

## Mitos y realidades de la delincuencia informática. Un estudio sobre la reforma del Código Penal brasileño en materia de delitos informáticos, a la luz del Derecho penal Internacional.\* \*

Alfonso Galán Muñoz.

**Resumen:** En el presente artículo se analizan algunas de las principales novedades legislativas referidas a la delincuencia informática que se contemplan en el proyecto de reforma del vigente Código penal brasileño, claro ejemplo, a nuestro juicio, del proceso de internacionalización y modernización que están sufriendo todos los ordenamientos jurídico-penales de los países industrializados. No sólo se presta atención a las más destacadas novedades de Derecho penal sustantivo planteadas por dicha reforma, sino que también se estudia el papel que el ordenamiento jurídico brasileño pretende otorgar a los proveedores de servicios de Internet en el siempre complejo proceso de persecución de los delitos cometidos en la red.

**Palabras-clave:** delitos informáticos – legislación criminal brasileña – internet.

**Abstract:** In the present article there are analyzed some of the principal legislative innovations referred to the computer crime that it contemplate in the project of reform of the current penal Brazilian Code, clear example, to our judgment, of the process of internationalization and modernization that are suffering all the criminal law arrangements of the industrialized countries. Not only one pays attention to the most out-standing innovations of substantive Criminal law raised by the above mentioned reform, but also the role is studied that the juridical Brazilian arranging always tries to grant to the providers of Internet services in complex process of pursuit of the crimes committed in the network.

**Key-words:** computer crimes – brasilian criminal law – internet.

### 1. Introducción.

Vivimos tiempos de cambio. 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 solas<sup>1</sup>.

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

---

· El presente artículo contiene, ampliadas y desarrolladas las conclusiones que expuse en mi ponencia presentada al Seminario “*Perspectivas da justiça criminal. A agenda das reformas penais a luz das experiências nacional e internacional*”, organizado por la Secretaria de Asuntos Legislativos del Ministerio de Justicia y la Asociación de abogados de Sao Paulo y que se desarrollo entre los días 1 y 3 de Septiembre de 2008.

\* A lo largo del texto se utilizan las abreviaturas PCPB a la hora de aludir al Substitutivo que pretende reformar la legislación penal brasileña en esta materia; CPB al aludir al vigente Código penal Brasileño y CPE al hacerlo al Código penal español.

<sup>1</sup> SIEBER, U. “Límites del Derecho Penal”. Revista Penal, nº 22, 2008. Pg. 134 y ss

De hecho, los ejemplos de delincuencia transnacional son múltiples y cada vez más numerosos y van desde el terrorismo o el tráfico de drogas, hasta el blanqueo de capitales o el tráfico ilegal de personas.

Sin embargo, si hay un ámbito en el que la globalización ha mostrado lo inútiles que pueden resultar los esfuerzos exclusivamente nacionales por controlar los peligros que genera el uso de las nuevas tecnologías, éste ha sido el de la denominada criminalidad informática.

Nadie discute el hecho de 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 nuestro mundo, pero tampoco parece que se pueda negar que al hacerlo también han aparecido nuevas posibilidades de abusos y 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<sup>2</sup>. 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<sup>3</sup>. Así pues, todos los Estados necesitan de la colaboración de otros Estados para controlar y perseguir este tipo de actividades transnacionales y ello ha llevado a que cada vez existan más contactos y situaciones de conflicto entre los distintos ordenamientos jurídicos nacionales, dando lugar al incremento del fenómeno de la “interlegalidad” en el ámbito penal<sup>4</sup>.

La disparidad de criterios nacionales a la hora de solucionar los problemas que plantea el mundo de las nuevas tecnologías es inmensa y así, por ejemplo, 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 solo permitido sino completamente lícito que da lugar a una poderosa industria generadora cientos de millones de dólares de beneficios al año.

Sin embargo, parece imprescindible realizar un cierto acercamiento o armonización de las legislaciones nacionales si se quiere evitar que algunos países puedan llegar a

---

<sup>2</sup> BECK, U. *¿Qué es la globalización?* Ed. Paidós, Barcelona, 2008 Pg. 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” (...) Pg. 127

<sup>3</sup> 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*, nº 15, 2006-1. Pg. 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*, nº 22, 2008. Pg. 55

<sup>4</sup> No es de extrañar, por tanto, que ante esta situación, algunos autores como VOGEL, J. consideren 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*, nº 22, 2008. Pg. 161

convertirse en verdaderos *safe harbour* o en “paraísos de la criminalidad informática” desde los que los delincuentes podrían realizar sus actividades ilícitas con total impunidad.

Es precisamente esta necesidad de armonización internacional la que ha llevado a que el denominado Derecho penal informático se nos presente como uno de los ejemplos más paradigmáticos de la internacionalización del Derecho penal.

Ahora bien, esta internacionalización, difícil e incluso cuestionable en algunos aspectos<sup>5</sup>, 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 que atiendan a las nuevas necesidades de protección que tiene la sociedades de la Información; y, por otra, también puede ser una armonización “limitadora” o restrictiva de la intervención penal que venga a extender unos estándares de garantías mínimas que todos los países deberían reconocer a sus ciudadanos, con lo que se limitaría el ejercicio de su *ius puniendi* en este ámbito<sup>6</sup>.

Sin embargo, y pese a la existencia de esta dicotomía, la realidad nos demuestra que son pocos, como veremos, los instrumentos internacionales que hablan de garantías jurídicas del ciudadano frente al Estado y muchos, sin embargo, los que recomiendan o incluso obligan a los Estados a crear nuevos delitos que protejan a sus ciudadanos de esos enormes y en algunos casos, casi míticos peligros que les acechan tras las aparentemente inocentes pantallas de sus ordenadores.

Pero, ¿son reales todos estos peligros? ¿Cuánto hay de mito y cuánto de realidad en los peligros propios de la criminalidad informática?

## **2. Mitos y realidades sobre los nuevos riesgos de la Sociedad de la Información.**

El denominado Derecho penal Informático es, como no podía ser de otro modo, un hijo de su tiempo.

Los modernos sistemas informáticos se utilizan para controlar con máxima precisión mecanismos complejos que resultarían imposibles de controlar si estuviesen bajo el exclusivo control de un hombre.

Son estos sistemas los que controlan y gestionan la generación de energía nuclear, el tráfico aéreo o la mayor parte de las operaciones financieras actuales.

Nos encontramos, por tanto, con unas herramientas tecnológicas que aseguran con una precisión que escapa a la capacidad humana muchos aspectos de nuestras vidas y sin

---

<sup>5</sup> 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? (...). Pg. 182 y ss o lo comentado por VOGEL, J. con respecto al Derecho penal internacional, en “La internacionalización del Derecho penal”. (...). Pg. 167, entre otros.

<sup>6</sup> VOGEL, J. “La internacionalización del Derecho penal”. Pg. 163

embargo, o tal vez, precisamente por ello, todos estos mecanismos son vistos como nuevos focos de peligros y riesgos que han de ser necesariamente controlados y asegurados.

Posiblemente sea ese temor a los riesgos procedentes de estos nuevos sistemas el que ha determinado que el denominado Derecho penal informático sea mayoritariamente considerado como una de las muestras más evidentes del llamado “Moderno Derecho penal” que rige en la que se ha venido a denominar “Sociedad del Riesgo”<sup>7</sup>.

Los ciudadanos de estas sociedades quieren vivir completamente seguros y para ello le piden al Estado que los proteja de cualquier posible riesgo mediante la utilización del instrumento jurídico más severo y contundente de que dispone, el Derecho penal.

Sin embargo, parece que las viejas estructuras de este Derecho, sustentadas y creadas alrededor del delito doloso de lesión de bienes jurídicos individuales, no resultan adecuadas para conseguir tal fin. Mucho más eficaz, en términos securitarios, es el uso de delitos de peligro abstracto o presunto que permitan castigar a cualquier persona que realice una conducta que no se ajuste a lo que nos resulta completamente conocido y cierto, y que por ello y sólo por ello, se va a mantener dentro del ámbito de lo generalmente permitido.

Se pasa así a incriminar por precaución, atendiendo a la existencia de riesgos no conocidos ni probados, sino imprevisibles o presuntos. Riesgos que además se refieren a bienes jurídicos tan indeterminados que suelen ser delimitados y definidos mediante la genérica referencia a la “seguridad” de algún ámbito de nuestra realidad (la seguridad colectiva, la seguridad vial, la seguridad ciudadana o, como no, la seguridad informática), con lo que se facilita enormemente la tarea que todo legislador democrático debería afrontar a la hora de justificar la restricción de libertad que supone su decisión de crear cualquier nuevo delito.

Parece que es suficiente con acudir al comodín de la “seguridad” para que nadie cuestione lo que el legislador ha decidido castigar y, todavía menos, cómo lo ha hecho.

Esta situación ha determinado que bajo la apariencia de una extensión o expansión del Derecho penal dirigida a cubrir la aparición de nuevas y reales situaciones de desprotección, se encuentre oculta en muchos casos una verdadera intensificación de la intervención penal, ya que, no solo se prohíben nuevas conductas lesivas derivadas del mundo de las nuevas tecnologías, sino que, además, se las suele castigar con mayores penas que a las conductas delictivas tradicionales por considerarlas, siempre y en todo caso, como más graves y peligrosas que a éstas.

---

<sup>7</sup> Véase, sobre esta cuestión, SILVA SÁNCHEZ, J. M. “La expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales”. Ed. Civitas. 2ª Ed. Madrid, 2001. Pg. 25 y ss GRACIA MARTÍN, L. “Prolegómenos para la lucha por la modernización y expansión del Derecho Penal y para la crítica del discurso de resistencia”. Ed. Tirant lo Blanch. Valencia, 2003. Pg. 60 y ss. HASSEMER, W. *Persona, Mundo responsabilidad. Bases para una teoría de la imputación*. Valencia, 1999. Pg. 88; SIEBER, U. “Límites del Derecho Penal”. (...). Pg. 156; LÓPEZ ORTEGA, J. J. “La admisibilidad de los medios de investigación basados en registros informáticos”, en *Delincuencia informática. Problemas de responsabilidad*. Cuadernos de Derecho Judicial IX, 2002 Pg. 82 y ss; MATELLANES RODRÍGUEZ, N “Vías para la tipificación (...)”. Pg. 54 y ss o GALÁN MUÑOZ, A. “Expansión e intensificación del Derecho Penal (...)” Pg. 22, entre otros.

Ya en algún trabajo anterior, traté de demostrar como el discurso expansivo y el intensificador se entremezclan y confunden de forma significativa en el Derecho penal español de las nuevas tecnologías y como la utilización del tal vez viejo, pero no por ello menos importante y útil, principio de lesividad resulta una herramienta esencial para diferenciar ambas facetas del Derecho penal informático<sup>8</sup>.

A mi juicio para que se pueda entender que una conducta típica realmente afecta a un bien jurídico colectivo y genera, por tanto, un peligro con respecto al mismo que podría legitimar su represión penal anticipada o más intensa, se hace necesario que la misma cumpla dos condiciones básicas.

En primer lugar, tiene que ser una conducta que realmente pueda llegar a ocasionar una lesión o daño efectivo del valor que supuestamente se trata de proteger, ya que, solo dicha posibilidad, por muy lejana que pueda ser, permite considerarla como una actuación realmente peligrosa y lesiva para dicho bien jurídico o valor. Pero, además, y en segundo lugar, dicho peligro tiene que ser tan amplio que pudiese realmente llegar a lesionar los bienes jurídicos individuales de una pluralidad indeterminada de personas y no solo los de un grupo perfectamente delimitado y concretable de los mismos.

Sólo cuando se constaten ambos hechos, la existencia de un riesgo no meramente presunto sino real y la indeterminación de su frontera de peligro en términos cuantitativos, se podrá decir que nos encontramos ante una conducta que, aún cuando no haya llegado a dañar ningún bien jurídico individual, ha puesto en peligro un número tan significativo de los mismos que representa una verdadera lesión de la seguridad de todos ellos.

Tal vez un ejemplo del propio mundo de la delincuencia informática, nos ayude a entender mejor lo anteriormente comentado.

Cuando un sujeto borra o daña los datos de otro, no pone en peligro los datos contenidos en el resto de sistemas informáticos. Éstos, los que se encuentran en el resto de ordenadores no se ven afectados en nada por la conducta realizada por dicho sujeto. El único sistema afectado, los únicos datos lesionados son los del concreto titular de aquel sistema que recibe el ataque, con lo que se demuestra lo erróneo que resultaría considerar este tipo de conductas como lesivas de un bien jurídico colectivo y no de uno exclusivamente individual.

Distinta, muy distinta, de esta conducta lesiva individual será la realizada por aquel sujeto que crease y difundiese un virus en la red que estuviese diseñado para extenderse por la misma y para borrar la información contenida en todos los discos duros en los que se instalase.

Con la simple realización de esta conducta no se ha dañado todavía ningún dato informático. Lo que sí se ha hecho es generar un peligro de destrucción o de daño con respecto a los mismos. Un peligro cierto y real que puede generar la destrucción de los datos contenidos no en un único ordenador, sino en un número indeterminado de ellos.

---

<sup>8</sup> Sobre este aspecto y su repercusión en la crítica del Derecho penal español de las nuevas tecnologías véase, GALÁN MUÑOZ, A. "Expansión e intensificación del Derecho Penal (...) Pg. 29 y ss

No estamos ya ante una conducta que afecta a los datos de una sola persona. Estamos ante una actuación que pone en cuestión y en verdadero peligro los datos de todos los sujetos que intervienen en la red, hecho que nos permitirá considerarla como una conducta realmente lesiva de la “seguridad de los sistemas informáticos”, con lo que se podrá justificar que se castigue de forma anticipada y de modo incluso más severo que aquellas otras que solo viniesen a poner en cuestión o a lesionar un bien jurídico estrictamente individual.

Como se puede comprobar, es cierto que existen nuevos y enormes riesgos específicamente informáticos (piénsese, por ejemplo, en referencia al ejemplo anterior, en los enormes daños económicos que puede generar la difusión de un virus altamente dañino en la red; daños que cualquiera puede producir con un simple ordenador), pero también lo es que hay muchos otros que se fundamentan más en el mito que en la realidad.

Veamos ahora cuánto hay de mito y cuánto de realidad en el proyecto de Reforma del Decreto-Lei nº 2848 del Código penal brasileño.

### **3. La reforma del Código Penal brasileño en materia de criminalidad informática**

Resulta absurdo pensar que el proceso de internacionalización del Derecho penal informático o de las nuevas tecnologías va a dar lugar a una homogenización de los modelos nacionales de protección en esta materia, ya que, como bien señala VOGEL, este proceso no puede olvidar que las particularidades y peculiaridades que presentan las distintas culturas y tradiciones jurídicas nacionales pueden provocar que la “importación” sin más de elementos e instrumentos jurídicos legítimos y funcionales en unos ordenamientos jurídicos resulte ilegítima y disfuncional en otros<sup>9</sup>

Se deben tener en cuenta todas las peculiaridades de un sistema jurídico para poder emitir un juicio global sobre la eficacia o funcionalidad de cualquiera de los instrumentos que la componen, con lo que resultaría temerario por mi parte tratar de emitir un juicio de esta clase sobre la reforma proyectada sin conocer previamente dichas peculiaridades y sin analizar la realidad social sobre la que sistema brasileño de protección frente a la delincuencia informática se pretende proyectar.

Sin embargo, no creo que este hecho resulte óbice alguno para poder analizar, desde un punto de vista estrictamente técnico, algunos de los aspectos de la comentada reforma que más poderosamente me han llamado la atención.

En concreto, y dada la amplitud y diversidad de temas que en la misma se abordan, me gustaría dedicar algunas reflexiones generales a la regulación que el citado proyecto otorga a los denominados delitos de daños informáticos y a los de accesos no autorizados a sistemas informáticos, para finalmente centrar mi atención, siquiera de forma somera, en una de las cuestiones transversales a toda la criminalidad informática que mayor componente transnacional presenta, la referida al papel que los proveedores de servicios están llamados a desempeñar en el proceso de persecución penal de los delitos cometidos a través de Internet; tema que también es abordado por la referida reforma.

#### **3.1. La reforma de los delitos de daños**

<sup>9</sup> VOGEL, J. “La internacionalización del Derecho penal”. (...). Pg. 167

Como ya he tenido ocasión de exponer, la imparable implantación de los sistemas informáticos en nuestras vidas cotidianas ha planteado un enorme problema de adaptación a los tradicionales instrumentos conceptuales utilizados por el Derecho.

En los ordenadores prima lo incorporado e intangible, mientras que el mundo que vivían nuestros legisladores decimonónicos era un mundo mucho más corporal y aprehensible.

Nadie cuestiona la necesidad de proceder a adaptar los instrumentos jurídicos tradicionales a las necesidades de este nuevo mundo. Sin embargo, dicho proceso de adaptación tiene que tratar de no caer en el temor irracional hacia lo desconocido, si se quiere evitar que este nuevo mundo (el mundo virtual) se convierta en un universo mucho más controlado y opresivo que el resto de nuestra realidad cotidiana.

Es por ello, por lo que considero que sería útil partir de una suerte de principio básico, “el principio de neutralidad jurídica de las nuevas tecnologías”; un principio conforme al cual se debería entender que el hecho de que una conducta se realice por medio de sistemas informáticos o de alguna de las modernas tecnologías de la información no puede determinar, por sí solo y automáticamente, que se le tenga que otorgar un tratamiento jurídico diferente a aquel otro comportamiento análogo que se hubiese realizado sin utilizar dichos sistemas.

En efecto, parece lógico pensar que si una conducta está permitida y es lícita fuera de la realidad virtual de los ordenadores también debería serlo dentro de la misma. Ningún problema parece haber en ello.

En realidad, el verdadero problema se plantea cuando una actuación prohibida y sancionable en el mundo físico no tiene la misma consideración si se realiza dentro del denominado mundo virtual.

Por ejemplo, ¿por qué dañar dolosamente cualquier cosa de un tercero, incluso la dotada de un valor patrimonial mínimo, se castiga por el Derecho penal y destruir un dato o un programa informático con un valor económico infinitamente mayor, debe quedar sin ningún castigo precisamente por carecer los mismos del carácter corporal que caracteriza a las cosas a efectos penales? ¿Por qué alterar un documento impreso realizado por un tercero para perjudicarlo puede castigarse como delito de falsedad y hacerlo con uno que sea digital no?

Nos encontramos en estos casos y en otros muchos, con conductas muy semejantes que sin embargo reciben un tratamiento jurídico muy diferente por el mero hecho de que cuando el legislador creó nuestras leyes penales no pudo prever el enorme número de posibilidades que las modernas tecnologías de la información nos iban a aportar.

Las lagunas de punición son importantes y la necesidad de que el legislador las cubra urgentes, pero ¿cómo hacerlo?

La técnica más habitualmente utilizada ha sido la de la asimilación, esto es, el legislador ha asimilado la conducta ilícita realizada en el mundo virtual con aquella efectuada en el mundo corporal con la que encontraba más semejanzas.

Así, lo ha hecho, por ejemplo, el legislador español con relación a los documentos y los daños informáticos -aunque bien es cierto que con bastante peor fortuna en este último delito que en el primero-; y así también parece querer hacerlo el legislador brasileño en la nueva redacción que pretende dar a los artículos 163, 297 y 298 del Código penal vigente en dicho país.

Centrémonos en el primero de dichos artículos, en el referido a los daños. Dice el nuevo precepto que será constitutivo de daños:

*“Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:  
.....”(NR)”*

Como se puede comprobar la asimilación hecha por el legislador entre los objetos corporales y los datos inmateriales es completa, lo que va a evitar los múltiples problemas concursales e interpretativos que tenemos en España a la hora de analizar y aplicar nuestra regulación referida a los denominados daños informáticos, ya que, al aparecer éstos contemplados en un tipo cualificado del delito general de daños que no se exige, por lo menos de forma expresa, que se ocasione merma patrimonial alguna para imponer su correspondiente pena, no está nada claro si el legislador no ha querido convertir a los daños informáticos en una figura delictiva autónoma y de naturaleza diversa al resto de los delitos de daños.

En concreto, se podría pensar que nos encontramos ante una figura que castiga de forma autónoma y cualificada la destrucción o alteración de los elementos lógicos de un sistema informático con independencia de su valor patrimonial, con lo que se tendría que considerar que dicha figura siempre entraría en concurso de delitos y no de leyes con aquellas otras que valorasen y castigasen la producción de los daños materiales que se pudiesen ocasionar al borrar o destruir los datos informáticos, como serían, por ejemplo, los derivados de la destrucción física del soporte en el que los datos dañados estuviesen almacenados<sup>10</sup>.

Mucho más lógico parece considerar, como hace el proyecto brasileño, a los daños que recaigan sobre datos o programas informáticos como ataques que solo serán delictivos cuando realmente afecten al patrimonio ajeno y entender, en consecuencia, que el concreto valor de dicha afección patrimonial debe ser valorado de forma conjunta y global con el que se derivasen de los daños ocasionados a los objetos corporales que les sirviesen de soporte o que se utilizasen para procesarlos o utilizarlos.

Otra gran ventaja de la tipificación brasileña frente a la española es la completa asimilación que se produce entre los medios de ataques referidos a los objetos materiales e inmateriales.

Se castiga el destruir, inutilizar o deteriorar tanto cosas como datos electrónicos, lo que determina que no sea necesario alterar la sustancia de la cosa dañada (física o no) para

<sup>10</sup> Critico con esta posibilidad y favorable a considerar incluibles en los daños castigados y valorados por el art. 264.2 CPE a los que recaigan sobre los soportes se muestra GONZÁLEZ RUS, J. J. “Los ilícitos en la red (I): Hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes”, en *El cibercrimen: nuevos retos jurídico-penales nuevas respuestas político-criminales*. Ed. Comares. Granada, 2006. Pg. 259; solución que, sin embargo es cuestionada por MATA Y MARTÍN, R. M. *Delincuencia informática y Derecho penal*. Ed. Edisofer. Madrid, 2001. Pg. 65.

poder apreciar la comisión de este delito, cuestión que, sin embargo, sigue siendo discutida en España donde el Código penal solo contempla la inutilización como modalidad comisiva de los daños referidos los elementos lógicos de los sistemas informáticos (datos o programas), siendo, por tanto, dicha conducta atípica cuando se refiere a cualquier otro tipo de objeto<sup>11</sup>.

Esta situación puede cambiar en breve como consecuencia, precisamente, de una normativa armonizadora internacional.

En concreto, como consecuencia de la más que probable transposición de la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea, relativa a los ataques contra los sistemas Informáticos, cuyos artículos 3 y 4 obligan a todos los países miembros de la Unión Europea a castigar penalmente no solo el deterioro o destrucción de datos informáticos, sino también su inutilización o el hecho de que por esos u otros medios se pudiese llegar a provocar la obstaculización o interrupción significativa el funcionamiento de un sistema informático<sup>12</sup>.

No solo se exige, por tanto, que se castigue el deterioro o la mera inutilización de datos o programas, sino que también se obliga a los Estados miembros de la UE a establecer previsiones penales que repriman las denominadas “Denegaciones de Servicios” (*Denial of Service*), esto es, aquellos supuestos en los que la lesión patrimonial se derivase del bloqueo o de la reducción del rendimiento del sistema informático atacado.

Estos efectos perturbadores pueden generar enormes perjuicios patrimoniales (piénsese, por ejemplo, en los que se ocasionaría a una empresa de transporte aéreo si se inutilizase la *web* desde la que vende sus billetes a sus clientes) y, sin embargo, no son sancionados ni aparecen contemplados como posibles resultados consumativos del delito de daños contemplado en la reforma del Código penal brasileño, hecho que sin duda dará lugar a discusiones judiciales y quien sabe si también obligará a futuras reformas legales.

Ahora bien, no creo que ésta sea la principal deficiencia de la reforma de los daños propuesta. En mi opinión, su principal problema se deriva de algo que no está contenido en el tenor literal del propuesto artículo art. 163 PCPB, sino que se encuentra en otro lugar, en el artículo que define muchos de los conceptos utilizados en la reforma, el artículo 16 del texto de la reforma.

---

<sup>11</sup> Este hecho ha llevado a que parte de la doctrina española considere necesaria la alteración de la “sustancia” de los datos para apreciar la comisión de este delito. Así, por ejemplo, GONZÁLEZ RUS, J. J. “Los ilícitos en la red (I):...” (....) Pg. 256, RODRÍGUEZ MOURULLO, G./ ALONSO GALLO, J. / LASCURAÍN SÁNCHEZ, J. A. “Derecho penal e Internet” en Régimen jurídico de Internet. Ed. LA Ley, Madrid, 2002. Pg. 256, entre otros.

<sup>12</sup> En concreto estos dos preceptos establecen que “**Artículo 3 Intromisión ilegal en los sistemas de información.** Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

**Artículo 4 Intromisión ilegal en los datos.** Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Este precepto define el concepto de dato informático (o electrónico como se califica a lo largo de todo el texto) estableciendo que será tal “...*qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado*”, concepto que si bien resulta perfectamente aplicable al de dato utilizado en los nuevos delitos de falsedad documental contenidos en los nuevos artículos 297 y 298 PCPB, no parece que se corresponda con el que se debería utilizar como objeto material de los daños.

En efecto, no todo dato dotado de valor patrimonial y susceptible de ser destruido, dañado o inutilizado, ha de representar hechos, informaciones o conceptos. De hecho, muchos de ellos no lo hacen. Son simples expresiones numéricas que interactúan unas con otras, gracias a la utilización de los programas que los procesan para dar lugar a la enorme variedad de posibilidades que nos brinda un ordenador, desde leer un texto, ver una foto, escuchar música, hasta simplemente jugar con ese personaje (*avatar*) que hemos creado a nuestro gusto en alguno de los múltiples juegos de *roll* que se desarrollan en la red.

Mucho más correcto me parece, por tanto, considerar que cuando aludimos a datos informáticos o electrónicos a efectos del delito de daños nos estamos refiriendo a “*las unidades elementales procesadas por un sistema informático y de cuya combinación resulta la información contenida en el sistema*”<sup>13</sup>; concepto éste que además de ser más amplio que el utilizado por el citado art. 16 PCPB, permite diferenciar nítidamente al objeto material propio de este delito del contemplado en el delito de falsedad documental, el documento electrónico o informático.

En cualquier caso, resulta evidente que nos encontramos ante un caso de verdadera asimilación legislativa que cubre una laguna de punición mediante la introducción de un delito doloso y de lesión que nada tiene que ver con el Moderno Derecho penal de la Sociedad de la Información.

Pero claro, la reforma no se queda aquí. También crea e introduce un delito que podría hacernos pensar que nos encontramos, ahora sí, ante una manifestación de ese nuevo Derecho Penal; el delito de “Inserción o Difusión de Código Malicioso” contemplado en el art. 163-A PCPB, precepto que establece que:

**“Art. 163-A.** *Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.*

*Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.”*

Nos encontramos ante una figura delictiva que, a diferencia de la anterior, se consuma antes de la efectiva lesión del patrimonio individual de ningún sujeto, lo que nos podría llevar a pensar que estamos ante uno de esos delitos de peligro para bienes jurídicos colectivos que caracterizan al denominado “Moderno Derecho penal”.

---

<sup>13</sup> GONZÁLEZ RUS, J. J. “Protección penal de sistemas, elementos, datos, documentos y programas informáticos”, RECPC 01-14 (1999), en [http://criminet.ugr.es/recpc/recpc\\_01-14.html#1.DAÑ](http://criminet.ugr.es/recpc/recpc_01-14.html#1.DAÑ) (Ult. vis. 1-8-2008); el mismo autor en “Los ilícitos en la red (I):...” (...). Pg. 256 y MATA Y MARTÍN, R. M. *Delincuencia informática* (...) Pg. 66

En concreto, podríamos creer que estamos ante un delito que adelanta las barreras de intervención penal para protegernos de los enormes peligros que los virus, las bombas lógicas y demás códigos informáticos dañinos nos pueden llegar a producirnos a todos; pero, ¿es realmente así?

A mi juicio no.

No lo es, en primer lugar, porque esta figura permite castigar a todo aquel que introduzca alguno de estos códigos maliciosos en un ordenador, aún cuando el código en cuestión no esté diseñado ni sea idóneo para extenderse ni para dañar otros ordenadores o sistemas informatizados distintos de aquel en el se introdujo inicialmente. No se exige, por tanto, que se produzca afección colectiva alguna para apreciar este delito. Su injusto se configura y se completa con la mera puesta en peligro del patrimonio individual de cualquier persona, circunstancia que demuestra, a mi modo de ver, que nos encontramos ante un delito protector de un bien jurídico de naturaleza eminentemente individual (el patrimonio) y no ante uno que realmente trate de proteger valor colectivo alguno.

Pero es que, además y por otra parte, si nos detenemos un poco en el análisis del artículo comentado nos daremos cuenta de que el mismo no castiga la mera creación de esos peligrosos códigos, sino su difusión y de que ésta sólo es típica cuando se efectúa de forma dolosa (art. 18.II CPB), circunstancias ambas que van a determinar que este nuevo delito castigue conductas constituirían, por sí solas y en todo casos, verdaderos actos ejecutivos del delito de daños del artículo 163 PCPB<sup>14</sup>, con lo que el nuevo art. 163-A PCPB no castigará conductas inicialmente atípicas e impunes, sino actuaciones que se podrían haber sancionado, sin mayores problemas, utilizando el tipo delictivo de la tentativa del delito de daños contemplado en el artículo que lo precede (art. 163 PCPB).

Aquí no hay una expansión extensiva del Derecho penal. No estamos ante una figura que realmente adelante las barreras de intervención penal a actuaciones que eran atípicas antes de su creación.

---

<sup>14</sup> En contra de esta postura parece posicionarse GONZÁLEZ RUS, J. J. quien señala que la carga de un programa en un sistema informático no es un acto de ejecución del delito de daños informáticos, lo que le lleva entender que estas conductas sólo podrían ser castigadas acudiendo a la vía de la comisión por omisión al haberse convertido quien introdujo el virus todavía no operativo y que puede estar pendiente del cumplimiento de una determinada condición para estarlo (como sucede, por ejemplo, con las bombas lógicas) como un garante por ingerencia de los resultados lesivos a que dicha conducta hubiese dado lugar, al haber sido él quien había generado el peligro del que éstos proceden. “Los ilícitos en la red (I): ...” (...) Pg. 266. A nuestro juicio, lo único que se produce en tales casos es un distanciamiento temporal entre el acto ejecutivo del delito y la efectiva producción de su resultado consumativo, circunstancia que si bien puede dar lugar a algunas alteraciones relevantes en el curso causal que, conforme a los criterios de la imputación objetiva, ha de unir ambas para completar el injusto consumado del delito de daños, no impide en absoluto apreciar el desvalor objetivo y subjetivo propio de la tentativa (incluso acabada) del mismo. En este sentido se manifiestan también MATA Y MARTÍN, R. M. *Delincuencia informática* (...) Pg. 75 y CORCOY BIDASOLO, M. “Protección penal del sabotaje informático. Especial consideración de los delitos de daños”. La Ley, nº 2400. 1990. Pg. 1014 y 1015 quien, además, acertadamente destaca como el hecho de que el sujeto pueda impedir la producción del resultado consumativo que trato de realizar mediante la inserción y difusión del virus es algo que puede resultar relevante a efectos de la apreciación de su posible desistimiento, pero no incide en modo alguno en la apreciación de la realización de la tentativa de este delito.

Pero entonces, ¿qué sentido tiene castigar este tipo de conductas de forma autónoma? Es decir, ¿por qué el legislador ha convertido a estas conductas en delito independientes si ya podría castigarlas como tentativas de daños?

La respuesta a esta cuestión resulta a mi juicio evidente. Lo único que el legislador ha pretendido al crear este delito es incrementar las penas que habrían de aplicarse a las tentativas de daños que se efectuasen mediante la difusión de virus y otros códigos maliciosos en sistemas informáticos. Esa es su principal y casi única finalidad. Una finalidad intensificadora de la intervención penal que le ha llevado, entre otras cosas, a castigar igual a quien difunde un código altamente peligroso para todos los sistemas informáticos, que quien se limita a insertar un código malicioso que sólo puede afectar al concreto sistema en el que se inserta<sup>15</sup>, asimilación punitiva que olvida que ambas conductas presentan una naturaleza jurídica y un contenido de injusto netamente diferenciados y que lleva a que este delito presente serios problemas de proporcionalidad.

Sin embargo, la regulación penal del proyecto referida a los códigos maliciosos no termina aquí sino que también establece que

*“§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:*

*Pena – reclusão, de 2(dois) a 4 (quatro) anos, e multa.”*

Se castiga así la consecución del efectivo resultado pretendido por el difusor del código malicioso, es decir la del perjuicio patrimonial, y se hace, como no, incrementando la pena aplicable a aquel que lo hubiese ocasionado.

Sin embargo existe una diferencia notable entre el daño o perjuicio patrimonial aquí contemplado y el recogido, por ejemplo, en el tipo básico de daños del ya comentado artículo 163 PCPB. En el aquí contemplado no se exige que la efectiva afección patrimonial se derive de la destrucción o inutilización del dato informático, sino que puede proceder de la destrucción, deterioro, alteración o incluso -y esto es importante- de la mera obstrucción del funcionamiento del sistema informático infectado o de la producción de un funcionamiento no autorizado del mismo.

Estamos hablando, por tanto, de la producción de una verdadera denegación de servicios, resultado que, como vimos, puede dar lugar a enormes lesiones patrimoniales para quien lo sufra, pero que no se contempla como posible resultado consumativo del delito del tipo básico de daños.

---

<sup>15</sup> No deba olvidarse que el art. 16.IV del proyecto de reforma define al código malicioso como “...o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida”, con lo que su transmisibilidad a múltiples sistemas informáticos, no es un requisito de la delimitación de este instrumento peligroso, ni parece que sea una exigencia típica delimitadora del injusto objetivo del artículo 163-A, ya que, en éste permite castigar la difusión en la red, en un dispositivo de comunicación, pero también en un sistema informatizado individual, concepto definido de forma amplia por el art. 16.II de la citada reforma y que engloba desde los sistemas individuales de procesamiento de datos más complejos hasta los más simples.

Así pues, el nuevo art. 163-A PCPB puede servir para sancionar algunas de las producciones dolosas de denegaciones de servicios, con lo que cubriría, en cierta medida, la laguna de protección que presentaba el delito de daños del artículo 163 PCPB.

Sin embargo, este nuevo delito solo castiga aquellas denegaciones de servicio que se deriven del uso y la difusión de códigos maliciosos, con lo que dejará sin castigo otras muchas conductas que podrían dar lugar al mismo resultado lesivo sin utilizar tales códigos, como sucederá, por ejemplo, con aquellas que consiguiesen bloquear el ordenador ajeno mediante la simple y directa eliminación de algún dato o programa contenido en el mismo o con aquellas que consiguiesen el mismo resultado “bombardeando” el sistema informático en cuestión con un número tal de peticiones de servicios que llegasen a saturar su capacidad de procesamiento o de transmisión<sup>16</sup>.

Pero los problemas presentados por esta nueva figura delictiva no acaban aquí. La tipificación propuesta con respecto a las lesiones patrimoniales derivadas de denegaciones de servicio dará lugar a que, cuando la difusión o distribución del código malicioso realizada provoque (como suele provocar) no solo la inutilización o la obstrucción del funcionamiento del sistema sino también la pérdida o inutilización de algunos de los datos dotados de valor económico contenidos en el mismo, se tenga que apreciar el correspondiente concurso de delitos entre esta nueva figura delictiva y la contemplada en el art. 163 PCPB, lo que puede llevar a que se apliquen penas no proporcionadas a la gravedad del injusto realmente ocasionado.

Es por ello, por lo que consideró que sería mucho más adecuado incluir a la obstaculización o pérdida de funcionalidad del sistema informático como uno más de los posibles resultados patrimonialmente lesivos que se castigan en el tipo básico de los daños, ya que, ello permitiría castigar tales lesiones patrimoniales con independencia del medio que se hubiese utilizado para ocasionarlas y haría que las mismas se pudiesen valorar mediante la apreciación de un único delito de daños y no a través de ficticia concurrencia de varios de ellos; mientras que, por otra parte, también entiendo que sería conveniente retocar el delito de difusión o inserción de códigos maliciosos para convertirlo en un delito que solo castigase actuaciones difusoras que realmente pudiesen afectar a una cantidad indeterminada de sistemas informáticos, lo que lo convertiría en un verdadero delito protector de un bien

---

<sup>16</sup> Podría pensarse que el nuevo tenor literal del art. 266 del proyecto que venimos comentando podría cubrir esta laguna de punición al ampliar el número de conductas que podrían castigarse conforme a dicho delito y considerar como constitutivo de dicho delito *“Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:..... “(NR)”*. Sin embargo, esta primera impresión resulta errónea, ya que parece incuestionable, -dada la ubicación sistemática del comentado precepto-, que nos encontramos ante delito que solo permitirá castigar a aquellas perturbaciones de los sistemas informáticos que realmente tengan una relevancia o una repercusión pública y colectiva, con lo que aquellas otras que simplemente afecten al patrimonio de un concreto individuo seguirían quedando sin castigo, mientras no se realicen mediante el uso de uno de los códigos maliciosos de los que habla el art. 163-A. del proyecto.

jurídico colectivo, dotado de una naturaleza jurídica netamente diferenciada de la propia de la mera tentativa del delito de daños<sup>17</sup>.

### **3.2. Los accesos no autorizados a redes de ordenadores o sistemas informáticos.**

Mucho más próximo a las peculiaridades propias del denominado moderno Derecho penal se muestra la persecución y el castigo penal de las conductas de lo que se ha venido a denominar como intrusismo informático, *Hacking* o “acceso no autorizado a redes de ordenadores, dispositivos de comunicación o sistemas informatizados” como las califica el proyecto de reforma que venimos comentando.

El merecimiento y la necesidad del castigo de las actuaciones de mero intrusismo informático han suscitado un vivo debate en el seno de la doctrina española, encontrando su incriminación penal tanto partidarios como detractores.

Para los primeros, su incriminación vendría a facilitar la siempre difícil prueba de la ejecución de los delito informáticos, puesto que, a pesar a que muchas de estas acciones intrusitas no ocultan sino verdaderos actos ejecutivos de delitos contra la intimidad o contra el patrimonio, siempre resulta difícil probar que se hubiesen realizado con la concurrencia los elementos subjetivos que permitiría castigarlos como tentativas de dichos delitos (p. ej. la intención de descubrir secretos o el dolo de dañar o perjudicar)<sup>18</sup>.

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 accediese al mismo<sup>19</sup>.

En estos casos, como en todos los que se han venido a denominar de “Hacking blanco” resulta imposible apreciar la realización de tentativa delictiva alguna.

De hecho, muchas de estas conductas no presenta ninguna dañosidad objetiva que pueda justificar su castigo, por cuanto ni ponen en peligro el patrimonio del dueño del sistema informático vulnerado, ni inciden sobre ningún ordenador que contengan informaciones que puedan ser consideradas como secretos personales o industriales a efectos

---

<sup>17</sup> Sobre las concretas repercusiones técnicas y las ventajas que tiene esta configuración típica respecto al principio de proporcionalidad en los delitos informáticos patrimoniales como los de daños o el de estelionato informático, véase, con más extensión, lo comentado por GALÁN MUÑOZ, A. En “El nuevo delito del artículo 248.3 CP: ¿un adelantamiento desmedido de las barreras de protección penal del patrimonio?” La Ley nº 3 2004. Pg. 1859 y ss

<sup>18</sup> GUTIÉRREZ FRANCÉS, M<sup>a</sup> L. “El intrusismo informático (Hacking): ¿represión penal autónoma?”. *Informática y derecho: Revista iberoamericana de derecho informático*, nº 12-15, 1996 Pg.1180 y GONZÁLES RUS, J. J. quien considera que será realmente excepcional el caso en el que la intromisión ilícita no este animada por ninguna finalidad ilícita. “Los ilícitos en la red (I):...” (...). Pg. 247

<sup>19</sup> ORTS BERENQUER, 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. Pg. 92. MATELLANES RODRÍGUEZ, N. “Vías para la tipificación...” (...) Pg. 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. Pg. 55 y ss

de lo establecido en los delitos contemplados en los art. 197 y 278 del CPE<sup>20</sup>. Es por ello, por lo que la mayoría de la doctrina española ha entendido que el ordenamiento penal español considera, por lo menos por el momento, a los meros accesos no autorizados a sistemas informáticos ajenos o *Hacking* como conductas completamente atípicas<sup>21</sup>. Y digo por el momento porque parece que esto tendrá que cambiar en breve y tendrá que hacerlo, precisamente, como consecuencia del proceso de internacionalización del Derecho penal informático español.

Existen diversos instrumentos internacionales que expresamente exigen la incriminación penal de este tipo de conductas. Entre ellos se destacan, a mi modo de ver, dos<sup>22</sup>, el que nos viene dado por el Convenio del Consejo de Europa sobre criminalidad informática (firmado en Budapest el 23 de Noviembre de 2001 y abierto a la firma de cualquier país y no sólo de los países europeos) y, de nuevo, la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea, relativa a los ataques contra los sistemas informáticos, cuyo artículo 2 obliga a todos los Estados miembros de la Unión a sancionar penalmente los accesos ilegales a los sistemas de información<sup>23</sup>.

Dejando ahora a un lado los evidentes problemas técnicos y de legitimación que presenta la incriminación de este tipo de conductas, hemos de señalar que la misma parece dar el espaldarazo definitivo al surgimiento de un nuevo bien jurídico de naturaleza netamente informática. Un bien que algunos denominan “pacífico uso y disfrute de las redes informáticas a través de redes telemáticas”<sup>24</sup>; otros “confianza en el funcionamiento de los sistemas informáticos”<sup>25</sup> o “inviolabilidad informática”<sup>26</sup>, pero que el PCPB ha decidido llamar “Seguridad de los sistemas informáticos”

En efecto, el nuevo art. 285-A PCPB crea el delito de acceso no autorizado a redes, dispositivos de comunicación o sistemas informáticos, insertándolo en un capítulo, el IV, que tiene como título “**Dos Crimes Contra A Segurança Dos Sistemas Informatizados**”, estableciendo que:

<sup>20</sup> Entre otros, ORTS BERENGUER, E. / ROIG TORRES, M. “Delitos contra la intimidad, ...” (...) Pg. 92 y ss

<sup>21</sup> MORÓN LERMA, E. *Internet y Derecho penal: (...)*. Pg. 64, GONZÁLES RUS, J. J. “Los ilícitos en la red (I):...” (...) Pg. 246; GALÁN MUÑOZ, A. “Ataques contra sistemas informáticos”. En Boletín de información del Ministerio de Justicia., Año 60, Nº 2015, 2006. Pg. 226 y 227

<sup>22</sup> También lo destaca MATELLANES RODRÍGUEZ, N. “Vías para la tipificación...” (...) Pg. 57 y ss

<sup>23</sup> 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” (...) Pg. 225 a 232

<sup>24</sup> ROMEO CASABONA, C. “Los datos de carácter personal como bienes jurídicos penalmente protegidos” (...), en *El cibercrimen: nuevos retos jurídico-penales nuevas respuestas político-criminales*. Ed. Comares. Granada, 2006. Pg. 189

<sup>25</sup> GUTIÉRREZ FRANCÉS, M<sup>a</sup> L. “El intrusismo informático (Hacking):...” (...) Pg.1183. En esta línea parece posicionarse, MATELLANES RODRÍGUEZ, N. “Vías para la tipificación...” (...) Pg. 65

<sup>26</sup> GALÁN MUÑOZ, A. “Ataques contra sistemas informáticos” (...) Pg. 228

**“285-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:  
Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.”**

Como fácilmente se podrá deducir, este precepto convierte o pretende convertir en delito al mero intrusismo informático, es decir, al mero acceso no autorizado a un sistema informático ajeno, conducta que hasta ahora el ordenamiento penal brasileño también mantenía en el ámbito de lo atípico.

La opción legislativa por la incriminación de estas conductas se corresponde perfectamente con las tendencias internacionales que acabamos de comentar.

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 nos encontramos ante un delito que castigue la puesta en peligro de un bien jurídico individual, sino la efectiva lesión de un nuevo bien jurídico, con carácter netamente informático y de naturaleza colectiva, como sería la denominada seguridad informática<sup>27</sup>.

En concreto, se consideraba que este delito sería un delito de mera actividad pero también de efectiva lesión, ya que, la mera realización de su conducta típica (el acceso) lesionaría, siempre y en todo caso, a ese nuevo bien jurídico colectivo que se engloba en el concepto de seguridad informática.

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 entender que el acceder a un único sistema informático afecta o incluso lesiona la seguridad de los sistemas informáticos en general supone desdorar de cualquier contenido material de injusto a la supuesta afección de este nuevo bien jurídico colectivo.

¿En qué me afecta a mí que se acceda al ordenador de mi vecino o al de un completo desconocido? ¿Qué lesión o, cuándo menos, qué puesta en peligro sufre el sistema informático de mi despacho o el de mi casa 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.

---

<sup>27</sup> GUTIÉRREZ FRANCÉS, M<sup>a</sup> L. “El intrusismo informático (Hacking):...” (...). Pg. 1163 y ss; postura que parece seguir MATELLANES RODRÍGUEZ, N. “Vías para la tipificación del acceso ilegal...” (...). Pg. 67.

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 a la seguridad de todos los sistemas informáticos, sino un valor de corte netamente individual y de naturaleza claramente informática que solo puede ser protegido frente a los ataques informáticos más graves y más peligrosos que se realicen contra el mismo.

En concreto, considero que nos encontramos ante un delito que debería proteger un nuevo bien jurídico que, pese a tener una naturaleza eminentemente informática, presenta notables similitudes con un bien jurídico tradicional, de naturaleza netamente individual, como es la intimidad.

En tal sentido, considero que este delito debería proteger el derecho a la privacidad informática entendiendo por tal, aquella esfera o parte de la intimidad individual que se concreta en el derecho que toda persona tiene a mantener sus sistemas informáticos y los datos contenidos en los mismos al margen de intromisiones ajenas no deseadas.

Estamos hablando de una suerte de inviolabilidad informática que presentaría notables similitudes con aquella otra inviolabilidad (la del domicilio) que el Derecho penal tradicionalmente ha protegido para garantizar el derecho fundamental a la intimidad y proximidad que puede servirnos de gran ayuda a la hora de valorar y delimitar correctamente el injusto típico que debería castigar este nuevo delito<sup>28</sup>.

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, por sí sola, esa peligrosísima actuación que ha de ser severamente castigada por el ordenamiento penal por el bien de todos y pasa a convertirse en lo que realmente es, una actuación desviada e injusta, pero que tan solo 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 aquellas otras que realmente afectan a la seguridad de los todos los sistemas informáticos.

Por otra parte, y por lo que se refiere a la concreta configuración típica de este delito, hemos de señalar que, dado que lo que en realidad protege es la inviolabilidad de los sistemas informáticos individuales como posibles contenedores de información sensible, debería ser un delito que no tutelase a los sistemas informáticos en sí mismos considerados (el hardware), sino a la información que éstos 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<sup>29</sup>, sino el acceso a los datos o programas en ellos contenidos. No es

---

<sup>28</sup> Ya defendí este concepto extensivo de la intimidad y que le lleva a incluir una nueva faceta hasta el momento no incluida como tal en el mismo en GALÁN MUÑOZ, A. “Ataques contra sistemas informáticos” (...) Pg. 228

<sup>29</sup> 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 nº 18. 2006. Pg. 235,

necesario que los sistemas informáticos contengan informaciones secretas o de carácter personal. Tampoco que el intruso llegue a conocerlos o a entenderlos. Lo que se requiere es que se acceda a algún sistema que contenga algún dato o algún programa, ya que, de lo contrario, el acceso realizado resultaría completa y absolutamente inocuo y debería permanecer en el ámbito de la más absoluta atipicidad.

De hecho, esta concepción parece ajustarse en mucha mejor medida con las propias exigencias del Derecho Internacional, esto es, tanto del art. 2 del Convenio sobre Criminalidad Informática del Consejo de Europa, como del artículo segundo de la Decisión Marco de la Unión sobre Ataques Informáticos; normas ambas en las que se exige que se castigue penalmente el acceso no autorizado tanto a todo o como a una parte del sistema informático; expresión que, a mi modo de ver, pone de manifiesto como lo que se quiere proteger no es tanto el sistema informático como elemento material considerado, como los elementos lógicos en él contenidos, esto es, los datos y los programas informáticos.

Por otra parte, esta concepción tiene otro importante efecto típico, ya que, va a resultar decisiva a la hora de fijar y delimitar qué consentimiento podrá convertir en atípico el acceso realizado.

Cómo fácilmente se puede comprobar, el nuevo artículo 285-A del PCPB convierte a la concurrencia de la autorización del legítimo titular del sistema en causa de exclusión de la tipicidad del acceso ajeno realizado sobre el mismo.

Podría pensarse que nada se puede reprochar a la descripción típica de dicho delito en este concreto aspecto, más allá de su evidente falta de congruencia con el carácter supraindividual que se pretende otorgar a su injusto típico, puesto que, solo si se considera, como aquí se hace, que dicho delito tiene una naturaleza netamente individual y no una colectiva como parece pretender el legislador, 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 plantea un problema mucho más grave que el derivado de esta evidente incongruencia, ya que, parece obligar a entender que cualquier sujeto que utilice un ordenador ajeno para guardar sus datos cometerá la conducta típica de este nuevo delito si trata de acceder posteriormente a dichos datos sin contar con el consentimiento expreso del titular del sistema donde los almacenó, mientras que este sujeto podrá acceder, sin embargo, a dichos datos aunque no contase con el consentimiento de aquel que los creó.

Se llegaría así a la absurda situación de que si contratásemos o utilizásemos un servicio de almacenamiento de datos ajeno con la finalidad de guardar en el mismo cualquier clase de datos que no tuviese la consideración de secretos (p. ej. si alquilamos un ordenador para trabajar con él y guardar el producto de nuestro trabajo o si utilizamos para tal fin el sistema de almacenamiento de la intranet de nuestro lugar de trabajo), solo podríamos acceder a los mismos, a nuestros datos, en la medida en que contásemos con el consentimiento de aquel que nos hubiese suministrado el sistema de almacenamiento, mientras que este sujeto, el

proveedor, podría acceder a ellos siempre que quisiese, incluso contrariando nuestra expresa voluntad en contra.

Esto, evidentemente, carece de todo sentido.

Mucho más lógico es entender que al protegerse la inviolabilidad de los datos o de los programas y no la de los sistemas informáticos que los contienen, solo 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 el acceso realizado en una conducta completamente inocua para el bien jurídico protegido por este delito y, por tanto, en una conducta completamente atípica con respecto al mismo.

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 creo que lo más adecuado sería delimitar el tipo objetivo de este delito aludiendo 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, ello permitirá atender a las concretas circunstancias fácticas y legales que se presenten en cada caso concreto a la hora de determinar si el acceso realizado fue lícito o no<sup>30</sup>.

Por otra parte, también creo que sería conveniente delimitar los accesos típicos de este nuevo delito exigiendo que los mismos tengan que realizarse vulnerando alguna medida de seguridad establecida para impedirlos, posibilidad que aparece expresamente contemplada en los dos textos internacionales anteriormente citados y que, a mi juicio, presenta importantes ventajas, ya que, no solo permite incrementar el desvalor de acción propio del injusto de este delito -con lo que limitará su ámbito de aplicación y legitimará cuando menos en cierta medida su represión penal-, sino que, además, hará factible que se puedan resolver, con una cierta seguridad jurídica, algunos de los casos prácticos más problemáticos de entre 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 solo sobre una parte del mismo.

Evidentemente, 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 en ellos 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 o quienes por el contrario solo pueden acceder a una parte de ellos y tienen vetado el acceso al resto, cuestión que resultará decisiva a la hora de determinar si han cometido un delito 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 se condicione la protección penal de los datos o programas frente a accesos no deseados al establecimiento y a la vulneración de alguna medida de seguridad

<sup>30</sup> GALÁN MUÑOZ, A. "Ataques contra sistemas informáticos" (...). Pg. 229

dirigida a evitarlos, ya que, mientras la exigencia del establecimiento de dicha medida permitirá delimitar de forma segura qué datos no eran accesibles para todos los usuarios del sistema, la referida a la vulneración de dichas medidas por parte del sujeto activo de este delito demostrará que éste conocía perfectamente el carácter no autorizado de su conducta, con lo que facilitara la prueba de su dolo típico<sup>31</sup>.

En cualquier caso, y aún con la restricción comentada, parece imposible negar que este nuevo delito representa una importante extensión expansiva del Derecho penal, ya que, permitirá castigar muchas actividades que antes de su creación eran completamente atípicas. De hecho, la expansión es realmente notable y dará lugar a la apreciación de múltiples concursos de delitos, como los que se tendrán que apreciar cuando a la intromisión informática le siga la realización de cualquier otra actividad delictiva como un delito de daños informáticos, de revelación de secretos, de estelionato, etc...

Sin embargo, esta expansión de la intervención penal no resulta en modo alguna comparable a la que ocasiona el nuevo art. 171 §2º.VII del PCPB; precepto en el que se castiga con la misma pena que al autor de la estelionato consumado al que “*VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:*”.

Fíjese el lector, que el legislador no exige la producción de perjuicio patrimonial alguno. Ni siquiera la idoneidad típica de la conducta para causarlo. Lo único que exige este nuevo tipo para alcanzar la consumación es que se difunda un código malicioso (p. ej. un troyano que funcione como una *Backdoor*) con la finalidad de facilitar el acceso a dispositivos de comunicación, computadoras o redes de los mismos.

Nos encontramos, por tanto, ante la incriminación de una conducta que, a mi modo de ver, podría ser considerada, todo lo más, como constitutiva de una mera tentativa del nuevo delito de acceso no autorizado a sistemas informáticos, cuando no, como un mero acto preparatorio de dicho delito, circunstancia que no ha impedido que el legislador la sancione con la misma pena que al delito de estelionato consumado, lo que nos enfrentará a muchas cuestiones prácticas que van a encontrar una muy difícil respuesta.

Así, por ejemplo, si quien difunde este tipo de códigos maliciosos ha de ser sancionado con la misma pena que al autor del delito de consumado de estelionato, ¿cómo se tendrá que castigar entonces al que no sólo difunde el código en cuestión sino que también lo usa para acceder al sistema? ¿Con la pena de del estelionato consumado como establece el 171 §2º.VII del PCPB? ¿Con la, inferior por cierto, del delito consumado de acceso no autorizado del artículo 285-A, ya que, se tendría que entender que dicho delito absorbería el desvalor completo del injusto castigado por el art. 171 §2º VII PCPB, como el tipo consumado absorbe de forma general al meramente intentado? ¿O se le debería castigar siempre con la pena de ambos delitos?

Pero, ¿y si el sujeto que difunde el código malicioso no accede los sistemas en el que éste se encuentra, sino que se limita a facilitar dolosamente que otro lo haga para cometer un delito? ¿Responderá solo por el delito del art. 171 §2º VII PCPB? ¿O tendrá que hacerlo

---

<sup>31</sup> Sobre esta cuestión véase con mayor extensión GALÁN MUÑOZ, A. “Ataques contra sistemas informáticos” (...). Pg.229 y ss

también como participe en el delito de acceso no autorizado o de estelionato que dicho sujeto habría cometido como verdadero autor?

El despropósito punitivo es absoluto.

No es solo un problema de ubicación sistemática, el que se esconde tras la creación de este nuevo delito. En realidad, su creación pone en tela de juicio las reglas más básicas delimitadoras de los concursos, de la tentativa y de la consumación o de la autoría y de la participación, con lo que hace que la propia Teoría General del Delito deje de funcionar en este concreto ámbito como el sistema proporcional de imputación de responsabilidad penal que debería ser.

Ante un problema de esta magnitud considero que lo mejor sería derogar este precepto aún antes de que entre en vigor, ya que, a mi modo de ver, solo haciéndolo se podrá evitar que el proceso de expansión e intensificación que caracteriza al Derecho penal informático y a todo el “Moderno Derecho penal” en general, entre de lleno en el Derecho penal informático brasileño ocasionando algunas de las numerosas incongruencias punitivas a las que desgraciadamente nos tiene tan acostumbrados en España<sup>32</sup>.

#### ***4. El siempre difícil papel de los proveedores de Servicios en la investigación y persecución de los delitos informáticos***

Uno de los temas que más debates prácticos y doctrinales está generando en Europa con respecto a la criminalidad informática, es precisamente el referido al papel que están llamados a desempeñar los proveedores de servicios de Internet tanto en la investigación, como, incluso, en la comisión de aquellos delitos que se realizan a través de la red; tema que, como no podía ser de otro modo, también ha sido abordado por la reforma proyectada del Derecho penal brasileño.

En concreto, el texto del proyecto establece en su artículo 22 que:

*“O responsável pelo provimento de acesso a rede de computadores é obrigado a:*

*I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e por esta gerados, e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;*

*II – preservar imediatamente, após requisição judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações requisitadas por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;*

*III – informar, de maneira sigilosa, à autoridade competente, denúncia da qual tenha tomado conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.*

<sup>32</sup> Sobre este fenómeno, véase GALÁN MUÑOZ, A. “Expansión e intensificación...” (...). Pg. 22 y ss

*§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.*

*§ 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R\$ 2.000,00 (dois mil reais) a R\$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.*

*§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001”.*

Como fácilmente se puede comprobar, el citado precepto no obliga al proveedor a vigilar o a controlar los contenidos que ayuda a difundir; exigencia que vendría, a mi juicio, 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 si hace es obligarle a informarle de manera sigilosa a la autoridad competente de la comisión de los delitos que tuviese conocimiento, -obligación que, en el ordenamiento jurídico penal español es predicable, si bien de forma limitada, respecto a cualquier sujeto y no sólo con respecto al proveedor (art. 450.2 CPE)- y sobretodo, exigirle que recolecte, almacene y custodie una serie de datos referidos a las comunicaciones ajenas que ayude a realizar, ordenándole que suministre dichos datos a las autoridades encargadas de una investigación cuando ello le sea requerido judicialmente.

El objetivo de esta medida es evidente. Se trata de implantar un sistema de “trazabilidad legal”<sup>33</sup>, 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. estelionatos, daños, difusión de pornografía infantil, etc...) deban quedar necesariamente impunes.

En concreto, se trata de establecer un sistema que permita identificar al usuario que hubiese realizado dichas conductas una vez que se hubiese constatado su realización, tarea que sólo se podrá llevar a cabo con total seguridad si los proveedores de servicios mantienen almacenados, por lo menos durante un tiempo, aquellos datos que permitirían localizar a quien las realizó o cuando menos el terminal de la red desde el que lo hizo.

Ahora bien, dado el marcado carácter transnacional de la red, tampoco resultará posible identificar y perseguir a los autores de estas conductas si no existen o se crean instrumentos de cooperación internacional que permitan a las autoridades investigadoras de un país acceder a los datos almacenados por los proveedores afincados en otro o si éstos no

<sup>33</sup> Así lo denomina, acertadamente a mi juicio, LÓPEZ ORTEGA, J. J. “La admisibilidad de los medios de investigación ...” (...). Pg. 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. Pg. 211

están obligados a conservarlos conforme a lo establecido por la legislación vigente en el país en que se encuentren, lo que pone nuevamente de manifiesto lo importante que resulta la armonización y la colaboración internacional en materia de criminalidad informática.

No debe sorprender, por tanto, que muchos de los instrumentos internacionales que se han ocupado de los diversos aspectos relativos a la criminalidad informática se hayan ocupado especialmente de regular esta materia<sup>34</sup>.

Así, por ejemplo, y por citar de nuevo algunos con significativa importancia en la realidad legislativa europea actual, podemos destacar, de nuevo, los preceptos contenidos en los artículos 14 y siguientes de la Convención del Consejo de Europa sobre Delincuencia Informática, hecha en Budapest el 23 de noviembre de 2001, o los muy diversos y variados instrumentos normativos desarrollados por la Unión Europea con incidencia en esta materia, como serían, entre otros, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 15 de marzo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la Privacidad y las Comunicaciones electrónicas) y, sobretodo, la Directiva 2006/24/CE, de 12 de Julio, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso o de redes públicas de comunicaciones; directiva ésta que dio lugar a la aparición de la vigente Ley 25/2007, de 18 de octubre, conservación de datos relativos a las comunicaciones que transpuso su contenido al ordenamiento español, y modificó algunos artículos importantes de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Todos estos instrumentos internacionales tratan de proteger el anonimato de las comunicaciones cibernéticas como nueva manifestación del concepto de intimidad, cuando menos de una forma limitada y temporal, y para conseguirlo articulan sistemas de trazabilidad legal que al mismo tiempo que obligan a los proveedores de sus países firmantes a conservar ciertos datos referidos a las comunicaciones ajenas que ayuden a realizar, también les exige que custodien dichos datos y que mantengan la confidencialidad respecto a los mismos, debiendo entregarlos y revelarlos tan solo cuando así les fuesen exigido por una autoridad judicial.

Esta parece ser la práctica más conforme a las exigencias de un Estado democrático y no la establecida 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 no se garantiza ni se respeta el derecho a la intimidad y al secreto de las comunicaciones de sus usuarios.

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.

---

<sup>34</sup> 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. Pg. 181

En España, los importantes cambios legislativos realizados por las ya citadas leyes 32/2003, General de Telecomunicaciones y 25/2007, de conservación de datos relativos a las comunicaciones, han venido a regular 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 regula y definen los datos que los proveedores han de almacenar, el periodo por el que han de hacerlo, cómo y cuándo pueden y deben cederlos, cómo se deben protegerlos de accesos no autorizados (art. 3, 5, 7 y 8 respectivamente de la ley 25/2007) y también, como no podía ser de otra forma, se fijan qué acciones están obligados a adoptar para garantizar la interceptación de telecomunicaciones y las identificaciones que les pudiese requerir una autoridad judicial (art. 33 Ley 32/2003).

Sin embargo, estas reformas legislativas no han encontrado el reflejo que era de esperar en las normas procesales que rigen cuándo, cómo y en qué medida se puede solicitar a dichos intermediarios de la red que efectúen dichas interceptaciones o que comuniquen dichos datos.

En efecto, la implantación de las nuevas tecnologías y el desarrollo de una enorme e importante normativa referida a su regulación no han tenido efecto alguno en la regulación procesal de la investigación penal en España.

Los enormes avances tecnológicos, la gran variedad de novedosas técnicas de comunicación no han provocado cambio alguno de la Ley de Enjuiciamiento Criminal española, lo que ha ocasionado que los juristas 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, o cuándo y de qué forma se pueden, cuando menos, monitorizar los movimientos que los usuarios realizan en dicha red.

Así, por ejemplo, nos encontrábamos con el despropósito de que los Tribunales españoles ni siquiera saben con certeza cuál es el correcto procedimiento que se debería 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 entienden que lo correcto sería utilizar el cauce procesal previsto en el segundo apartado de dicho artículo, referido a la interceptación de las comunicaciones telefónicas<sup>35</sup>.

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<sup>36</sup>.

<sup>35</sup> Sobre este tema véase, 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. Pg. 314 y ss

<sup>36</sup> Así lo consideraban algunos como señala LÓPEZ ORTEGA, J. J. "La admisibilidad de los medios de investigación ..." (...). Pg. 95

Pese al incomprensible e inadmisiblesilencio 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 solo las comunicaciones postales, telegráficas o telefónicas tradicionales, sino también a aquellas otras que se realicen por cualquiera de los modernos medios informáticos<sup>37</sup>, lo que ha llevado a que se proyecte el estatuto jurídico de dicho derecho fundamental a las comunicaciones realizadas, por ejemplo, por correo electrónico<sup>38</sup>.

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, por ejemplo, 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?<sup>39</sup>

Las cuestiones parecen no tener fin y, sin embargo, no encuentran ninguna respuesta cierta ni el ámbito legislativo nacional ni, lo que todavía es más preocupante, 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 de los Derechos y de las persecuciones penales nacionales. También puede y debería llevar a que estableciesen unos estándares de garantías mínimos comunes a todos los ordenamientos nacionales, lo que daría lugar a una verdadera armonización restrictiva de muchas de dichas legislaciones.

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 derecho a la intimidad y al secreto de las comunicaciones.

<sup>37</sup> 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. Publicacions Universitat Jaume I, 1997. Pg. 410.

<sup>38</sup> MORALES PRATS, F. "La investigación del cibercrimen (II)". IURIS nº 102, 2006. Pg. 35

<sup>39</sup> Sobre este tema y la, a mi juicio tan solo aparente habilitación que otorga el art. 20 ET a tales efectos, véase GARCÍA GONZÁLEZ, J. "Intervenciones de terceros en el correo electrónico..." (...). Pg 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.". En "Derecho a la dignidad e intimidad del trabajador", en [www.iustel.com](http://www.iustel.com) (ult. vis. 10-8-2008)

Pese a todo, como también sucede con el reconocimiento constitucional de tales derechos a nivel nacional, las mencionadas convenciones internacionales se limitan a hacer unas referencias muy genéricas a dichos derechos, lo que las convierte en unos referentes importantes, pero no completamente precisos y eficaces a la hora de responder a todas las preguntas que plantea el imparable avance y expansión de las telecomunicaciones.

Mucho más útil resulta, sin embargo, el desarrollo y la interpretación que los Tribunales internacionales han realizado de las mismas a la hora de controlar su respeto por parte de los Estados que las han ratificado.

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 al controlar 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 ingerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta ingerencia 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 español y europeo 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 de este Tribunal que han tenido incidencia sobre 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 v. El 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 la privacidad, con lo que su policía podría efectuarlas sin ningún control o autorización; mientras que, por otra parte y al mismo tiempo, 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 a un determinado sujeto, 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 la “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 establecida a este respecto. 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, lo que permite que este Tribunal pueda entrar a valorar y a enjuiciar si las concretas normativas nacionales de los Estados firmantes de la Convención las respetan o no.

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 no solo no puede regularse esta materia en una norma o ley secreta, sino que además ha de hacerse en una ley que sea lo suficientemente clara 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, ya que, como afirma el propio Tribunal “*una ley que concede discreción debe indicar el ámbito de esa discreción*”; aunque esto no quiere decir que todos los ciudadanos deban poder prever siempre y con todo detalle cuando 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. 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 -como expresamente afirmaba el juez *Pittiti* en su opinión particular concordante con la Sentencia-, obligará a que la adopción y la proporcionalidad de dichas interceptaciones siempre deba ser judicialmente controlada<sup>40</sup>.

<sup>40</sup> 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. Pg. 180 y ss

Ahora bien, si esta sentencia es conocida y ha tenido un enorme impacto en la regulación que nos ocupa ha sido por la solución que dio al segundo de los problemas planteados por los representantes del Reino Unido, esto es, aquel que cuestionaba si el mero “*metering*” era una actividad que realmente afectase al secreto de las comunicaciones y que tuviese cumplir, por tanto, con los mismos requisitos que cualquier otra conducta limitadora de dicho derecho fundamental; cuestión a la que el Tribunal respondió de forma nuevamente afirmativa, señalando 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 artículo 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<sup>41</sup>, 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 necesariamente de la autorización judicial motivada que expresamente exige el art. 18.3 de la Constitución Española para interceptar las comunicaciones de cualquier sujeto<sup>42</sup>, postura jurisprudencial que parecía obligar a extender dicha garantía también 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 (IP, fecha y hora de conexión, duración etc...).

Así lo entendió parte de la doctrina española<sup>43</sup>, encontrando un respaldo notable, a mi modo de ver, tanto en algunas de las más recientes resoluciones del Tribunal Europeo de Derechos Humanos<sup>44</sup>, como en los propios textos de las reformas legislativas españolas, (p. ej. art. 7.2. Ley 25/2007 y art. 33 de la Ley 32/2003); textos que, al igual que el brasileño, condicionan la entrega de estos datos por parte de los proveedores que tienen que

---

<sup>41</sup> 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 solo los datos relativos al contenido de lo transmitido están amparados por la protección que otorga dicho derecho. *Delincuencia informática y Derecho penal* (...). Pg. 164

<sup>42</sup> 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 nº 7086, 2009. [www.diarialaley.laley.es](http://www.diarialaley.laley.es) (ult. vis. 8-1-2009)

<sup>43</sup> 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” (...). Pg. 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” en *El cibercrimen: nuevos retos jurídico-penales nuevas respuestas político-criminales*. Ed. Comares. Granada, 2006. Pg. 272

<sup>44</sup> 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 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)

almacenarlos, 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 están obligados a entregarlos.

Parecía, por tanto, que al fin una de las cuestiones planteadas respecto a las garantías jurídicas que se habían de dar al anonimato de las comunicaciones electrónicas 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 del conocido programa de intercambio 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 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.

Así pues, 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, son revelados y publicados voluntariamente por su propio titular (el usuario de la red) desde el mismo momento en que se conecta a Internet; 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 un IP que puede ser fácil y públicamente conocido?

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, en la mayoría de los casos, cómo funciona realmente dicha red ni los datos y señales que va dejando al utilizarla. Hablar en estos casos de un verdadero consentimiento del usuario no es más que una pura ficción<sup>45</sup>.

Pero no, también y sobretodo, porque esta afirmación supone desconocer el verdadero fundamento que llevó al Tribunal Europeo de Derechos humanos a afirmar en reiteradas ocasiones que esta clase de datos están amparados por el derecho fundamental al secreto de las telecomunicaciones.

Si se analizan las Sentencias emitidas por el citado Tribunal desde el caso *Malone*, nos 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, 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 todos sus ciudadanos conociendo simplemente qué prensa 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!

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 recordarán, en no pocos aspectos y de forma alarmante, a los que se describían en el “*Big Brother*” Orweliano.

---

<sup>45</sup> En este sentido consideramos mucho más acertada la consideración realidad por LÓPEZ ORTEGA, J. J. que afirmaba 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 ...” (...). Pg. 95. En contra de esta postura y a favor de la apreciación del consentimiento del usuario, se ha manifestado, sin embargo, recientemente, RODRÍGUEZ LAINZ, J. L. “Dirección IP; IMSI e intervención judicial...” (...), postura que no podemos compartir por los motivos comentados.

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 controlada, 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<sup>46</sup> y es por ello, por lo que considero que su uso siempre debería ser controlado y autorizado por un órgano judicial independiente que compruebe, no solo que su utilización inicial es necesaria y está justificada, sino también que se emplea de una forma adecuada y proporcionada a los fines que justificaron su uso inicial <sup>47</sup>.

## 5. Conclusiones

De lo expuesto hasta el momento se deduce que el fenómeno informático representa sin lugar a dudas uno de los mayores retos a los que se enfrenta no solo del Derecho penal brasileño o 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.

Vivimos, como bien afirma BECK, en una “Sociedad del Riesgo mundial”<sup>48</sup> y eso hace que el Derecho penal necesite de la colaboración internacional para poder hacer frente a los retos que dicha 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 una forma muy similar, problemas penales muy similares.

Esto mismo es lo que ha hecho Brasil, con su proyecto de reforma. Una reforma en la que se pueden encontrar tanto luces como sombras, pero que refleja de modo ejemplar la tesitura en la que se encuentra el Derecho penal actual.

En este proyecto se contienen soluciones normativas perfectamente proporcionadas y adecuadas (como las referidas a la regulación de los daños informáticos). Otras que bajo la apariencia del adelantamiento de la protección penal esconden, en realidad, la semilla de su intensificación (como sucede con respecto a los supuestos de difusión de Códigos maliciosos). Y también, como no podía ser de otro modo, algunas que se insertan y son claros ejemplos de

---

<sup>46</sup> ROMEO CASABONA, C. señala que este concepto, el de privacidad, resulta más amplio y global que el de intimidad que lude a facetas de la personalidad que asiladamente 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” (...). Pg. 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.

<sup>47</sup> 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” (...). Pg. 411 y ss, MATA Y MARTÍN, R. M. *Delincuencia informática* (...) Pg. 159 y ss, GARCÍA GONZÁLEZ, J. “Intervenciones de terceros en el correo electrónico...” (...). Pg. 316 y ss

<sup>48</sup> BECK, U. *¿Qué es la globalización?* (...). Pg. 87 y ss y 190 y ss

ese “Moderno Derecho penal” que pone en cuestión los más esenciales principios de la Teoría General del delito como sistema democrático y proporcionado de imputación de responsabilidad penal, como sucede, a mi juicio, en el delito de difusión de código malicioso que facilita el acceso no autorizado a sistemas informáticos ajenos.

Delitos y problemas semejantes a los que plantea este último delito se pueden encontrar en muchos de los ordenamientos jurídicos europeos, incluido en el español, actuando, a mi juicio, la imparable creación y transposición de normas internacionales armonizadoras relativas a la criminalidad informática como un elemento determinante de su proliferación.

De hecho, si por algo se caracteriza el proceso internacional armonizador que se está produciendo en el ámbito del denominado Derecho penal informático, como visto a lo largo de este trabajo, es por el hecho de que está actuando como factor multiplicador del proceso expansivo que vive el Derecho penal Moderno en general<sup>49</sup>, sin que, sin embargo, esté generando una paralela extensión de las garantías y derechos de que deberían limitar a este Derecho.

Se podría decir, por tanto, sin demasiado temor a equivocarnos que en este concreto ámbito, en el del Derecho penal informático internacional, el binomio prevención-represión está venciendo de nuevo a aquel otro que se conforma por la unión de garantías y libertades<sup>50</sup>.

Así lo demuestra a mi modo de ver, por ejemplo, la regulación internacional referida al papel que los proveedores están llamados a desempeñar en esta aldea global en que vivimos. Una regulación que se ha preocupado muy mucho de obligarles a almacenar y a entregar a las autoridades una serie de datos referidos a las comunicaciones de sus clientes, pero que, sin embargo, no ha creado ni se ha preocupado de definir con la misma precisión los instrumentos procesales mínimos que deberían protegernos de los posibles abusos que podrían cometer los principales usuarios de dichos datos, los Cuerpos y Fuerzas de Seguridad del Estado.

Este es el Derecho penal informático que estamos creando. Un Derecho penal que protege nuestra privacidad de las casi míticas o incluso imaginarias agresiones que pueden efectuarle personas, casi legendarias, como los “temibles” *Hackers*, pero que nos deja, sin embargo, completamente indefensos frente a las mucho más reales y posibles lesiones que puede ocasionar a dicho bien jurídico aquellos sujetos que, si bien tienen el deber de protegerlo, en ocasiones, y esto no lo podemos ni debemos olvidar nunca, pueden ser quienes mayores daños le pueden ocasionar<sup>51</sup>.

<sup>49</sup> Este efecto 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 (...)* Pg. 83

<sup>50</sup> 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 otean perspectivas de futuro garantistas par ala intimidad del ciudadano*" "La investigación del delito..." (...) Pg. 36

<sup>51</sup> 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 -véase sobre este tema véase lo comentado por GARCÍA GONZÁLEZ, J. "Intervenciones de terceros en el correo electrónico..." (...). Pg. 314 quien se cuestiona si resultaría aplicable el delito del art. 534 (registro

Todo ello se hace y se acepta en aras a conseguir esa sacrosanta sensación de seguridad que los ciudadanos de las modernas sociedades postindustriales parecen querer conseguir aunque sea a costa de perder gran parte de sus libertades y derechos.

Sin embargo, y frente a ello, no deberíamos olvidar nunca que no resulta posible crear un verdadero Derecho penal protector del ciudadano que no lo proteja, en primer lugar e incluso de forma preferente, del propio Derecho penal.

Esto no solo es una mera cuestión de principios, sino también una cuestión práctica o funcional, ya que, como afirma DÄUBLER-GMELIN, “... *conculcar derechos fundamentales tal y como representa, por ejemplo, adoptar medidas de vigilancia acústica y óptica en la esfera privada, comporta graves perjuicios al derecho estatal y a la libertad ciudadana, reduce la capacidad de actuación y en cambio no combate eficazmente la delincuencia ni contribuye a mejorar la seguridad de los ciudadanos. Es una cuestión de tiempo llegar a destruir esa ilusión de seguridad, lo cual contribuirá a la pérdida de confianza en el orden democráticamente legitimado*”<sup>52</sup>. Esperemos que podamos cambiar esta dinámica político-criminal antes de que llegue ese momento.

## BIBLIOGRAFÍA

BECK, U.

-¿Qué es la globalización? Ed. Paidós, Barcelona, 2008

CORCOY BIDASOLO, M.

-“Protección penal del sabotaje informático. Especial consideración de los delitos de daños”. La Ley, nº 2400. 1990.

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, nº 15, 2006-1.

---

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* v. Reino Unido, la monitorización o el *metering* es algo distinto de la interceptación, conducta ésta que es la única que se castigan en los art. 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.

<sup>52</sup> DÄUBLER-GMELIN, h. “Globalisierung keineswegs Hand in Hand mit globalem Recht”, en Frankfurter Rundschau, nº 90, (18 de abril de 1997), citada por BECK, U. ¿Qué es la globalización? (...). Pg. 252

-“El nuevo delito del artículo 248.3 CP: ¿un adelantamiento desmedido de las barreras de protección penal del patrimonio?” La Ley nº 3 2004.

-“*Ataques contra sistemas informáticos*”. En Boletín de información del Ministerio de Justicia,. Año 60, Nº 2015, 2006

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.

GONZÁLEZ RUS, J. J.

-“Los ilícitos en la red (I): Hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes”, en *El cibercrimen: nuevos retos jurídico-penales nuevas respuestas político-criminales*. Ed. Comares. Granada, 2006.

GONZÁLEZ RUS, J. J.

-“Protección penal de sistemas, elementos, datos, documentos y programas informáticos”, RECPC 01-14 (1999), en [http://criminet.ugr.es/recpc/recpc\\_01-14.html#1.DAÑ](http://criminet.ugr.es/recpc/recpc_01-14.html#1.DAÑ) (Ult. vis. 1-8-2008).

GOÑI SEIN, J. L

-“Derecho a la dignidad e intimidad del trabajador”, en [www.iustel.com](http://www.iustel.com) (ult. vis. 10-8-2008)

GRACIA MARTÍN, L.

-“Prolegómenos para la lucha por la modernización y expansión del Derecho Penal y para la crítica del discurso de resistencia”. Ed. Tirant lo Blanch. Valencia, 2003.

GUTIÉRREZ FRANCÉS, M<sup>a</sup> L.

-“El intrusismo informático (Hacking): ¿represión penal autónoma?”. *Informática y derecho: Revista iberoamericana de derecho informático*, nº 12-15, 1996

HASSEMER, W.

-*Persona, Mundo responsabilidad. Bases para una teoría de la imputación*. Valencia, 1999.

LÓPEZ ORTEGA, J. J.

-“Libertad de expresión y responsabilidad por los contenidos en Internet” en *Internet y Derecho Penal*. Cuadernos de Derecho Judicial X. Ed. CGPJ. Madrid, 2001.

-“La admisibilidad de los medios de investigación basados en registros informáticos”, en *Delincuencia informática. Problemas de responsabilidad*. Cuadernos de Derecho Judicial IX, 2002.

MATA Y MARTÍN. R. M.

-*Delincuencia informática y Derecho penal*. Ed. Edisofer. Madrid, 2001.

-“La protección penal de datos como tutela de la intimidad de las personas y las nuevas tecnologías”. *Revista Penal* nº 18. 2006.

MATELLANES RODRÍGUEZ, N,

-“Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)”. *Revista Penal*, nº 22, 2008.

MEYER-LADEWIG, J.

-*Europäische Menschenrechts-Kovention. Handkommentar*. V. Nomos, Baden-Baden, 2006.

MORALES PRATS, F.

-“La investigación del ciberdelito (II)”. *IURIS* nº 102, 2006.

-“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.

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. Publicacions Universitat Jaume I, 1997.

MORÓN LERMA, E.

-*Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*. Ed. Aranzadi. Pamplona, 2002.

MUÑOZ MACHADO, S.

-*La regulación de la red: Poder y Derecho en la red*. Ed. Taurus. Madrid, 2000.

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.

RODRÍGUEZ MOURULLO, G./ ALONSO GALLO, J. / LASCURAÍN SÁNCHEZ, J. A.

-“Derecho penal e Internet” en Régimen jurídico de Internet. Ed. LA Ley, Madrid, 2002.

RODRÍGUEZ LAINZ, J. L.

-“Dirección IP; IMSI e intervención judicial de comunicaciones electrónicas” en LA LEY nº 7086, 2009. [www.diariolaley.laley.es](http://www.diariolaley.laley.es) (ult. vis. 8-1-2009)

ROMEIO CASABONA, C.

-“Los datos de carácter personal como bienes jurídicos penalmente protegidos” en *El cibercrimen: nuevos retos jurídico-penales nuevas respuestas político-criminales*. Ed. Comares. Granada, 2006.

SIEBER, U.

-“Límites del Derecho Penal”. *Revista Penal*, nº 22, 2008.

SILVA SÁNCHEZ, J. M.

-“La expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales”. Ed. Civitas. 2ª Ed. Madrid, 2001.

VOGEL, J.

-“La internacionalización del Derecho penal”. *Revista Penal*, nº 22, 2008.