEGA, J.J., «Intimidad informática y Derecho penal…» (…), pág. 120; postura que parece seguir MATELLANES RODRÍGUEZ, N. en «Vías para la tipificación del acceso ilegal... (I)» (...), pág. 67, si bien, posteriormente limita esta consideración sólo a los accesos informáticos que denomina «no personales» o de uso público, caracterizados por no contener informaciones de sujetos particulares en «Vías para la tipificación del acceso ilegal a los sistemas informáticos (II)», *Revista Penal*, n.º 23, 2009, págs. 66 y ss. CARRASCO ANDRINO, M.M., por su parte, critica la ubicación otorgada por el anteproyecto al comentado delito, precisamente, por considerar que éste nada tiene que ver con la intimidad, lo que le lleva a abogar por su inclusión dentro un nuevo capítulo que se debería ubicar en sede de delitos contra la seguridad colectiva, «El acceso a un sistema informático» (…), págs. 355 y ss.

sión, ya que, la simple realización de su conducta típica (el acceso) lesionaría, siempre y en todo caso, a ese nuevo bien jurídico colectivo que se delimita mediante el concepto de seguridad informática[20].

Sin embargo, y frente a esta concepción, siempre he defendido que lo que se afecta o se puede afectar por la realización de este tipo de conductas no es ningún bien jurídico colectivo, sino uno eminentemente individual.

De hecho, parece evidente que considerar que el acceso a un único sistema informático afecta o incluso lesiona la seguridad de los sistemas informáticos en general, supone desdotar de cualquier contenido material de injusto a la supuesta afección de este nuevo bien jurídico de carácter colectivo.

¿En qué me afecta a mí que se acceda al ordenador de mi vecino o al de un completo desconocido? ¿Qué lesión o, cuando menos, qué puesta en peligro sufre el sistema informático de mi despacho, el de mi casa o el de cualquier otro sujeto como consecuencia de dicha intromisión? Es más, ¿se afecta a algún otro ordenador distinto del accedido cuando se accede al mismo sin autorización?

La respuesta a mi juicio es evidente e inmediata. El acceso no autorizado a un sistema informático no afecta sino al sistema que es accedido.

Ninguna afección real de índole colectiva o supraindividual se produce con tal conducta, luego se tendrá que entender que lo que se ve afectado por este tipo de actuaciones no es la seguridad de todos los sistemas informáticos, sino un valor de corte netamente individual y de naturaleza claramente informática que sólo puede ser protegido frente a los ataques informáticos más graves y más peligrosos que se realicen contra el mismo.

En concreto, y a mi juicio, nos encontramos ante un delito que protege un nuevo bien jurídico que, pese a tener una naturaleza netamente informática, presenta notables similitudes con otro de corte tradicional y eminentemente individual, la intimidad.

De hecho, considero que nos encontramos ante un delito que protege un nuevo derecho cercano al derecho fundamental a la intimidad pero diferente de éste. Se protege el derecho a la inviolabilidad informática, entendiendo por tal a aquel derecho instrumental y puramente formal que permite o faculta a toda persona a mantener sus sistemas informáticos y, sobre todo, a los datos y a los programas contenidos en los mismos al margen de intromisiones ajenas no deseadas.

Estamos hablando de una suerte de privacidad o, más bien, de inviolabilidad informática que presentaría notables similitudes con aquellas otras inviolabilidades como la del domicilio[21] o la de las comunicaciones, que el ordenamiento jurídico en general y el Derecho penal en particular ha protegido para convertir, dichos ámbitos o medios, en reductos especialmente protegidos frente a intromisiones ajenas en los que las personas puedan desarrollar y ejercer su derecho fundamental a la intimidad de la forma más libre y abierta posible[22].

Una vez que se ha negado cualquier posible y casi «mística» afección de valores colectivos en la realización de un simple acceso no autorizado, tendremos que entender que esta conducta está lejos de ser esa peligrosísima actuación para la «seguridad informática» de todos, de la que algunos hablan, y pasa a convertirse en lo que realmente es, una actuación desviada e injusta, pero que tan sólo atenta contra un bien jurídico de naturaleza individual (la inviolabilidad informática), con lo que presenta un desvalor de injusto tan nimio que no debería ser castigada con una pena tan grave como la que le podría corresponder a aquellas otras actividades que si viniesen a atentar contra la seguridad de todos los sistemas informáticos.

---

20. En este sentido, habla MATELLANES RODRÍGUEZ, N., de la presencia de un bien jurídico intermedio y señala que «… el delito, se comporta como una forma de lesión efectiva para la seguridad del sistema informático, dada la vulneración de las medidas de seguridad, pero, al propio tiempo, el acceso al dato que este quebranto implica deja paso a una afección, por lo menos en grado de tentativa y por tanto de riesgo concreto, respecto a otros bienes jurídicos individuales, ya tutelados en otros delitos en función del ánimo inherente a la acción del sujeto» en «Vías para la tipificación del acceso ilegal... (II)» (...), pág. 70. Otros, sin embargo, como LÓPEZ ORTEGA, J.J., iban un paso más allá y afirmaban que este delito se configuraría como un delito de peligro abstracto para la seguridad de los sistemas informáticos, que no requeriría la efectiva vulneración de dicho bien jurídico para alcanzar la consumación y que actuaría como barrera de contención protectora de dicho bien jurídico «Intimidad informática y Derecho penal (…)», pág. 120.

21. No debe sorprender, por tanto, que el CP italiano ubique el delito de acceso abusivo del art. 615-ter entre los que tutelan la inviolabilidad domiciliaria, aunque a mi juicio la cercanía conceptual entre ambas inviolabilidades no puede llevar a confundirlas, por lo que no sorprende que MORALES GARCÍA LAS trate hablando de una suerte de «domicilio informático» en «Apuntes de política criminal en el contexto tecnológico...» (...), pág. 28. Sobre la tipificación italiana y su concreta problemática véase CARRASCO ANDRINO, M.M., «El acceso a un sistema informático» (…), págs. 348 y ss.

22. Ya defendí este concepto de la inviolabilidad informática, como derecho individual cercano y mediatamente protector de la intimidad pero diferente de ella, en un trabajo anterior, si bien consideré necesario incluir el delito que vendría a protegerlo en un capítulo autónomo que remarcase la autonomía y especificidad de su injusto con respecto al que configura el resto de delitos protectores de otras facetas o aspectos de la intimidad. Véase en tal sentido, GALÁN MUÑOZ, A., «Ataques contra sistemas informáticos» (...), pág. 228; propuesta que no ha sido acogida por el legislador que ha optado por incluir este delito dentro del artículo referido al descubrimiento y revelación de secreto, lo que, a mi juicio, puede generar confusión sobre la concreta naturaleza jurídica de este delito, dando lugar a innecesarios problemas concursales.

Se protege la inviolabilidad de los sistemas informáticos individuales como posibles contenedores de información sensible para la intimidad y es precisamente por ello, por lo que el tipo delictivo propuesto no tutela a los sistemas informáticos en sí mismos considerados (el hardware), sino a la información que contienen.

¿Qué sentido tendría castigar a la persona que accede sin consentimiento a la BIOS o al disco duro completamente vacío del ordenador de un tercero?

Evidentemente, ninguno.

Lo que realmente dotaría de contenido material al injusto de este delito no es el mero acceso a los sistemas[23], sino el acceso a los datos o programas que contienen. No es necesario que los sistemas informáticos contengan documentos electrónicos propiamente dichos, ni informaciones secretas, ni datos de carácter personal[24]. Tampoco que el intruso llegue a conocerlos o a entenderlos. Ni siquiera se requiere que los datos contenidos representen realidades o conceptos comprensibles para el sujeto. Lo que se requiere es que se acceda a algún dato o programa informático contenido en un sistema informático, ya que, si se accede de forma no autorizada a un sistema completamente vacío, nos encontraríamos ante una actuación que resultaría completa y absolutamente inocua para el bien jurídico protegido, con lo que debería permanecer en el ámbito de la más absoluta atipicidad.

Esta concepción, por otra parte, se ajusta, a mi juicio, en mucha mejor medida, con las propias exigencias del Derecho Internacional, esto es, tanto con las del art. 2 del Convenio sobre Criminalidad Informática del Consejo de Europa, como con las contenidas en el artículo segundo de la Decisión Marco de la Unión sobre Ataques Informáticos; normas ambas que exigen que todos los países afectados por las mismas castiguen penalmente el acceso no autorizado tanto a todo o como a una parte del sistema informático, exigencia que, a mi modo de ver, pone de manifiesto que lo que se quiere proteger no es tanto al sistema informático como unidad material y física en sí misma considerada, como a los elementos lógicos el mismo contiene, esto es, a los datos y a los programas informáticos que estén en él almacenados.

Esta concepción tiene otro importante efecto típico, ya que, va a resultar decisiva a la hora de fijar y delimitar qué consentimiento o autorización ha de concurrir para que el acceso realizado deje de ser típico.

Si se considera que el delito de Hacking debe proteger la seguridad de los sistemas informáticos ilegítimamente accedidos y, en consecuencia, se afirma que su injusto se consuma en el momento en que se consigue acceder al sistema físicamente considerado, se tendría que entender —como proponen algunos autores y se propugna en las reformas legislativas de algunos países (p. ej., Brasil)[25]—, que si concurre la autorización del legítimo titular del sistema accedido con respecto al acceso efectivamente realizado, éste, el acceso, dejará de ser penalmente relevante y pasará a ser completamente atípico[26].

Parece que nada se podría reprochar a esta postura más allá de su evidente falta de congruencia con el carácter supraindividual que quienes la defienden pretenden dar al bien jurídico protegido por dicho delito, ya que, sólo si se considera, como aquí se hace, que dicho delito tiene una naturaleza netamente individual y no una colectiva, se podrá llegar a entender que el consentimiento de un único sujeto (el del titular del sistema informático en este caso) pueda llegar a determinar la total atipicidad del acceso realizado.

Sin embargo, la exigencia de la ausencia de consentimiento por parte del titular del sistema informático accedido para configurar el injusto típico de este delito plantea un problema práctico mucho más grave que el derivado de esta evidente falta de congruencia técnica, ya que parece obligar a entender que cuando un sujeto guarda sus datos en un ordenador ajeno, sólo podrá acceder a los mismos si cuenta con el consentimiento del titular de dicho sistema, mientras que este sujeto, el titular del ordenador, podrá acceder a dichos datos siempre que quiera.

Se llegaría así a la absurda situación de que si utilizásemos un servicio de almacenamiento de datos ajeno con la finalidad de guardar en él cualquier clase de datos que no tuviese la consideración de secreto o si alquilásemos un ordenador para crear un programa de nuestra propia invención y almacenarlo en su disco duro, sólo podríamos acce-

23. Así lo entienden en España MATA Y MARTÍN, R.M., «La protección penal de datos como tutela de la intimidad de las personas y las nuevas tecnologías», *Revista Penal,* n.º 18, 2006, pág. 235, MATELLANES RODRÍGUEZ, N. en «Vías para la tipificación del acceso ilegal... (I)» (...), pág. 63.

24. No existe solapamiento alguno entre este delito con el del art. 197.2 CP, como bien señala CARRASCO ANDRINO, M.M., «El acceso a un sistema informático» (…), pág. 356, ni tampoco con el del primer apartado del mismo artículo, el referido al apoderamiento de secretos de carácter personal, puesto que los datos contenidos protegidos por este delito, como señala MATELLANES RODRÍGUEZ, N., puede ser «… cualquiera, no necesariamente un dato personal o un dato que denote un aspecto íntimo de la persona» en «Vías para la tipificación del acceso ilegal... (II)» (...), pág. 61.

25. En concreto, el nuevo art. 285-A —contemplado en el por el momento proyecto de reforma del Código penal brasileño— trata de crear el delito de acceso no autorizado a redes, dispositivos de comunicación o sistemas informáticos, al establecer que será delito el «... Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida», conducta que se pretende sancionar con pena de «reclusão, de 1 (um) a 3 (três) anos, e multa».

26. Así lo afirma expresamente en nuestra doctrina CARRASCO ANDRINO, M.M., al señalar que «… el legitimado para autorizar es el titular del sistema informático en el que se contienen los datos o programas informáticos, ya sea persona física o jurídica» en «El acceso a un sistema informático» (…), págs. 360 y ss.

der a nuestros datos o a dicho programa en la medida en que contásemos con el consentimiento de aquel que nos suministró el sistema en el que los almacenamos; mientras que, curiosamente, este sujeto, el proveedor del sistema, podría acceder a dichos datos y al programa siempre que quisiese, sin que importe que para conseguirlo hubiese tenido que vulnerar las medidas de seguridad que hubiésemos establecido precisamente para impedírselo.

Esto, evidentemente, carece de cualquier sentido.

Mucho más lógico es entender que al protegerse la inviolabilidad de los datos o de los programas contenidos en los sistemas informáticos y no la de éstos en sí mismos considerados, sólo quien tiene la capacidad de autorizar que se acceda a los primeros, esto es, a los datos o programas, podrá emitir aquella autorización o consentimiento que convertirá en permitido al acceso realizado y lo excluirá del ámbito típico del delito que venimos analizando.

El problema entonces será delimitar quién puede permitir el acceso a cada dato o programa contenido en un ordenador, cuestión en muchos casos compleja y que remite a la múltiple y muy diversa regulación extrapenal que puede tener incidencia sobre este tema (p. ej., normativa laboral, de propiedad intelectual, relativa a las telecomunicaciones, etc.). Es por ello por lo que considero un acierto del tipo delictivo propuesto que el mismo aluda al carácter no autorizado del acceso realizado y no a la concurrencia o a la ausencia del consentimiento de un único y concreto sujeto, ya que dicha referencia permitirá atender a las concretas circunstancias fácticas y legales que se presenten en cada caso concreto a la hora de determinar quién puede autorizar el acceso a cada uno de esos contenidos[27].

Por otra parte, también considero un acierto que el tipo delictivo comentado delimite los accesos típicos de este nuevo delito exigiendo que los mismos tengan que realizarse vulnerando cualquier medida de seguridad establecida para impedirlos[28], posibilidad que aparece expresamente contemplada en los dos textos internacionales anteriormente citados y que, a mi juicio, presenta importantes ventajas.

En concreto, esta exigencia no sólo permitirá incrementar el desvalor de acción propio del injusto de este delito[29], con lo que limitará su ámbito de aplicación y legitimará cuando menos en cierta medida su represión penal, sino que además y al mismo tiempo hará factible que se puedan resolver, con una cierta seguridad jurídica, algunos de los casos prácticos más problemáticos de los que se pueden plantear en relación a este nuevo delito, los referidos a los accesos no autorizados realizados no sobre todo el sistema informático, sino tan sólo sobre una parte del mismo.

Existen muchos casos en los que los sistemas informáticos son utilizados por varias personas, sin que ello quiera decir que todas ellas están legitimadas o autorizadas a acceder a todos los datos y programas allí contenidos. El problema entonces será determinar qué sujetos de los que están generalmente autorizados a utilizar un sistema pueden acceder a todos los datos o programas en él contenidos y quiénes, por el contrario, sólo pueden hacerlo a una parte de ellos y tienen vetado el acceso al resto, cuestión que resultará decisiva a la hora de determinar si ha cometido un acceso no autorizado o no.

Como fácilmente se puede imaginar estos casos pueden plantear múltiples problemas probatorios lo que dará lugar a una enorme inseguridad jurídica, problemas que, sin embargo, quedarán notablemente reducidos, cuando no totalmente resueltos a efectos penales, desde el mismo momento en que la protección penal frente a accesos no deseados se condicione al establecimiento y a la vulneración de alguna medida de seguridad dirigida a evitarlos, ya que, mientras la existencia de dicha medida permitirá delimitar de forma segura qué datos no eran accesibles pa-

27. GALÁN MUÑOZ, A., «Ataques contra sistemas informáticos» (...), pág. 229.

28. En tal sentido entiendo que la medida de protección que se ha de vulnerar puede ser de cualquier clase y naturaleza (*password*, *firewall*, biométricos, etc.), pero tiene que ser un sistema o una medida dirigido a impedir el acceso y no a evitar otros posibles abusos o daños en el sistema (p. ej., antivirus, bloqueadores de script, etc.). GALÁN MUÑOZ, A., «Ataques contra sistemas informáticos» (...), pág. 230. En el mismo sentido, MATELLANES RODRÍGUEZ, N. alude como medida de protección a dispositivos lógicos, palabras claves, contraseñas, etc., en «Vías para la tipificación del acceso ilegal a los sistemas informáticos (II)» (…), pág. 65; mientras que CARRASCO ANDRINO, M.M., señala, acertadamente a mi modo de ver, que tampoco basta con que las medidas traten de impedir el acceso al lugar en el que se encuentra el sistema, sino a los datos contenidos en el mismo y que el mero acceso a, por ejemplo, la clave del *router* que protege y conecta al ordenador a una red no da lugar a la consumación de este delito, por cuanto dicha conducta ocasiona la necesaria vulneración de la medida de seguridad que se exige en el tipo delictivo comentado y no puede ser valorada nuevamente para apreciar el acceso a los datos que se exigen para su efectiva consumación. «El acceso a un sistema informático» (…), págs. 358 y 360.

29. A mi modo de ver no se puede entender, como hace CARRASCO ANDRINO, M.M., que cuando no se establecen medidas de seguridad se está autorizando tácitamente a que cualquiera pueda acceder a los datos o programas contenidos en un sistema [«El acceso a un sistema informático…» (…), pág. 361. La ausencia de dichas medidas hace que el acceso a los datos o programas se pueda cometer de un modo menos agresivo y lesivo, con lo que si se realiza quedará al margen de la tipicidad de este delito, pero en modo alguno autoriza ni legitima de modo general a terceros a acceder a dichos datos. De hecho, los accesos realizados sobre datos informáticos no especialmente protegidos pero que reciben la protección de otros delitos (p. ej., revelación de secretos del art. 270 CP o de secreto industrial del art. 198 CP) puede dar lugar a la apreciación de dichos delitos, precisamente como consecuencia de que se efectúa sin el consentimiento de quien puede autorizar que se acceda a los mismos, pero no lo ha hecho.

ra todos los usuarios del sistema, la exigencia típica de su vulneración por parte del sujeto activo de este delito servirá para demostrar que el mismo conocía perfectamente el carácter no autorizado de su conducta, con lo que facilitará la prueba de su dolo típico[30].

En cualquier caso, y aun con la restricción comentada, parece imposible negar que este nuevo delito representa una importante expansión extensiva del Derecho penal, ya que, permitirá castigar muchas actividades que antes de su creación eran completamente atípicas.

Pese a ello, la decisión de proceder a esta notable expansión de la intervención penal se pretende tomar sin el debido debate social, político ni doctrinal.

La decisión, se nos dice, procede de instancias internacionales, con lo que parece que el Gobierno actúa como mero ejecutor de una decisión que le es casi ajena o extraña y el parlamento como un simple órgano legitimador de una incriminación que está obligado a ratificar aun en contra de su voluntad.

Parece que, por fin, los gobiernos han conseguido encontrar el camino para que sus más cuestionables decisiones incriminadoras pasen a ser aprobadas sin ninguna discusión o controversia social ni política.

Basta con realizar una convención internacional o promover la creación de una norma europea referida a dichas materias, para que la limitación de libertad que supone la creación de todo delito pase a considerarse como algo necesario y casi irremediable que nos viene dado de una instancia superior y casi incuestionable.

Entonces no puede sorprender que los legisladores nacionales también hayan utilizado este cómodo y nuevo camino para justificar el modo en que se ha regulado la realización de algo tan problemático y sensible como es la investigación de los delitos cometidos en esa red de redes que es Internet.

Veamos algunas de las normas internacionales que mayor incidencia han tenido en esta materia y el modo en que las mismas han influido en nuestra propia legislación.

3. Derecho internacional y la persecución de delitos en Internet: el siempre difícil papel de los proveedores de Servicios en la investigación y persecución de los delitos informáticos

La aparición de las nuevas conductas lesivas realizadas por medios informáticos y el hecho de que muchas de ellas se efectúen mediante el uso de esa red de redes mundial que llamamos Internet, han determinado que no sólo el Derecho penal sustantivo tenga problemas a la hora de dar adecuada respuesta a las peculiaridades que presenta el denominado «universo virtual». Tampoco parece que el Derecho procesal cuente con unos instrumentos normativos suficientemente adaptados a una realidad tan compleja y polimórfica como la que nos viene dada por las modernas autopistas de la información.

Estamos ante una red que permite múltiples y muy diversas formas de comunicación y de actuación (e-mail, web, chats, conexiones P2P, etc.), dotada de una estructura que favorece el anonimato de los cibernautas y que, además, no conoce limitaciones espaciales ni de fronteras, hechos que han llevado a LÓPEZ ORTEGA a afirmar que resulta imprescindible articular nuevos instrumentos procesales y de investigación «… que contemplen las condiciones en que se desarrolla la cibercriminalidad: volatilidad, carácter transfronterizo, rápida asimilación del progreso técnico y estructura descentralizada de la red»[31].

Dado el carácter marcadamente transfronterizo de esta nueva realidad social y de la delincuencia que se desarrolla en su seno, parece que esos nuevos y necesarios

30. Sobre esta cuestión véase con mayor extensión GALÁN MUÑOZ, A., «Ataques contra sistemas informáticos» (...), págs. 229 y ss. No podemos compartir, por tanto, la postura defendida por CARRASCO ANDRINO, cuando afirma que es necesario cambiar este tipo delictivo para que el mismo castigue tan sólo la vulneración de medidas de protección del sistema informático en sí y no la de los que tratan de evitar el acceso a datos o programas contenidos en el mismo, para evitar posibles solapamientos de este nuevo delito con alguno de los que protegen la propiedad intelectual. En «El acceso a un sistema informático» (…), págs. 358 y 362. A mi modo de ver, esta propuesta dejaría injustificadamente sin protección a muchos sujetos que tienen que compartir el uso sus sistemas con terceros o que desarrollan sus tareas utilizando terminales conectados a redes a los que otros sujetos también tendrían legítimo acceso (no se debe olvidar que, por sistema informático se entiende, tal y como reconoce al propia autora, tanto al ordenador individual como a un conjunto de ordenadores conectados entre sí). Pero es que, además y por otra parte, también parece olvidar que este nuevo delito castiga acceder a los programas contenidos en un sistema informático vulnerando las medidas de seguridad establecidas para evitar dicho acceso, mientras que lo que se castiga en los delitos contra la propiedad intelectual es copiar, reproducir, plagiar, distribuir o comunicar públicamente dichos programas o crear, poner en circulación o tener medios que sirvan para desprotegerlos, esto es, para privarles del sistema que trata de impedir, por ejemplo, que se puedan copiar. Resulta erróneo, por tanto, conceptuar [como hace, LÓPEZ ORTEGA, J. J., «Intimidad informática y Derecho penal…» (…), pág. 122], al delito de Hacking como el delito que castiga la fase ejecutiva del delito del art. 270.3 CP (el de fabricación puesta en circulación e incluso tenencia de medios destinados a desproteger programas de ordenador). Ambos delitos castigan conductas netamente diferenciadas y protegen bienes jurídicos claramente diversos, con lo que sólo podrán concurrir en concurso de delitos y nunca en concurso de leyes, como parece sostener este autor; evitándose de este modo cualquier posible solapamiento típico entre los dos.

31. LÓPEZ ORTEGA, J.J., «Intimidad informática y Derecho penal…» (…), pág. 132.

instrumentos jurídicos deberían crearse mediante la aprobación de normas penales y procesales de origen internacional[32]; normas que, evidentemente, no se han hecho esperar.

Existen numerosos instrumentos internacionales que tratan de garantizar y de facilitar la cooperación judicial y policial entre países en la persecución de los más diversos delitos con incidencia transnacional, como sucede, por ejemplo, el Convenio de asistencia judicial en materia penal entre los Estados de la Unión europea, de 29 de mayo de 2000 o el ya citado Convenio del Consejo de Europa sobre el cibercrimen, de 23 de noviembre de 2001[33]. Pero también se han ido creando una serie de normas y convenios internacionales, sobre todo a nivel europeo, que tratan de asegurarse de que las normativas nacionales relativas a la investigación penal de los denominados delitos informáticos sean lo suficientemente homogéneas como para conseguir que los anteriormente citados instrumentos de cooperación internacional resulten realmente efectivos a la hora de perseguir a las distintas manifestaciones de esa clase de criminalidad.

Estos últimos instrumentos parten de la base de que cualquier pretensión de realizar una investigación penal de delitos cometidos en Internet resultaría inútil si no se contase con la colaboración de los intermediarios de dicha red (los proveedores de servicios).

Resulta imposible saber desde qué terminal informático se realiza una determinada conducta sin conocer la dirección IP (*Internet Protocol*) que permite que dicho terminal se identifique y se conecte con el resto de los que conforman Internet. Sin embargo, cada vez es más frecuente que los usuarios ocasionales de Internet se conecten y naveguen por la red utilizando direcciones IP dinámicas que le son otorgadas de forma automática por su proveedor de servicios mediante el protocolo internacional DHPC (*Dynamic Host Configuration Protocol*), con lo que la dirección de cada terminal cambia en cada sesión o conexión a Internet[34].

Este constante cambio de direcciones va a llevar a que el objeto de las interceptaciones lícitas de las telecomunicaciones realizadas en Internet no se pueda determinar atendiendo al mero dato del IP que en un momento dado correspondiese al terminal que se quiere interceptar, ya que, al cambiar dicha terminal de dirección con cada conexión no se podrá conocer la dirección que le corresponde, después de que se haya desconectado, hasta el mismo momento en que se vuelva a conectar. Pero es que, además, y por otra parte, este constante cambio de direcciones también provocará que sólo se pueda determinar el terminal desde el que se cometió un concreto delito si se tiene la posibilidad real de averiguar a qué terminal de la red le correspondía la concreta dirección IP desde la cual se había realizado la conducta delictiva en el concreto momento en que se había hecho[35].

Estos hechos van a llevar a que, en muchos casos, la interceptación de comunicaciones realizadas en Internet y la determinación del terminal de procedencia de las posibles conductas delictivas realizadas en su seno, sólo se puedan efectuar si se cuenta con la colaboración de aquellos sujetos o entidades que tienen la capacidad técnica necesaria para poder interceptar todas las comunicaciones realizadas desde un concreto terminal y para registrar y almacenar todos aquellos datos que permitirán identificar al terminal desde el que dichas conductas se realizaron, los proveedores de servicios de Internet.

Es por ello por lo que las distintas normas internacionales específicamente referidas a las técnicas de investigación penal en Internet como el ya citado Convenio del consejo de Europa sobre Cibercriminalidad o las Directivas 2000/31/CE, 2002/58/CE y 2006/24/CE del Parlamento europeo y el Consejo, exigen a los países que están vinculados por sus disposiciones que obliguen a dichos sujetos (a los proveedores), a colaborar con las autoridades en la realización de todas aquellas interceptaciones de las comunicaciones de sus clientes que le sean judicialmente requeridas y que les exijan que almacenen algunos datos referidos a las comunicaciones de dichos sujetos durante un determinado período de tiempo, con objeto de que los mismos pudiesen ser utilizados por dichas autoridades en caso de que los necesitasen en el desarrollo de una investigación criminal.

Como fácilmente se puede comprobar, ninguna de estas normas obliga al proveedor a vigilar o a controlar los contenidos que ayuda a difundir; exigencia que, a mi juicio, vendría a establecer un sistema de censura previa completamente incompatible con el derecho a la libertad de expresión que debe respetar todo verdadero Estado democrático de Derecho.

Lo que hacen es obligarle a cooperar técnicamente en las interceptaciones que le sean judicialmente requeridas y exigirle que recolecte y almacene una serie de datos referidos a las comunicaciones ajenas que ayude a realizar,

32. De hecho no le falta razón a MUÑOZ MACHADO, S., cuando señala que la regulación referida a esta materia trasciende lo nacional o lo europeo y exige una regulación a escala mundial. *La regulación de la red: Poder y Derecho en la red,* Ed. Taurus, Madrid, 2000, pág. 181.

33. FERNÁNDEZ RODRÍGUEZ, J.J., *Secreto e intervención de las comunicaciones en Internet*, Ed. Thomson Civitas, Madrid, 2004, pág. 122.

34. Sobre la evolución producida en Internet que ha llevado de la utilización mayoritaria de IP estáticas al uso actual generalizado de IP dinámicas, y sobre sus peculiaridades, véase RODRÍGUEZ LAINZ, J.L., «Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas», *La Ley,* n.º 7086 (versión digital disponible en www.laley.es; últ. vis. 10-2-2009).

35. Para entender la concreta repercusión práctica que esta técnica de conexión tuvo en la investigación penal de delitos en Alemania resulta interesante leer MICHELS, H. *Straftaten und Strafverfolgerung im Internet,* BWV, Berlín, 2003, págs. 20 y ss.

ordenándole que los custodie durante un determinado período de tiempo y los entregue tan sólo a las autoridades encargadas de una investigación criminal cuando ello le sea judicialmente requerido.

El objetivo de esta última medida es evidente. Se trata de establecer un sistema que permita identificar al usuario, o cuando menos el terminal, desde el que hubiese realizado alguna conducta delictiva en la red, sin tener que sacrificar el derecho al anonimato, del que, en principio, disfrutan todos sus usuarios; objetivo que sólo se podrá alcanzar si los proveedores de servicios mantienen almacenados los datos que permitirían localizar a quien realizó dichas conductas, o cuando menos el terminal desde el que lo hizo, de una forma completamente confidencial, debiendo entregarlos y revelarlos tan sólo cuando así les fuesen exigido por una autoridad judicial[36].

En definitiva, se pretende implantar un sistema de «trazabilidad legal»[37] que permita mantener el anonimato general de las acciones realizadas por los usuarios de la red, sin que ello tenga que suponer que aquellas que pudiesen llegar a alcanzar relevancia penal (p. ej., estafas informáticas, daños, difusión de pornografía infantil, etc.) deban quedar necesariamente impunes[38].

Esta parece ser la práctica y el sistema más conforme a las exigencias de un Estado democrático y no los establecidos por aquellos regímenes —como el de Arabia Saudita o el de China— que convierten a los proveedores de servicios en verdaderos vigilantes, censores y delatores de la red, con lo que transforman Internet en un lugar completamente vigilado y controlado en el que los derechos a la intimidad y al secreto de las comunicaciones de sus usuarios ni se garantizan ni se respetan.

Ahora bien, el problema que se plantea a continuación es determinar en qué medida influirá el establecimiento de este sistema de trazabilidad sobre la investigación y persecución penal de los delitos cometidos en la red, cuestión que parece encontrarse lejos aún de encontrar una solución unánimemente aceptada.

En España, los importantes cambios legislativos realizados por las leyes 34/2002, de 11 de julio, de servicios de la sociedad de la Información (LSSI), 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT) y la todavía reciente ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones (LCDC), han regulado de forma bastante exhaustiva el comportamiento que los proveedores han de seguir y las medidas que han de adoptar para garantizar la eficacia de la investigación penal.

Se establece el deber de colaboración del proveedor en las intervenciones de comunicaciones que le sean judicialmente requeridas (art. 33 LGT). Se les obliga a almacenar determinados datos referidos a las comunicaciones realizadas por los usuarios de sus servicios. Se definen los datos que han de almacenar, el período por el que han de hacerlo, cómo y cuándo pueden y deben cederlos y también cómo deben protegerlos frente a posibles accesos no autorizados (arts. 3, 5, 7 y 8 LCDC respectivamente).

Sin embargo, y sorprendentemente, la implantación de este sistema facilitador de la investigación penal de los delitos cometidos en Internet no se ha visto complementada ni respaldada con ninguna reforma de las normas que rigen cuándo, cómo y en qué medida se puede solicitar a dichos prestadores de servicios que efectúen las interceptaciones de las que habla la LGT o que comuniquen los datos que delimita la LCDC.

Ni los enormes avances tecnológicos, ni la gran variedad de novedosas técnicas de comunicación existentes en Internet, ni el desarrollo de una importante y compleja normativa destinada a establecer un sistema facilitador de la investigación de los delitos cometidos en el seno de esta red, han provocado cambio alguno en la Ley de Enjuiciamiento Criminal española, hecho que ha llevado a que los juristas españoles se muevan en una enorme incertidumbre a la hora de determinar cuándo y con qué requisitos se pueden interceptar algunas de las comunicaciones que se realizan en Internet.

Así, por ejemplo, nos encontrábamos con el despropósito de que los Tribunales españoles ni siquiera saben con certeza qué procedimiento habrán de seguir para interceptar algo, tan cotidiano a día de hoy, como un correo electrónico (e-mail), ya que, mientras algunos autores consideran que para hacerlo se debe seguir el procedimiento establecido para la detención de correspondencia privada, postal o telegráfica contemplado en el art. 579.1 LECr; otros se decantan por entender que ello sólo se podrá hacer utilizando el cauce procesal previsto en el segundo apartado de dicho artículo, referido a la interceptación de las comunicaciones telefónicas[39].

36. En este sentido, he de señalar que comparto plenamente la postura defendida en su día por MORALES PRATS, F., cuando consideraba que la revelación no autorizada de los datos custodiados por los proveedores de servicios de Internet podría y debería ser considerada como una conducta perfectamente subsumible en el delito de revelación de secreto profesional, lo que permitiría castigar al sujeto responsable de la misma, como verdadero autor del delito contemplado en el art. 199.2 del Código penal Español. «La investigación del ciberdelito (II)», *Iuris,* n.º 102, 2006, pág. 35.

37. Así lo denomina, acertadamente a mi juicio, LÓPEZ ORTEGA, J.J., «La admisibilidad de los medios de investigación...» (...), pág. 98, y el mismo autor en «Libertad de expresión y responsabilidad por los contenidos en Internet» en *Internet y Derecho Penal,* Cuadernos de Derecho Judicial X, Ed. CGPJ, Madrid, 2001, pág. 211.

38. De este modo, y como bien señala MICHELS, H., se llega a que el anonimato de las comunicaciones realizadas en Internet sólo sea relativo, *Straftaten und Strafverfolgerung im Internet*. (…).

39. Sobre este tema véase, con mayor extensión, FERNÁNDEZ RODRÍGUEZ, J.J., «Secreto e intervención de las comunicaciones en Internet». (…), págs. 147 y ss.; MACHENA GÓMEZ, M., «dimensión jurídico penal del correo electrónico», *La Ley,*

Tampoco han faltado opiniones que niegan o cuando menos cuestionan que sea necesario contar con autorización judicial alguna para controlar y acceder a los e-mails de un determinado sujeto, ya que, entienden que al ser Internet un canal abierto de comunicación todos los contenidos que se difundan o distribuyan en dicha red son contenidos públicos que resultan libremente accesibles para todos sus usuarios[40].

Pese al incomprensible e inadmisible silencio legal respecto a esta cuestión, parece haberse alcanzado un cierto consenso doctrinal y jurisprudencial a la hora de entender que el derecho al secreto de las comunicaciones, reconocido por el art. 18.3 de la Constitución española, comprende no sólo las comunicaciones postales, telegráficas o telefónicas tradicionales, sino también aquellas otras que se realizan por cualquiera de los modernos medios informáticos[41], lo que ha llevado a que se proyecte el estatuto jurídico de dicho derecho fundamental a las comunicaciones realizadas, por ejemplo, por correo electrónico[42].

Sin embargo, esta solución no ha resuelto todos los problemas que plantea el uso de las nuevas tecnologías de la información.

¿Qué datos son los que se protegen por el derecho al secreto de las comunicaciones? ¿Todos los que se publican y difunden en Internet? ¿Sólo algunos? ¿Cuándo comienza y cuándo termina el acto de comunicación protegida? ¿Cabe que algunas de estas comunicaciones sean interceptadas o controladas, incluso por particulares para ejercer derechos tales como, por ejemplo, el que ordenamiento laboral español reconoce al empleador y que le permite establecer sistemas de control del cumplimiento de las obligaciones laborales por parte de sus trabajadores?[43].

Las cuestiones parecen no tener fin y, sin embargo, no encuentran respuesta segura alguna ni en el ámbito legislativo nacional ni en el internacional.

Como ya señalé al comienzo de este trabajo, la internacionalización del Derecho penal no tiene porque ser un fenómeno que siempre dé lugar a una armonización extensiva del Derecho y de la persecución penal nacional. También puede y debería generar ciertas armonizaciones restrictivas de los ordenamientos jurídicos nacionales al obligarles a contemplar y a respetar unos estándares de garantías mínimas comunes e indisponibles.

Esto último es lo que, de hecho, tratan de hacer muchas de las Convenciones Internacionales de Derechos Humanos; instrumentos normativos en los que se contemplan entre otros derechos básicos de la persona y del ciudadano, algunos con notable incidencia procesal como los referidos a la intimidad o al derecho que todo ciudadano tiene al secreto de sus comunicaciones.

Pese a todo, las mencionadas convenciones internacionales, como también sucede con las propias constituciones nacionales, se limitan a hacer unas referencias muy genéricas a dichos derechos, lo que las convierte en referentes importantes, pero no completamente precisos y eficaces, a la hora de responder a todas las preguntas que plantea el imparable avance y expansión del uso de Internet.

Mucho más útil resulta, sin embargo, el desarrollo y la interpretación que los Tribunales internacionales han realizado de dichas disposiciones convencionales a la hora de controlar si los Estados que han ratificado dichas convenciones respetaban lo establecido en las mismas.

Entre estas interpretaciones jurisprudenciales me gustaría destacar, por su importancia en la materia que venimos analizando, la que ha desarrollado el Tribunal Europeo de Derechos Humanos en su labor de control de las actividades de los Estados firmantes del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, que podrían violar el art. 8 de la Convención, precepto en el que se establece que:

> «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injeren-

n.º 6475, versión digital consultada en www.laley.es (últ. vis. 12-1-2009) o GARCÍA GONZÁLEZ, J., «Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial». En *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Ed. Comares, Granada, 2006, págs. 314 y ss.

40. Así lo consideraban algunos como señala LÓPEZ ORTEGA, J.J., «La admisibilidad de los medios de investigación...» (...), pág. 95.

41. MORENO CATENA, V., «La intervención de las comunicaciones personales en el proceso penal». En *La reforma de la justicia penal (Estudios homenaje al Prof. Klaus Tiedemann),* Ed. Publicactions Universitat Jaume I, 1997, pág. 410. En el mismo sentido, FERNÁNDEZ RODRÍGUEZ, J.J., «Secreto e intervención de las comunicaciones en Internet» (…), pág. 149.

42. MORALES PRATS, F., «La investigación del ciberdelito (II)», *Iuris,* n.º 102, 2006, pág. 35.

43. Sobre este tema y la, a mi juicio, tan sólo aparente habilitación que otorga el art. 20 ET a tales efectos, véase GARCÍA GONZÁLEZ, J., «Intervenciones de terceros en el correo electrónico...» (...), pág. 303, y GOÑI SEIN, J.L., quien afirma que «... a través de los mecanismos informáticos el empresario puede controlar el tiempo de trabajo efectivo de los trabajadores, los desplazamientos del trabajador dentro del lugar de trabajo, el número de llamadas telefónicas y la duración de las mismas. Nuevamente las facultades de control del empresario encuentran su límite en el debido respeto a la dignidad humana. Por tanto, la utilización de esta medida de control será lícita siempre que se limite al control de la prestación laboral y, excepcionalmente, cuando sea imprescindible por motivos productivos, es decir, cuando la realización de la prestación laboral implique la utilización de mecanismos informáticos que inevitablemente registran una serie de datos sobre la actividad del trabajador que van más allá del control sobre el cumplimiento de sus tareas». «Derecho a la dignidad e intimidad del trabajador» en www.iustel.com (últ. vis. 10-8-2008).

cia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Como se puede comprobar, la delimitación normativa de este derecho fundamental no puede ser más general, y sin embargo, el desarrollo y la aplicación práctica que del mismo ha realizado el citado Tribunal resulta esencial para entender el papel que el Derecho europeo y, por derivación, también el español otorga a los proveedores de servicios en las investigaciones de delitos informáticos realizados en la red.

Resulta imposible realizar, en este momento, siquiera un somero análisis de todas las resoluciones que este Tribunal ha dedicado a la materia que nos ocupa, pero sí me gustaría destacar de entre todas ellas, aquella que a mi juicio se encuentra en el origen de toda la normativa europea referida a las comunicaciones realizadas en Internet, la Sentencia de 2 de agosto de 1984, referida al *Caso Malone vs. Reino Unido*.

En esta sentencia se planteó por parte de la Comisión Europea de Derechos Humanos, si el seguimiento y la interceptación que habían realizado las autoridades policiales británicas sobre las comunicaciones telefónicas del señor *Malone*, al que consideraban sospechoso de realizar actividades de receptación de bienes robados, eran acordes con el texto y las exigencias derivadas del citado art. 8 de la Convención.

Los representantes del Reino Unido afirmaron que la inexistencia de una normativa específicamente referida a la interceptación de este tipo de comunicaciones en su ordenamiento jurídico permitía entender que el mismo no reconocía el derecho a su privacidad, con lo que resultaba perfectamente lícito y permitido que su policía efectuase interceptaciones de comunicaciones sin control o autorización judicial alguna. Además, y por otra parte, dichos representantes también pusieron en tela de juicio que la mera conducta del denominado *metering*, esto, es el mero control del registro de las llamadas efectuadas por o al señor Malone, pudiese ser considerada como una actividad que realmente afectase a dicho derecho fundamental.

La respuesta del Tribunal a la primera de las cuestiones planteadas por los representantes del Reino Unido fue contundente.

El secreto de las conversaciones realizadas mediante los sistemas telefónicos resulta perfectamente incardinable en los conceptos de «vida privada» y de «correspondencia» que protege y reconoce el art. 8 de la convención, lo que determina que dicho secreto tenga que ser garantizado por todos los Estados firmantes y que sólo pueda ser limitado conforme a las exigencias establecidas por el apartado 2 de dicho artículo, esto es, conforme a la ley y las necesidades de una sociedad democrática.

En este sentido, afirma el citado Tribunal que cuando este precepto alude a la concordancia con la ley como referente básico de las posibles limitaciones de este derecho fundamental, no se está refiriendo a la concreta ley doméstica nacional que regule dicha materia. Cuando la Convención exige que la interceptación de las comunicaciones se realice de acuerdo con la ley está haciendo referencia a las exigencias propias del Estado de Derecho que aparecen expresamente contempladas en el preámbulo de la Convención, circunstancia que va a permitir que este Tribunal pueda entrar a valorar y a enjuiciar si dichas exigencias son respetadas o no por cada una de las concretas normativas nacionales de los Estados firmantes de la Convención.

Es partiendo de esta base, desde la que el alto Tribunal afirma que la interceptación de las telecomunicaciones tiene que ser necesariamente regulada por una ley que pueda ser conocida por todos los sujetos a los que puedan sufrir dicha medida. Esto es, una ley susceptible de ser conocida por todos los ciudadanos, ya que todos ellos pueden sufrir dichas interceptaciones.

Ello supone que esta materia no sólo no puede regularse por una norma o ley secreta, sino que además debe contemplarse en una ley que sea lo suficientemente clara y precisa como para dar una adecuada indicación a sus destinatarios (todos los ciudadanos) de las circunstancias y de las condiciones bajo las cuales las autoridades podrán interceptar sus comunicaciones. Como afirma el propio Tribunal, «una ley que concede discreción debe indicar el ámbito de esa discreción», lo que no quiere decir que todos los ciudadanos deban poder prever siempre y con todo detalle cuándo las autoridades están interceptando sus comunicaciones, ya que, ello convertiría en inútil cualquier investigación policial realizada por este medio.

Sin embargo, para cumplir con las exigencias derivadas de la mencionada convención, a juicio del Tribunal, no basta con que esta cuestión se regule en una ley clara y precisa. El ejercicio de la capacidad de interceptación, unida al secreto que le es inherente, genera unas posibilidades de abuso por parte de las autoridades públicas tan enormes que su uso debe verse limitado y controlado por una serie de garantías jurídicas que aseguren que su utilización va a resultar acorde con las exigencias de toda sociedad democrática; lo que obligará (como expresamente afirmaba el juez Pittiti en su opinión particular concordante con la Sentencia), a que tanto la adopción, como la proporcionalidad de dichas interceptaciones, deban estar siempre judicialmente controladas[44].

44. Véase en este sentido, y sobre las importantes limitaciones que el citado Tribunal ha extraído de la referencia a las exigencias derivadas del Estado de Derecho y entre las cuales destaca la proporcionalidad, lo comentado por MEYER-LADEWIG, J. *Europäische Menschenrechts-Kovention. Handkommentar.* V. Nomos, Baden-Baden, 2006, págs. 180 y ss.

Ahora bien, si esta sentencia es conocida y se ha llegado a convertir en un referente básico a la hora de analizar la regulación que nos ocupa ha sido por la solución que dio al segundo de los problemas que le plantearon los representantes del Reino Unido, esto es, a aquel que cuestionaba si el mero *metering* era una actividad que realmente afectase al secreto de las comunicaciones y que tuviese que cumplir, por tanto, con los mismos requisitos y exigencias que cualquier otra conducta limitadora de dicho derecho fundamental; cuestión a la que el Tribunal respondió de forma nuevamente afirmativa, al señalar que «... los registros de *metering* contienen información, en particular los números llamados, que es un elemento integral de las comunicaciones realizadas por teléfono. Consecuentemente, revelar dicha información a la policía sin el consentimiento del suscriptor equivale, en opinión del Tribunal, a una interferencia en el derecho garantizado en el art. 8».

Los efectos de esta declaración judicial no se hicieron esperar y así la jurisprudencia constitucional española, pese a la inicial reticencia del Tribunal Supremo[45], entendió en repetidas ocasiones que el acceso no consentido a la lista de llamadas de una persona por parte de los Cuerpos y Fuerzas de Seguridad del Estado requiere de la misma autorización judicial motivada que exige el art. 18.3 de la Constitución Española para interceptar sus comunicaciones[46]; postura jurisprudencial que, unida a la extensión de este derecho al campo de las nuevas tecnologías de la comunicación, como Internet, parecía obligar a que dicha garantía también se predicase con respecto a aquellos datos que identifican a quienes realizan sus comunicaciones en el mundo virtual, esto es, a los datos que definen a los emisores y receptores de información en Internet (identificación del usuario del terminal, IP asignado al mismo, fecha y hora de conexión, duración de la misma, etc.).

Así lo entendió parte de la doctrina española[47], encontrando un respaldo notable, a mi modo de ver, tanto en algunas de las más recientes resoluciones del Tribunal Europeo de Derechos Humanos[48], como en los propios textos de las reformas legislativas españolas; textos que si bien obligan a los proveedores a conservar determinados datos referidos a las comunicaciones de sus clientes por un período general de 12 meses (período que se pueda ampliar o reducir reglamentariamente en determinados casos como establece el art. 5. LCDC); condicionan su cesión, por parte de los proveedores que tienen que almacenarlos a los agentes que están facultados para recibirlos, a la emisión de una resolución judicial que, atendiendo a los principios de necesidad y proporcionalidad, ordene su entrega y concrete y determine cuándo y en qué medida se les han de ceder (arts. 6 y 7 LCDC).

Parecía entonces que, al fin, una de las cuestiones planteadas respecto a las garantías jurídicas del anonimato de las comunicaciones realizadas en Internet había encontrado una respuesta legal segura.

Pero la apariencia fue sólo eso, una mera apariencia. Una apariencia que, de hecho, sólo duró hasta que el Tribunal Supremo español se enfrentó al primer caso en el que dicha cuestión se le planteó.

En concreto, lo hizo en su todavía reciente Sentencia 236/2008, de 9 de mayo, donde se juzgó un caso en el que los miembros de la Unidad de Delitos Telemáticos de la Guardia Civil habían rastreado y recopilado, sin autorización judicial alguna, los IPs de todos los usuarios que habían compartido un archivo con contenidos de pornografía infantil a través de un conocido programa de intercambio de archivos P2P (Emule); recopilación que les aportó una serie de datos que pretendieron utilizar como prueba incriminatoria en el correspondiente proceso penal abierto contra una de las personas que habían descargado dicho contenido, por lo menos parcialmente.

Esta pretensión fue inicialmente desestimada por la Audiencia Provincial de Sevilla al entender que la prueba obtenida por dicho sistema había violado el derecho fundamental al secreto de las comunicaciones de la persona imputada, lo que la invalidaba conforme a lo establecido por el art. 11.1 de la Ley Orgánica del Poder Judicial español. Sin embargo, esta inicial postura jurisprudencial no fue compartida por el Tribunal Supremo en su ya citada sentencia donde se afirma —eso sí, «sin pretensiones de

45. Véase a este respecto lo comentado por MATA Y MARTÍN, R.M., con relación a la STS de 22 de marzo de 1999 en la que se consideraba que la obtención de los listados de llamadas telefónicas de un sujeto sin su consentimiento y sin orden judicial no vulneraba el derecho fundamental al derecho de las telecomunicaciones, con lo que no requerían de la emisión de auto judicial motivado para ser realizada; sentencia que lleva al citado autor a considerar que sólo los datos relativos al contenido de lo transmitido están amparados por la protección que otorga dicho derecho. *Delincuencia informática y Derecho penal* (...), pág. 164.

46. Véase, por ejemplo, la STC 230/2007, de 5 de noviembre, donde aparecen expresamente citadas muchas otras. Para tener una visión general sobre la polémica jurisprudencial comentada, véase RODRÍGUEZ LAINZ, J.L., «Dirección IP; IMSI e intervención judicial de comunicaciones electrónicas» en *La Ley* n.º 7086, 2009. www.laley.es (últ. vis. 8-1-2009).

47. Así ROMEO CASABONA, C., quien señala que la protección de las comunicaciones abarca tanto el proceso, el soporte, como la comunicación como su contenido mismo. «Los datos de carácter personal como bienes jurídicos penalmente protegidos» (...), pág. 188, de respeto a la confidencialidad de las comunicaciones y de derecho al anonimato del usuario, habla MORALES PRATS, F., «Los ilícitos en la red (II): pornografía infantil y ciberterrorismo» (…), pág. 272.

48. Véase en este sentido la Sentencia emitida por este Tribunal en el caso *Copland v. Reino Unido*, de 3 de abril de 2007 en la que se afirma de forma expresa que la mera monitorización (*metering*) no consentida de los e-mails enviados por un trabajador por parte de su empleador resulta una interferencia en el derecho que dicha ciudadana tenía a que se le respetase a su vida privada y su correspondencia.

sentar doctrina (obiter dicta)», lo que resulta cuando menos sorprendente, al ser en gran medida esta consideración la base central de su resolución—, que los datos identificativos de un titular o de un terminal no están amparados por el derecho a la inviolabilidad de las telecomunicaciones del art. 18.3 CE, sino por el más genérico derecho a la intimidad personal del apartado primero de dicho artículo[49].

De hecho, y a juicio del ponente de la comentada Sentencia, los datos referidos, por ejemplo, a las IPs de los usuarios de la red serían datos de carácter personal protegidos por Ley Orgánica 15/1999, pero no datos de los que se protegen por las previsiones referidas al secreto de las telecomunicaciones y, además, y esto resulta esencial, serían unos datos que no estarían preservados del conocimiento general, ya que se revelan y publican voluntariamente por su propio titular (el usuario de la red) desde el mismo momento en que se conecta a Internet y usa un programa P2P como Emule[50]; circunstancia esta última que determinará, a juicio del Tribunal Supremo español, que pueden ser rastreados y captados por las Fuerzas y Cuerpos de Seguridad del Estado con total libertad y sin necesidad de contar con autorización ni control alguno por parte de ninguna instancia jurisdiccional.

Se abría así de nuevo un debate en España que parecía estar ya definitivamente cerrado. ¿Se puede monitorizar y rastrear con total libertad, de forma indiscriminada y sin ninguna intervención judicial todo el tráfico de datos producido en Internet al realizarse el mismo, por lo menos en su mayor parte, desde terminales a las que se le asigna una dirección IP que puede ser fácil y públicamente conocida?

A mi juicio, no.

No, en primer lugar, porque la afirmación realizada por el Tribunal Supremo español, según la cual, al conectarse a Internet el usuario conoce y consiente la publicación de los datos referentes a su IP resulta algo más que cuestionable, ya que, en nada se corresponde con una realidad en la que el usuario medio ni tiene opción de elegir si quiere publicar dichos datos o no quiere hacerlo, ni conoce cómo funciona realmente dicha red, ni los datos y señales que va dejando al utilizarla. Hablar en estas circunstancias de un verdadero consentimiento siquiera tácito del usuario no es más que una pura ficción. Pero es que, además, aun cuando se apreciase este ficticio consentimiento, el mismo carecería de cualquier efecto práctico al entenderse, como aquí se entiende, que al estar dicho consentimiento referido a la autorización de una intromisión en un derecho fundamental (el del secreto de las telecomunicaciones), sólo tendrá efectos jurídicos si es un consentimiento expreso y no uno meramente tácito[51].

No, también y por otra parte, porque considerar, como algunos hacen[52], que estos datos son captables por cualquier sujeto sin necesidad de autorización judicial y establecer, sin embargo, que los proveedores no pueden utilizarlos salvo en los supuestos excepcionalmente permitidos en el art. 38 de la LGT, carece de cualquier sentido, ya que si son meros datos personales públicos, accesibles y recopilables por cualquier sujeto, ¿por qué el proveedor que los recopila no puede usarlos y cualquier otro sujeto que consiga hacerlo por sus propios medios sí? Es más, ¿por qué tiene que contar necesariamente con autorización judicial para poder cederlos a un agente facultado, si cualquier otro sujeto que los hubiese captado podría usarlos y cederlos sin contar con ella?

Y no, también y finalmente, porque esta afirmación supone desconocer el verdadero fundamento que llevó al Tribunal Europeo de Derechos humanos y también a nuestro Tribunal Constitucional a afirmar en reiteradas ocasiones que esta clase de datos, los denominados datos de tráfico, están amparados por el derecho fundamental al secreto de las telecomunicaciones aun cuando se hubiesen obtenido después de que el proceso comunicativo al que están referidos hubiese terminado y no mientras éste se estaba produciendo[53].

Si se analizan las Sentencias emitidas, sobre todo, por el citado Tribunal internacional desde el *caso Malone*, nos

49. Fundamento de Derecho Primero 4 de la STS 236/2008, de 9 de mayo.

50. Fundamento de Derecho Segundo de la STS 236/2008, de 9 de mayo.

51. Compartimos en este sentido lo señalado por FERNÁNDEZ RODRÍGUEZ, J.J., cuando negaba que se pudiese apreciar dicho consentimiento incluso en las actividades realizadas por un sujeto experto que conociese el funcionamiento y los riesgos de la red de una forma especial Ni siquiera cuando este sujeto realice conductas fácilmente detectables y rastreables y sepa que lo son, se puede entender que esté renunciando a su derecho al secreto de las telecomunicaciones, con lo que dicha renuncia sólo se podrá apreciar cuando se produzca de forma expresa. «Secreto e intervención de las comunicaciones en Internet» (…), págs. 110 y 111. En este mismo sentido, afirmaba LÓPEZ ORTEGA, J.J., que las tecnologías actuales permiten realizar un seguimiento invisible de la información de los usuarios, que se efectúa según este autor en muchos casos (a nuestro juicio habría que decir en la mayoría de los casos) sin contar con la voluntad de los usuarios «La admisibilidad de los medios de investigación...» (...), pág. 95. En contra de esta postura, sin embargo, y a favor de la apreciación del consentimiento del usuario, incluso del emitido de forma meramente tácita, se ha manifestado recientemente RODRÍGUEZ LAINZ, J.L., «Dirección IP; IMSI e intervención judicial…» (…), postura que no podemos compartir por los motivos comentados.

52. RODRÍGUEZ LAINZ, J.L., «Dirección IP; IMSI e intervención judicial…» (…).

53. Así, por ejemplo, véase el Fundamento Jurídico 6.º de la STC 123/2002, de 20 de mayo, o el Fundamento 2.º de la STC 230/2007, de 5 de noviembre, postura que ha sido criticada, sin embargo, por RODRÍGUEZ LAINZ, J.L., quien entiende que la interceptación o control de los denominados datos de tráfico sólo afectarán al secreto de las telecomunicaciones si se realiza mientras el proceso comunicativo se efectúa, pasando después los datos obtenidos a ser simples datos de carácter personal recogidos

encontraremos con que todas ellas consideran a la monitorización o *metering* de comunicaciones como una conducta lesiva para el secreto de las comunicaciones, precisamente, como consecuencia de que, pese a que los datos captados mediante estas conductas no aportan aparentemente ninguna información esencial sobre la intimidad de la persona (número de teléfono, dirección IP, etc.), no se puede olvidar que su unión con el uso y la utilización de los modernos sistemas de procesamientos de datos podrá permitir que las autoridades y los particulares que se dedicasen a recopilarlos, llegasen a conseguir muchas informaciones que sí afectarían de forma muy significativa a dicho derecho fundamental.

Piénsese, por ejemplo, en lo fácil que le resultaría al Estado realizar perfiles de muchos de sus ciudadanos simplemente conociendo la prensa que leen en la red, a qué concretos artículos acceden, qué foros visitan, a quiénes remiten sus e-mails, con quiénes establecen sus chats, qué entidades financieras utilizan, etc.

¡Incluso podría determinarse, en algunos casos, dónde estamos en cada momento y por dónde hemos pasado!

Es cierto que la utilización generalizada de direcciones IP´s dinámicas añade dificultades técnicas a la realización de este tipo de controles, pero ni impide que se puedan realizar con respecto a aquellos usuarios que utilicen conexiones estáticas, ni garantiza de forma completamente segura que no se puedan llegar a realizar con respecto a quienes no las usan.

Los peligros que acechan a nuestra intimidad tras este aparentemente inocuo procedimiento, como fácilmente se puede apreciar, no son pocos ni pequeños. De hecho, y como bien afirma el Juez Pettiti en su voto concordante con la Sentencia del *caso Malone*, la captación de estos datos unida a su procesamiento informatizado, si no se controlan adecuadamente, pueden permitir que el Estado establezca sistemas de control generalizados de las actividades de sus ciudadanos que recordarían, en no pocos aspectos y de forma alarmante, a los que se describían en el *Big Brother* orweliano.

Este peligro es real y no se puede olvidar. La posibilidad de abuso de este tipo de sistemas por parte de la administración, o incluso por parte de empresas privadas y particulares, es demasiado grande como para no tenerla en cuenta. Nos encontramos ante unos mecanismos de control que si no son utilizados de forma proporcionada y limitada pueden convertir Internet en un espacio en el que los derechos a la vida privada, a la intimidad y a la privacidad de todos los ciudadanos carezca de cualquier contenido real[54] y es por ello, precisamente por ello, por lo que considero que el uso de los mismos tiene que ser necesariamente controlado y autorizado por un órgano judicial independiente que compruebe, no sólo que su utilización inicial es necesaria y está justificada, sino también que se emplean de una forma adecuada y proporcionada a los fines que permitieron usarlos[55].

Esto es lo que, a mi modo de ver, trata de garantizar la LCDC en sus arts. 6 y 7. Una ley que, según entiendo, se vería completamente burlada si se considerase que los denominados datos de tráfico no son datos protegidos por derecho fundamental alguno, como algunos señalan[56], pero que tampoco conseguiría el objetivo de garantizar el anonimato relativo de las comunicaciones realizadas en Internet, si se llega a entender que los mismos son meros datos de carácter personal que se publican voluntariamente por el usuario de la red cuando se conecta a la misma, con lo que pueden ser libremente recopilados, incluso de forma generalizada e indiscriminada, por cualquier sujeto que quiera y tenga la capacidad técnica para poder hacerlo.

4. Conclusiones

De lo expuesto hasta el momento se deduce que el fenómeno informático representa uno de los mayores retos a los que se enfrenta no sólo el Derecho penal español, sino el de todos los países industrializados.

Nadie, ningún país ni individuo, escapa a los peligros que genera la universalización del uso y del abuso de sistemas informáticos.

---

en soportes informáticos, y que por ello reciben la protección otorgada por el derecho contemplado en el art. 18.4 CE y no la del art. 18.3 CE referido al secreto de las telecomunicaciones; postura que, sin embargo, el propio autor matiza con respecto a los datos recopilados por los proveedores de servicios de Internet; datos que, a su juicio, conforman una nueva categoría de datos y que gozan de una especial protección por expresa prescripción de la LCDC, lo que no impedirá que deban seguir siendo considerados generalmente como datos de carácter personal. «Dirección IP; IMSI e intervención judicial…» (…).

54. ROMEO CASABONA, C., señala que este concepto, el de privacidad, resulta más amplio y global que el de intimidad que alude a facetas de la personalidad que aisladamente consideradas pueden carecer de significación intrínseca, pero que enlazadas dan lugar a un verdadero retrato del individuo. «Los datos de carácter personal como bienes jurídicos penalmente protegidos» (...), págs. 175 y 176, lo que evidentemente se corresponde de forma perfecta con el problema que hemos venido comentando y que se deriva de la protección de otra faceta de la intimidad, la del secreto de las telecomunicaciones.

55. De hecho se le tendrían que aplicar todas las restricciones que se aplican a cualquier otra modalidad limitadora del derecho al secreto de las telecomunicaciones: resolución y control judicial, motivación, apertura de procedimiento penal, excepcionalidad, temporalidad, delimitación del objeto investigado, etc. Véase sobre las mismas lo comentado por MORENO CATENA, V., «La intervención de las comunicaciones personales en el proceso penal» (...), págs. 411 y ss., MATA Y MARTÍN, R.M., *Delincuencia informática* (...), págs. 159 y ss., GARCÍA GONZÁLEZ, J., «Intervenciones de terceros en el correo electrónico...» (...), págs. 316 y ss.

56. VELASCO NÚÑEZ, E., «Aspectos procesales de la investigación y defensa en los delitos informáticos» en *La Ley,* n.º 6506, 2006. Versión digital consultada en www.laley.es (últ. vis. 7-12-2008).

Vivimos, como bien afirma BECK, en una «Sociedad de Riesgo mundial»[57] y eso hace que el Derecho penal necesite la colaboración internacional para hacer frente a los retos que esta nueva realidad le plantea. Una colaboración que, de hecho, se ha puesto en marcha hace ya mucho tiempo y que ha sido decisiva para que la mayoría de los países industrializados hayan realizado o estén realizando importantes reformas legislativas que tratan de afrontar de forma muy similar problemas penales muy similares.

Ahora bien, si el proceso armonizador internacional que se está produciendo en el ámbito de la denominada criminalidad informática se caracteriza por algo es por el hecho de servir como coartada, cuando no como factor directamente multiplicador, de la expansión extensiva e intensiva que está sufriendo el Derecho penal referido a dicha clase de criminalidad[58].

Así lo demuestra, a mi juicio, el hecho de que dicho Derecho internacional se haya preocupado muy mucho de obligar a los ordenamientos jurídicos nacionales a proteger nuestra privacidad frente a las, en ocasiones, nimias y casi míticas agresiones que pueden efectuarle personas casi legendarias, como los «temibles» *Hackers* y de exigirles que establezcan sistemas de trazabilidad legal que garanticen la eficaz investigación de delitos cometidos en Internet, pero no les haya exigido con el mismo empeño que establezcan un sistema de garantías jurídicas que nos protejan frente a los mucho más reales y posibles ataques que pueden realizar contra nuestra privacidad aquellos sujetos que, si bien tienen el deber de protegerla, en ocasiones, y esto no lo podemos ni debemos olvidar nunca, pueden ser quienes mayores daños le pueden ocasionar[59].

Ninguna de las propuestas internacionales referidas a la represión y persecución de la criminalidad informática ni, lo que es todavía más preocupante, ninguna de las últimas reformas legislativas nacionales relativas a dichas materias, han conseguido acabar con la enorme inseguridad jurídica que reina en la investigación penal en Internet.

¿Qué comunicaciones pueden vigilar y controlar las fuerzas de seguridad sin orden judicial? ¿Todas las que se realicen por un medio no completamente cerrado? ¿Sólo las que se realicen por uno que esté completamente abierto? ¿Cuándo comienza y cuando termina el proceso comunicativo que se ampara por el secreto del art. 18.3 CE? ¿Qué procedimiento ha de seguirse para otorgar la autorización que permite limitar dicho derecho? ¿Qué datos quedan protegidos por el mismo? ¿Sólo los relativos al contenido de la comunicación en sí misma considerada? ¿Todos los datos de tráfico? ¿Únicamente algunos? ¿Cuáles? ¿Hasta qué momento se protegen los que se protegen?

Éstas y otras muchas preguntas referidas a la investigación penal en Internet siguen sin encontrar una solución clara y segura en nuestra legislación procesal y tampoco parece que la normativa internacional esté demasiado preocupada por dársela.

¿Dónde queda entonces la exigencia de legalidad de la intromisión en el secreto de las comunicaciones de la que habla el Tribunal Europeo de Derechos Humanos? ¿Dónde la claridad y la seguridad de los requisitos para su legítima interceptación?[60] ¿Cómo es posible que ninguna de las numerosísimas normas internacionales referidas a la criminalidad informática se haya encargado de dar una respuesta adecuada y armonizadora a esta cuestión? ¿Acaso la existencia de posibles divergencias en esta materia no puede llevar a que las pruebas consideradas como lícitas en un país sean tenidas como completamente prohibidas y nulas en otro, provocando así la impunidad de alguno de los hechos delictivos realizados mediante el uso de Internet?

El desequilibrio que muestran las distintas normas internacionales relativas a la criminalidad informática

57. BECK, U., *¿Qué es la globalización?* (...), págs. 87 y ss. y 190 y ss.

58. De hecho, este efecto expansivo del Derecho penal internacional no es exclusivo del Derecho penal informático, ya que, como bien señala SILVA SÁNCHEZ, J.M., la internacionalización del Derecho penal actúa como factor multiplicador de la expansión de todo el Derecho penal. En *La expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales,* Ed. Civitas, 2.ª ed., Madrid, 2001, pág. 83.

59. En este sentido se ha de destacar que, si bien en España todavía se discute sobre la concreta tipicidad que serviría para sancionar los accesos ilícitos al contenido de los correos electrónicos realizados por funcionarios o autoridades públicas mediando causa por delito; sobre este tema véase lo comentado por GARCÍA GONZÁLEZ, J., «Intervenciones de terceros en el correo electrónico...» (...), pág. 314, quien se cuestiona si resultaría aplicable el delito del art. 534 (registro ilegal) o el del 536 CPE (interceptación ilegal de comunicaciones), lo que parece incuestionable es que la conducta de monitorización, incluso la realizada a gran escala y por un particular o una empresa, no es incardinable en ninguno de los delitos que protegen el secreto de las comunicaciones, ya que, como bien reconoció el Tribunal Europeo de Derecho humanos en la tantas veces citada Sentencia Malone vs. Reino Unido, la monitorización o el *metering* es algo distinto de la interceptación, conducta ésta que es la única que se castiga en los arts. 197, 198 y 536 del vigente CPE, limitándose el castigo de los primeros dos delitos a aquellas actuaciones interceptadoras que se hubiesen realizado mediante el uso de algún artificio técnico.

60. No se puede ni debe olvidar en tal sentido el hecho de que nuestra actual legislación relativa a la interceptación de comunicaciones, contenida en la LECr, fue considerada como insuficiente por su imprecisión por el TEDH aún antes de la aparición de toda la problemática referida a los nuevos medios de comunicación de Internet en su Sentencia de 30 de julio de 1988 (caso Valenzuela Contreras), como señala FERNÁNDEZ RODRÍGUEZ, J.J., quien afirma, además, que si bien la imprecisión de dicha ley pudo ser inicialmente considerada como «aún constitucional», el excesivo e injustificable retraso de su reforma habrían llegado a convertirla en una norma completamente inconstitucional. «Secreto e intervención de las comunicaciones en Internet» (…), págs. 132 y 151.

en favor de la represión penal y en detrimento de seguridad y de las garantías jurídicas de los ciudadanos resulta tan enorme que incluso puede resultar contraproducente desde el punto de vista de la propia eficacia investigadora.

Es posible que ello se deba a que los organismos impulsores de estos instrumentos internacionales tienden a adoptar una política de máximos en cuanto a la cesión de garantías del ciudadano frente a los poderes públicos, en un empeño por acabar con cualquier posible laguna de punibilidad[61] y por contar con la ratificación y el respaldo del mayor número posible de gobiernos nacionales para sus instrumentos[62], pero lo cierto y verdad es que a día de hoy no se puede discutir que en este concreto ámbito, en el del Derecho penal informático internacional, el binomio prevención-represión está venciendo en toda la línea a aquel otro, casi olvidado, que se compone por la unión de las garantías y las libertades[63].

La eterna y cada vez más encarnizada guerra entre prevención y garantías del Derecho penal ha encontrado un nuevo campo de batalla, el del Derecho internacional. Un campo de batalla que el ciudadano ve lejano y considera ajeno, pero que va a influir, y está influyendo ya, en la delimitación y determinación de sus libertades y de sus derechos.

Cuanto antes se tome conciencia de este hecho y de que, pese a lo que se pueda pensar, dicha normativa se crea con la intervención y el respaldo de los gobiernos y de los parlamentos nacionales, antes dejará el legislador penal de utilizar a la legislación internacional como coartada aparentemente indiscutible de sus más polémicas decisiones incriminadoras y antes comenzarán a aparecer los necesarios instrumentos jurídicos que reequilibren la balanza entre prevención y garantías, permitiendo que el ciudadano pueda defenderse de los abusos que traten de cometer quienes actúan desde el aparentemente protector ámbito de las administraciones públicas.

61. Este es el motivo que a juicio de SILVA SÁNCHEZ, J.M., lleva a que el denominado Derecho penal europeo tenga una pretensión fundamentalmente punitivista. «Los principios inspiradores de las propuestas de un Derecho penal europeo. Una aproximación crítica» en *Revista Penal,* n.º 13, 2004, pág. 145.

62. Así lo afirma, por ejemplo, MORALES GARCÍA, con respecto a la Convención europea sobre Cybercrime del Consejo de Europa en «Apuntes de política criminal en el contexto tecnológico....» (...), págs. 18 y ss.

63. De hecho, no le falta razón, por tanto, a MORALES PRATS, F., cuando hablando del procedimiento investigador de los delitos informáticos afirma que «... no parece que en el horizonte se oteen perspectivas de futuro garantistas para la intimidad del ciudadano» «La investigación del delito...» (...), pág. 36.