DÍAZ GÓMEZ, A., «El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest », *REDUR* 8, diciembre 2010, págs. 169-203. ISSN 1695-078X

# EL DELITO INFORMÁTICO, SU PROBLEMÁTICA Y LA COOPERACIÓN INTERNACIONAL COMO PARADIGMA DE SU SOLUCIÓN: EL CONVENIO DE BUDAPEST

Andrés DÍAZ GÓMEZ

ESTUDIANTE DE DOCTORADO
UNIVERSIDAD DE LA RIOJA



**RESUMEN:** La globalización y las transformaciones económicas que la explican han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos e Internet. Las peculiaridades de estos nuevos tipos exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra a elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales. Mediante esta técnica es posible lograr una armonización del Derecho sustantivo, así como en el ámbito procesal, que redunda definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales. Para lograrlo, la cooperación internacional, que se materializa principalmente a través de convenios internacionales, deberá reunir unos requisitos mínimos cualitativos. El Convenio sobre la Cibercriminalidad del Consejo de Europa se presenta como la única solución internacional existente para el tratamiento de la cuestión ciberdelictual. A pesar de sus deficiencias, se convierte en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito.

**ABSTRACT:** Globalization and economic transformations have made possible the development and mass-production of the new information technologies. Together with this, technological development has given rise to new ways of committing crime related to computer systems and internet. These new types of crime demand a joint, uniform and coherent treatment. Similarly, their specific problems involve transnational elements which require international cooperation. In this way it will be possible to achieve a harmonization of sub stantive law and also a harmonization at the procedural level resulting finally in a solution to the uncertainty surrounding cybercrime. To be successful, international cooperation will need to have certain qualitative requirements. The Convention on Cybercrime of the Council of Europe is the only international solution that exists for the treatment of cybercrime. In spite of its faults, it has become an adequate tool for legislative harmonization and the fight against cybercrime.

**PALABRAS CLAVE:** Cibercriminalidad, delitos informáticos, cooperación internacional, Convenio sobre la Cibercriminalidad del Consejo de Europa

**KEY WORDS:** Cybercrime, international cooperation, Convention on Cybercrime of the Council of Europe

## I. Hacia un mundo interconectado

El proceso de integración cultural, económica y social a nivel mundial, conocido popularmente como globalización, alcanza su punto álgido en nuestros días. Este fenómeno, surgido de las postrimerías de la guerra fría, arrastra tras de sí una innumerable cantidad de logros y desavenencias. Como principal beneficio, la creación de riqueza y mejora de las condiciones de vida. Como inconveniente primero, el proceso contrario: la ampliación de la brecha de la pobreza. La caí4da del muro de Berlín y los acontecimientos del mismo cariz coetáneos, cambiarían para siempre nuestra forma de ver el mundo. La división del globo este-oeste (comunismo-capitalismo), dejaría paso a otra bien distinta: norte-sur (riqueza-pobreza). El capitalismo se ha impuesto sin ya apenas oposición, y con él todos sus efectos secundarios. Los positivos y negativos.

También posee la facultad indudable de la homogeneización. Progresivamente se unifican no sólo los mercados, sino también culturas, sociedades. La religión y las costumbres se han totalizado, las democracias consolidado y los movimientos intercontinentales (personas, capitales y mercaderías) masificado. La mayor libertad de empresa es una realidad, la era del consumismo es un hecho.

Pero no es momento de analizar ideológicamente un fenómeno como éste, ni hacer disertaciones propias de un libro de filosofía. Tampoco creo que la exposición que antecede haya sido en vano, su significación reside en la importancia de la globalización para explicar el fenómeno de evolución tecnológica. Ello porque, no olvidemos, la globalización apunta a la modernización. Así, en este momento, cuando nos referimos a modernización, queremos aludir a la de tipo técnico o tecnológico, especialmente en lo relacionado con el transporte y las comunicaciones.

En efecto, la revolución en este sector ha sido tal que ha cambiado la forma del hombre de relacionarse con el mundo y las personas que le rodean. Un cambio tan grande que nadie hubiera podido preverlo jamás. No en vano, el acontecimiento ha sido llamado por algunos como «Tercera Revolución Industrial » o incluso «Revolución de la Inteligencia», haciendo uso ésta última, a mi juicio, de vocablos totalmente inapropiados para su denominación.

Es la aparición de las llamadas TIC's (Tecnologías de la Información y Comunicación) pero sobretodo, su masificación, el elemento que mejor define la nueva era que nos ha tocado vivir. Lo cierto es que esta tecnología representa, desde mi punto de vista, un salto cualitativo mayor aún que el descubrimiento de la electricidad.

Técnicamente, se consideran Tecnologías de la Información y Comunicación tanto al conjunto de herramientas relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de información, como al conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software)[1]. Se trata de instrumentos que nos permiten estar informados prácticamente al instante de lo que ocurre en el mundo, comunicarnos en menos de un segundo con cualquier persona de La Tierra. Por eso ahora pueden comprenderse mis palabras anteriores relacionadas con la monumental evolución que esto ha supuesto.

Dichas tecnologías aparecen plasmadas en distintos soportes físicos que todos conocemos, como son el teléfono –fijo y móvil-, el ordenador, la televisión, etc. Todos ellos continúan desarrollándose y evolucionando día a día, llegando incluso a mezclarse, y apareciendo híbridos de éstos. Como sabemos, es gracias a dispositivos como los enunciados que pueden crearse las redes, que son un conjunto de equipos informáticos

[1] http://www.recursoseees.uji.es/fichas/fc10.pdf

conectados entre sí que pueden intercambiar información[2]. Ante esta perspectiva, cualquier tipo de comunicación tradicional queda empequeñecido ante las vastas oportunidades ofrecidas por la nueva tecnología.

Pero si algo ha revolucionado la sociedad es Internet, gran invento del siglo XX y símbolo de la época actual. Internet ha facilitado las relaciones sociales, y en general toda comunicación e intercambio de información. Pero aún más; ha alterado de manera decisiva e irreversible nuestro modo de vivir y acercarnos a los demás.

Muchas de las actividades que hace unos años realizábamos con normalidad, como comprar o charlar, han dado un vuelco completo con la aparición de Internet. Además han aparecido nuevas formas de ocio, trabajo, comercio, publicidad, relaciones interpersonales y con la Administración... caracterizadas por el aumento de la facilidad y la rapidez, así como la realización de éstas a distancia.

Por otro lado, las estadísticas arrojan un imparable y progresivo crecimiento de las personas que acceden habitualmente a Internet año tras año[3]. Esto sin duda prueba su consolidación como elemento comunicativo, comercial o de ocio. Así las cosas, queda claro que Internet se ha convertido en un pilar fundamental de nuestras vidas, al menos en los países desarrollados. Desde realizar una transferencia bancaria a conversar con otra persona a 20.000 kilómetros de distancia, todo ello lo hace posible Internet y las nuevas tecnologías que la acompañan. Desde esta perspectiva, hasta tal punto estamos imbuidos en el mencionado contexto, que incluso desde algunos sectores se empieza a hablar de Internet como una verdadera necesidad fisiológica, más allá de las adicciones que pueda llegar a generar.

En los últimos años Internet ha sido objeto de análisis en numerosas publicaciones, tal es el interés que despierta. Uno de los más exhaustivos estudios describe con exactitud las características propias de este fenómeno, a saber: no hay fronteras reales, el lugar físico pasa a un segundo plano, multiculturalidad y «multilenguaje», comunicación «uno para muchos», facilidad de difusión de información, continuo crecimiento, portabilidad, falta de identificadores seguros e inexistencia de una autoridad real que la controle[4]. Este trabajo no tiene por misión el análisis de Internet, así que no nos detendremos en la observación particular de los presupuestos enunciados; baste decir que todos los factores enumerados servirán para encauzar la posterior argumentación de la ciberdelincuencia.

Internet es causa y a la vez consecuencia de la globalización. El surgimiento de la Red de Redes sólo era posible en una sociedad como la actual, de pensamiento global y tendente a la uniformidad, e igualmente su aparición acelera sin duda el proceso de homogeneización mundial. Desde nuestro punto de vista, Internet es el hijo predilecto de la globalización y a su vez garantía de la continuidad de ésta. En este sentido, mientras que la conveniencia de la globalización aún se discute, Internet prácticamente se ha consolidado como algo beneficioso y absolutamente necesario para la vida. Paradójicamente, incluso los grupos más reaccionarios (conocidos como «movimientos antiglobalización») utilizan

[2] REAL ACADEMIA ESPAÑOLA, *Diccionario de la Lengua Española*, Espasa Calpe, Madrid, 2001 (22ª edición).

[3] En España, según el último Estudio General de Medios (AIMC) la penetración a día de hoy –abril 2010- ha alcanzado un 35%. La evolución es la siguiente: 2000-5.6%; 2001-9%; 2002-10.6%; 2003-13.6%; 2004-16.8%; 2005-19.7%; 2006-22.2%; 2007-26.2%; 2008-29.9%; 2009-34.3%.

[4] *BÖRGE SVANTESSONS, D.J,* «The characteristics making Internet communication challenge traditional models of regulation», en *International Journal of Law and Information Technology*, vol. 13, nº 1, págs. 40-51, 2005 (en inglés). En la primera parte de su obra, el autor analiza desde el punto de vista jurídico las características esenciales de Internet, que permiten diferenciarla de otras formas de comunicación.

Internet como plataforma principal en pro de sus intereses combativos, como ha puesto de manifiesto López Martín[5].

## II. La globalización de la delincuencia

Hasta ahora se ha hablado de la revolución que ha supuesto Internet en todos los ámbitos de la vida humana, dentro del marco dinámico que es la globalización. Ahora trataremos de enmarcar este asunto dentro del tema que atañe a este trabajo: la criminalidad. En efecto, a lo largo del segundo y tercer capítulos se concretarán algunos de los aspectos concernientes a la criminalidad en la red.

Debemos tener en cuenta que si es cierto, como dijimos, que la red proporciona infinidad de posibilidades a las personas para desenvolverse en sus quehaceres cotidianos, también será cierto que suministrará igual cantidad de ocasiones para infringir la ley. Las oportunidades son para todos. No podemos ser ingenuos y pensar que las enormes utilidades, de diverso tipo, dejadas al descubierto por la nueva era informática no serán utilizadas también para aprovecharse ilegítimamente de los demás.

Dijimos que, existiendo el ocio convencional, surge con Internet uno distinto, virtual; si existía el comercio tradicional, surge también uno nuevo a través de la red, etc. Pues bien, si existía una delincuencia «tradicional», llámese como se quiera, surgirá a partir de ahora una nueva delincuencia alrededor de la Red. Y ésta es la realidad a la que debe hacer frente el Derecho, para la cual no sirven las herramientas tradicionales, como diremos en el capítulo siguiente. De este modo, desde nuestro punto de vista no se trata de que la aparición y posterior desarrollo de Internet haya facilitado la comisión de determinados delitos, como argumentan algunos autores, sino que tan sólo se han abierto nuevos caminos antes inexistentes. Prueba de ello es que no sólo han aparecido nuevas modalidades de los tipos penales tradicionales (como estafa informática), sino que también han aparecido nuevos delitos que antes era inconcebibles (daños informáticos). No es momento de detenerse en la variada tipología delictual que presentan, pues no es ese el objetivo de este trabajo.

La situación es más peliaguda de lo que pudiera parecer en un principio. Si bien es verdad que los delitos informáticos son seriamente castigados en la actualidad y que aumentan progresivamente los medios policiales para la investigación, los llamados «ciberdelincuentes» van siempre un paso (o varios) por delante de las autoridades encargados de perseguirlos. Pero no sólo esto; además el número de delitos informáticos aumenta año tras año a un ritmo vertiginoso, mucho más que el de usuarios nuevos que se conectan a Internet. La mayor parte de los ataques provienen de Estados Unidos, y se trata normalmente de estafas u otro tipo de ilícitos (no necesariamente penales) relacionados con el impago o no envío de productos y mercancías[6]. Del año 2008 al 2009, se observó un

[5] LÓPEZ MARTÍN, S, «Jóvenes, Internet y Movimiento Antiglobalización: usos activistas de las Nuevas Tecnologías», en *Revista de Estudios de Juventud*, nº. 76, 2007, págs. 183-199.

[6] INTERNET CRIME COMPLAINT CENTER, Internet Crime Report 2009, págs. 2-5, (en inglés) www.ic3.gov. Se trata una publicación anual norteamericana, avalada por varias de sus agencias, entre ellas el FBI, y publicada por un organismo encargado de recibir las quejas de los usuarios. Las estadísticas desde el año 2000 hablan de un incremento muy significativo en la cantidad de delitos y otros ataques perpetrados en Internet, con especial incidencia en algunos tipos de ilícitos.

Interesante es destacar también que en 2009 España es el octavo país del mundo con más presencia de ciberdelincuentes (0.7 %), según ésta publicación.

incremento nada menos que del 71 por ciento del *software malicioso*, y un 50 por ciento de *troyanos*[7]. La cuestión es ya muy preocupante.

Por otro lado, desde el punto de vista meramente económico, todo ello origina grandes pérdidas monetarias a las víctimas en particular y al sistema económico en general. Así, para el año 2009 las pérdidas (sólo contabilizadas aquellas conocidas a través de las denuncias) alcanzaron casi los 560 millones de dólares[8]. Pero, por supuesto, los ataques que se producen en la red no se agotan en delitos de índole económica. Además de éstos (como las distintas constelaciones de estafas y fraudes), existe un amplio abanico de conductas que, utilizando de alguna manera Internet, lesionan algún bien jurídico-penal protegido. Estamos hablando de, por ejemplo, robo de identidades, vulneración del derecho a la intimidad y destrucción de *software* por virus informáticos. Dicho lo cual, es cierto que este tipo de asaltos «gratuitos» es relativamente menor a los de tipo «lucrativo», aproximadamente un 30 o 35 por ciento respecto del total[9].

Por último, la red también es plataforma de terroristas de todo el mundo. Captar fondos o reclutar adeptos, hacer apología de sus ideas, planificar atentados, sembrar el terror psicológico o incluso atacar mediante *hackers* la infraestructura de un Estado, son posibilidades nada alejadas de la realidad en que vivimos[10]. Este último aspecto, tan importante, no ha sido Tratado por la doctrina hasta hace unos pocos años atrás.

## III. Derecho Penal y «ciberdelitos»

### III.1. Nuevos retos y nuevos problemas

Como se ha visto hasta ahora, la especificidad de Internet como medio de comunicación ha originado lo que será conocido como «ciberdelincuencia». Por su singularidad con respecto a la delincuencia tradicional, este fenómeno exige una consideración especial por parte del Derecho Penal, puesto que la mayor parte de los métodos clásicos, como se advertirá, no sirven.

Basándonos inicialmente en las características de Internet propuestas por Svantessons que anteriormente se citaron y añadiendo otras nuevas, trataremos de analizar a continuación los problemas y retos que plantean la aparición de los nuevos tipos penales de la Sociedad de la Información.

#### III.1.1. La indeterminación del ámbito geográfico

La inexistencia de fronteras reales es una de las características intrínsecas de Internet, que ofrece innumerables ventajas y como no podía ser de otro modo, inconvenientes para la persecución de actividades delictivas. En primer lugar, para iniciar cualquier política criminal, hay que conocer cuál va ser el terreno de actuación. Dicho de otra manera, saber «dónde está Internet»; estamos ante uno de los grandes problemas que existen, dada la dificultad de responder con exactitud a dicha pregunta. No se trata de que Internet no esté en ningún sitio, o de que esté en todos, como se suele decir. Internet no

[7] SYMANTEC, «Symantec Internet Segurity Threat Report 2009», Volumen XV, abril 2010, págs. 11 y 12 (en inglés) www.symantec.com/content/es/mx/enterprise/other_resources/ISTR_15_Global_ ExSummary.pdf

[8] INTERNET CRIME COMPLAINT CENTER, *op.cit.* pág 4. De 264.6 millones en el año 2008, las pérdidas pasaron a 559.7 millones de dólares en 2009.

[9] *Ibid*, pág 6-7. Debe notarse, no obstante, que es razonable la existencia de una cifra aún mayor, puesto que las «destrucciones gratuitas» exhiben una tendencia a menor denuncia, como es razonable pensar.

[10] Por todos: MERLOS GARCÍA, A, «Internet como instrumento para la Yihad», en *Revista Iberoamericana de filosofía, política y humanidades*, nº 16, 2006, págs. 81-90.

está en el aire: aun no siendo un ente físico al que estamos acostumbrados, sí está «en algún lugar». La ingente cantidad de información que la compone está alojada en servidores distribuidos por todo el globo. Dichos servidores, en realidad, no son más que *discos duros* y otras herramientas conectados entre sí y con la Red. Situados en edificios, llamados *centro de datos*, su valor es incalculable en todos los sentidos, pues contienen desde nuestros datos bancarios hasta saberes multidisciplinarios que ya no se encuentran en los libros. Es por este motivo que son sumamente protegidos, y en muchas ocasiones no es revelado su paradero por las empresas, pues un ataque físico contra estos edificios no sólo puede destruir información, sino también compañías e incluso Estados[11]. De este modo, un primer problema lo encontramos en la gran dificultad de encontrar el origen mismo de dónde está depositada la información en Internet. Ello puede ser de extrema importancia a efectos de, por ejemplo, eliminar una determinada información que vulnera el derecho al honor de la persona[12]. Igualmente afecta directamente al asunto de la determinación de la competencia y jurisdicción de los Estados, a la que nos referimos en el siguiente apartado. La cuestión se complica aún más si los contenidos ilícitos se ocultan tras una cortina de *mirrors*, de modo que una página Web puede en realidad estar en otro lugar del que aparenta[13].

Pero además, y dado que a la Red se puede acceder desde cualquier parte del mundo prácticamente al instante, el siguiente problema relacionado con la independencia geográfica de Internet lo encontramos en la dificultad de perseguir un ilícito de estas características. Quiérase decir que un sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientas que la información está en otro lugar diferente de éstos. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados.

### III.1.2. La facilidad de comisión

Cometer delitos informáticos es mucho más sencillo de lo que pudiera parecer. En primer lugar requieren escasos recursos por parte del delincuente (apenas un ordenador conectado a la Red) y como se ha visto, pueden asimismo cometerse desde cualquier lugar del mundo. Pero además puede ser extremadamente sencillo hacerlo, hasta el punto que una persona con escasos conocimientos de informática sería hipotéticamente capaz de lograrlo. Aún digo más, puede llegar a hacerlo sin siquiera ser muy consciente de ello. Lógicamente, en este punto conviene diferenciar entre los distintos tipos delictivos, puesto que salta a la vista que las grandes estafas informáticas o la creación de complejos programas destructores no pueden ser llevadas a cabo por personas con limitado conocimiento de sistemas informáticos. Sin embargo, existen otros delitos, aparentemente simples, que sí admiten su comisión por cuasi-ignaros informáticos. Así, a modo de ejemplo, es posible enviar *virus* creados por otros (con relativa facilidad) o sabotear

[11] SIEBER, U, «Criminalidad Informática: peligro y prevención», en MIR PUIG, S. *Delincuencia Informática*, PPU, Barcelona, 1992, págs. 13 y 14.

[12] Nos estamos refiriendo al delito de injurias y calumnias en particular, tipificado en arts. 205 ss. CP. Existe variada jurisprudencia sobre el asunto, como el caso *Dow Jones vs. Gutnick, Joseph*, que luego se comentará. En dicho caso, del que conoce la Corte Suprema australiana, se publican en un artículo de un conocido periódico americano ciertas declaraciones difamatorias, acusando incluso de la comisión de delitos, contra un empresario australiano. No deseo analizar en este momento la resolución del Tribunal, pero sí señalar, a propósito de la independencia geográfica a la que nos referimos en el apartado «a», un aspecto del que se ha preocupado poco la doctrina. Se trata de preguntarnos qué ocurriría si a pesar de obtener una sentencia condenatoria ejecutable, la empresa propietaria de los soportes físicos en los que se halla la información se negara a cumplir con ella. En este caso, la realización efectiva del derecho del sujeto difamado se hace muy complicada, dadas las dificultades que posee cualquier sistema procesal para hacer cumplir una resolución de estas características.

[13] Un «espejo» (del inglés *mirror*) es un sitio Web que contiene una réplica de otro, pudiendo estar situados en lugares totalmente diferentes. Ver lo que se oculta detrás de cada página Web puede llegar a ser tarea complicada, dependiendo de cuán habilidoso sea el infractor.

programas informáticos mediante *cracks*, generadores de claves o similares que se encuentran en la World Wide Web sin demasiada dificultad[14].

Ello pone de manifiesto, una vez más, las insólitas dimensiones que presentan los nuevos delitos, que juegan en un ámbito que invita a la comisión de ilícitos, por su simplicidad, muchas veces desconociendo el infractor la entidad antijurídica de su actuación.

### III.1.3. El problema de las múltiples jurisdicciones

Nos referimos en concreto a la aplicación espacial de la ley penal. La gran libertad para cometer delitos con independencia absoluta del territorio, como se ha expuesto en el anterior apartado, origina grandes problemas. Recordemos, el sujeto activo puede cometer sin problemas un delito desde un Estado diferente al que se encuentra el sujeto pasivo, incluso sin saber dónde se halla éste último. Esta nueva perspectiva, genera dudas a todos los niveles, tanto en relación al órgano estatal que va a conocer del asunto, como de la posibilidad de ejecutar la resolución recaída. Igualmente, un problema importante será la distinta regulación del Derecho sustantivo en los distintos Estados. Pudiera crearse un falso espejismo si pensamos que debido a que en la esfera penal jurisdicción y ley aplicable siempre coinciden, no existen dificultades en lo relativo a las reglas materiales que deben ser aplicadas. Lo cierto es que, más allá de esta circunstancia, encontramos gran cantidad de supuestos en que determinados actos son punibles con arreglo al Derecho Penal de un Estado, pero no de otro, dando lugar a obvias desigualdades y zonas de impunidad.

En fin, todo ello origina una laguna normativa internacional en el ámbito de la jurisdicción competente en materia de delitos informáticos, que origina numerosos conflictos, siendo finalmente perjudicado, especialmente, el particular. La inseguridad que ello genera es elevada. Muchas veces es difícil determinar cuál es la legislación nacional que se estaría violando, de existir alguna, ya que todo el contenido de Internet aparece simultáneamente en todo el mundo. Dentro de este contexto, prácticamente todas las actividades en Internet tienen un aspecto internacional que podría involucrar múltiples jurisdicciones o provocar el llamado efecto indirecto[15].

A la hora de abordar este asunto, la doctrina suele traer a colación dos importantes casos de la jurisprudencia internacional: el caso *Yahoo* y el caso *Dow Jones vs. Joseph Gutnick*. En cuanto al primero, en aplicación del principio de territorialidad, el Tribunal de Gran Instancia de París condenó a la empresa Yahoo por la venta en territorio francés de artículos de orientación nacionalsocialista (art. 645.1 CP francés)[16]. El alto Tribunal impuso a la mencionada empresa la obligación de destrucción de todos los datos, el bloqueo a los usuarios franceses a la página *web* y la prohibición de venta de los susodichos artículos. Hasta aquí no existe objeción alguna; el problema era que la empresa Yahoo tenía (y tiene)

[14] El envío de «virus», si produce daños, se concreta en el artículo 264.2 CP. Por otro lado, un *crack* es un programa utilizado para alterar el software original sin el consentimiento del propietario. Ello permite, entre otras cosas, la copia de programas, el acceso y la utilización de éstos sin necesidad de adquirirlos o la eliminación de las restricciones establecidas por los fabricantes. La facilidad de comisión es increíble y se trata de una práctica muy extendida entre los usuarios de Internet y las nuevas tecnologías. En España el tipo podría encajar en el art. 248 CP (estafa informática, encaje forzado y con dificultad) y especialmente en el art. 270.1 y 270.3 (delito contra la propiedad intelectual «*Será castigado [...] quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras...*»). Es necesario el ánimo de lucro.

[15] KURBALIJA, J y GELBSTEIN, E, «Gobernanza de Internet: Asuntos, Actores y Brechas», DiploFoundation, publicación en línea, año 2005, http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1090, pág. 82.

[16] http://eric_goldman.tripod.com/caselaw/yahoovlicranov2001.htm (en inglés).

su sede en territorio estadounidense, y alegó que la orden era imposible de cumplir. Ello porque en EEUU la venta de productos relacionados con el nacionalsocialismo no es delito alguno, y los servidores de la empresa se hallaban en dicho país. Igualmente, también se consigue demostrar la dificultad para identificar con seguridad los usuarios franceses que accedían a la página Web en cuestión. Ésta constituye una demostración palpable de los problemas aludidos, incluso plantea la cuestión respecto de que un país tenga o no el derecho de imponer sus leyes a compañías de otro país (principio del mínimo común denominador[17]).

En el segundo caso, *Dow Jones vs. Joseph Gutnick*, conoce la Corte Suprema australiana de un delito de difamación contra un empresario australiano cometido a través de un artículo de un conocido periódico americano[18]. En este caso también se entendió la jurisdicción de los Tribunales australianos en base al mismo principio de territorialidad.

Como se sabe, cuatro son los principios que, tradicionalmente, rigen la competencia de los Tribunales de un Estado. A saber: el principio de territorialidad, el de personalidad, el real o de protección y por último, el de universalidad[19]. Entre ellos se generan numerosos conflictos. Como afirma Eduardo Aboso, los dos casos enunciados presentan aristas comunes[20]. Tanto la nacionalidad de la empresa involucrada como su argumento para tratar de sustraerse de la jurisdicción extranjera. Éste consistió en destacar que el lugar de comisión de los hechos fue territorio americano (donde las actividades están permitidas y no constituyen delito alguno), y no australiano o francés. Tanto las autoridades francesas como australianas entendieron que el hecho se produjo en Francia o Australia.

Observamos así el problema de la aplicación concurrente de leyes penales según el principio de territorialidad de los Estados. Tras esta complejidad normativa, podemos preguntarnos por el criterio a utilizar para determinar la jurisdicción competente. En los casos mostrados evidenciamos la purga entre el criterio del país donde se encuentran los contenidos, o donde se suben los archivos (postura de las compañías) o el del país donde se descargan o se produce el perjuicio (Francia/Australia). La cuestión puede complicarse aún más: el conflicto puede también producirse entre otros principios más allá del de territorialidad. Como se decía anteriormente, se trata de una laguna que necesita ser subsanada cuanto antes, mediante los mecanismos internacionales.

### III.1.4. El problema de la responsabilidad penal

No nos referiremos aquí a las personas físicas que carecen de la responsabilidad penal de sus actos, sino a un tema particular que ha suscitado polémica en los últimos tiempos: la responsabilidad penal de las empresas en la comisión de delitos por Internet.

Huelga decir, que el principio general del que se parte, en la mayoría de los países, es la irresponsabilidad de las personas jurídicas (formulado usualmente como *societas delinquere non potest*). Teniendo esto en cuenta, se critican las posibles lagunas de punibilidad que pueden aparecer ante la complejidad de determinar la responsabilidad penal. Así, primero hay que lograr probar la actuación de la empresa, después quiénes fueron realmente los autores de la infracción, y finalmente el grado de responsabilidad de la actividad de los diferentes partícipes en el delito[21]. La tarea se presenta en ocasiones

KURBALIJA, J y GELBSTEIN, E, *op. cit*. A raíz del caso «Compuserve» (año 1996), se difundió el temor de que la totalidad de Internet tuviera que ajustarse a la legislación más restrictiva.

[18] http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html (en inglés)

[19] En España queda contemplado el principio de territorialidad (art. 23.1 LOPJ), de personalidad (art.23.2 LOPJ), de protección (art. 23.3 LOPJ) y de protección universal (art. 23.4 LOPJ).

[20] ABOSO, E y ZAPATA, M, *Cibercriminalidad y Derecho Pena*l, B de F, Buenos Aires, 2006. págs. 32 ss.

[21] ABOSO, E y ZAPATA, M, *op. cit*. pág 42.

sumamente complicada y ello, dice parte de la doctrina, por el empeño en no admisión de la responsabilidad de las personas jurídicas.

En mi opinión, el anterior se trataría más de un problema de prueba que de una verdadera posible impunidad. La respuesta al problema pasa antes por la mejora del marco de la actividad policial encargada de investigar estos delitos que de la implementación de un sistema de responsabilidad penal de las personas jurídicas para el ámbito de los ciberdelitos.

Sin embargo, ahondando aún más el panorama vigente, en el Derecho español la doctrina sí asume la posibilidad de comisión de éstos por determinadas personas jurídicas (aunque como se ha dicho, la eventual imposición de penas deberá hacerse, en su caso, sobre las personas físicas que estén al frente de la sociedad). Obviaremos la polémica acerca de la aplicabilidad del artículo 30 del Código Penal[22]. Así, considerando, en la línea de Gómez Tomillo, que no existe problema alguno en su aplicación a los delitos informáticos cometidos a través de internet, precisaremos a continuación su alcance[23].

En los supuestos más normales, se tratará de una responsabilidad subsidiaria de los directores de las empresas ante la imposibilidad real de acudir contra el creador del contenido antijurídico depositado en la WWW y será normalmente una omisión por parte de la empresa, que se abstiene de impedir la difusión del contenido ilícito[24]. Pero debemos señalar que para poder condenar por varios de los ciberdelitos es necesario dolo (algunos autores sólo exigen el mero «conocimiento efectivo» de la existencia de los datos, otros «algo más» que facilitar la mera entrada a internet: un auxilio más allá de la mera prestación del acceso) y la existencia de una posición formal de garantía. El autor antes señalado exige además «la equivalencia estructural de la omisión con el potencial comportamiento activo»[25].

Por la naturaleza de este trabajo, no vamos a entrar a analizar qué delitos informáticos son susceptibles de su comisión por personas jurídicas, en principio podría ser cualquier ciberdelito, aunque se dice que usualmente poseen una estructura peculiar[26].

Será especialmente interesante referirse a la responsabilidad de los Proveedores de Servicios de Internet (comúnmente llamados ISP, por sus siglas en inglés). Aún se discute sobre si la empresa proveedora de estos servicios debe ser responsable por los contenidos (ilícitos o delictivos) que circulan por la Red. A este respecto, las conclusiones manifestadas anteriormente pueden ser trasladadas a los ISP. Así pues, igualmente se exige a los Proveedores de Servicios de Internet obligaciones jurídicas de impedir acceso a contenidos antijurídicos, y se les hace responsables por vía omisiva.

Toda la exposición sobre la problemática de la responsabilidad de las personas jurídicas no es frívola en absoluto: se trata de una cuestión aún controvertida y de extrema

[22] En estos delitos y faltas que analizamos, el artículo 30.1 CP español excluye la responsabilidad penal a los cómplices y otras figuras de cooperación necesaria, atribuyéndola en exclusiva a los autores, de manera «escalonada, excluyente y subsidiaria» de la siguiente forma: los autores directos/los directores de la publicación o programa/los directores de la empresa difusora/los directores de la empresa grabadora o reproductora.

[23] GÓMEZ TOMILLO, M, *Responsabilidad penal y civil de los delitos cometidos a través de Internet*, Aranzadi, Cizur, 2004, págs. 21 a 30

[24] *Ibid*, pág. 103.

[25] *Ibid*, pág. 89 y 90. Esto es, diferencia entre los servicios moderados (donde el proveedor realiza un comportamiento activo positivo de difusión) y los no moderados (donde el proveedor no interviene positivamente en el servicio). En el primer caso la empresa sería responsable con la mera omisión de eliminación de los contenidos, mientras que en el segundo, para este autor, una omisión sería insuficiente por sí misma para imputar el delito.

[26] Para más información, *vid.* GÓMEZ TOMILLO, M, *op. cit.*, págs. 61 a 67.

importancia en el ámbito de los delitos informáticos, dada la cantidad de empresas que operan en Internet y el papel que éstas desempeñan. Toda esta problemática hace proliferar las iniciativas destinadas a introducir normativa *ad-hoc*, véase el ejemplo de la ley alemana de Servicios Telemáticos, que disciplina los presupuestos y límites de responsabilidad jurídica de los sujetos jurídicos que actúan en el ámbito de las redes telemáticas y en la gestión de éstas[27].

La responsabilidad penal de las empresas proveedoras de servicios a título de participación en delito ajeno de manera omisiva ya ha quedado, con seguridad, desacreditada. Por otro lado, la responsabilidad como autoría a simple vista parece algo factible, pero se observa que, salvo casos específicos, no será sencillo atribuir dicha responsabilidad. No debemos olvidar tampoco que el control por parte de los ISP a los usuarios es complejo, y que la mayoría de las ocasiones es muy complicado o imposible para estas empresas impedir la comisión de delitos. El control directo sobre los posibles autores de los contenidos ilícitos parece casi imposible de realizar tanto por el anonimato como por la movilidad de los delincuentes. Así las cosas, nos preguntamos a modo de conclusión si los proveedores de acceso a Internet son responsables penalmente por los contenidos mostrados en la Web. Parece que es posible, sólo en grado de autoría y mediante la condena a los responsables al frente de las sociedades que hayan ejecutado los actos ilícitos, aunque dados los requisitos jurídico-penales, será complicado atribuir finalmente dicha responsabilidad.

### III.1.5. Dinamismo y descontrol

Internet es un fenómeno relativamente reciente; su aparición se enmarca en la segunda mitad del siglo XX y su utilización a gran escala en los inicios del actual. Es quizás por este motivo que todavía hoy carece de pautas fijas de acción, de normativa capaz de responder a la mayor parte de los problemas que se plantean. El asunto se complica aún más por la enorme capacidad de cambio y síntesis que posee Internet. En primer lugar, avanza a gran velocidad, y constantemente se transforma, cambia. Se ha dicho incluso que no cambia, sino que aún más: fluye, padeciendo un «renacimiento constante». En segundo lugar, debido a su íntima transversalidad, cualquier cambio en Internet es susceptible de afectar a las demás ramas del ordenamiento jurídico. Ello hace necesario prestar especial atención a su regulación, puesto que no se trata de un tema trivial. Actualmente se siguen discutiendo muchos de los pilares básicos, fundamentales, de la normativa del funcionamiento de Internet, lo que provoca que el Derecho Informático esté aún en formación, dificultando la adopción de medidas y políticas uniformes.

Por otro lado, la ausencia de una autoridad real que controle Internet, no hace sino acrecentar los problemas. El gobierno de ICANN (Corporación de Internet para la Asignación de Nombres y Números) no es realmente tal, puesto que sólo se preocupa de cuestiones puramente técnicas, quedando al margen todo lo demás, entre otras cosas, la problemática ciberdelictual. La cuestión de los delitos informáticos es abordada a un nivel muy inferior al mundial, bien nacionalmente o mediante Tratados multilaterales, siendo la máxima referencia actual el conocido como «Tratado de Budapest», que sin embargo no alcanza salvo a un limitado número de países. Así las cosas, si es cierto que el Derecho siempre va a la zaga de la sociedad que trata de regular, en el caso del Derecho Informático la distancia entre éste y su objeto es aún mayor, dados los especiales factores enunciados [28].

De ahí que podamos afirmar que la regulación de las nuevas tecnologías y en especial de Internet va a estar siempre plagada de lagunas, que se van rellenar lentamente

[27] PICOTTI, L, «Fundamento y límites de la responsabilidad penal de los proveedores de acceso y servicio en Internet», en *Revista de Derecho y Proceso Penal*, nº 3, 2000, págs. 218 a 220.

[28] KURBALIJA, J y GELBSTEIN, E, *op. cit.* págs. 76 y 77.

mediante autorregulación, en tanto en cuanto no exista una norma positiva que otorgue perspectivas de cierta seguridad jurídica. Solución, ésta última, que nos parece la más acertada, pero prácticamente imposible, dada la diversidad de planteamientos y opiniones contrapuestas.

### III.1.6. Crecimiento constante y desconocimiento

Internet no sólo se amplía de forma vertical, como se acaba de decir (constante evolución tecnológica) sino también horizontal; esto es, cada vez llega a más personas. En efecto, el uso de Internet se expande a ritmo frenético, cada día llega a más hogares y cada día más personas aprenden a utilizar las nuevas tecnologías, como se indicó en el capítulo primero. Gracias a los esfuerzos realizados por gobiernos, Organizaciones Internacionales, asociaciones, etc., se ha logrado una disminución cualitativa de la *brecha digital*, y se sigue progresando en ello[29].

Estos resultados, beneficiosos sin duda para el conjunto de la sociedad, traen consigo multitud de problemas. El aumento del número de usuarios de Internet acompañado de la escasa regulación, también provoca el incremento de las posibilidades de cometer delitos, más cuanto mayor sea la ignorancia informática de los nuevos consumidores de Internet. Además, la precariedad normativa supone un problema añadido en los países subdesarrollados, se crean verdaderos «paraísos cibernéticos», donde incluso los propios Estados fomentan el vacío legal para atraer explotaciones que en otros países serían ilícitas[30]. A su vez, el crecimiento constante no hace sino sumarse al problema anterior del exacerbado dinamismo de la Red, lo que dificulta la realización de políticas concretas, que se ven rápidamente superadas por los nuevos problemas que se presentan.

La independencia progresiva también del lenguaje, ya sea mediante traductores en línea o mediante el simple desarrollo *sui géneris* de la multiplicidad lingüística, posibilita el acceso de cualquier persona a cualquier contenido sin impedimentos. Todo ello, unido a la poca importancia que se presta a la educación en las nuevas tecnologías de la información, especialmente en los adultos, convierte a los ignaros informáticos en un blanco muy fácil para los delincuentes. El desconocimiento de algunos usuarios de las reglas básicas de funcionamiento de Internet no sólo es susceptible de convertirlos en sujetos pasivos de conductas delictivas, sino hipotéticamente, en sujetos activos (como se ha señalado en el apartado 1.b) de este mismo capítulo).

Se habla usualmente de desigualdad cuando se trae a colación algún aspecto de la «brecha digital». Pero quiero poner de manifiesto otro tipo de desigualdad que parece olvidada; la existente entre aquéllos que conocen y aquéllos que desconocen los entresijos de los sistemas informáticos en general, la cual tendrá una notable importancia en los delitos que se pueden llegar a cometer. Los primeros podrán cometer delitos sobre los segundos, y defenderse mejor de sus posibles ataques. Los segundos, por ignorancia, serán el objetivo y los más perjudicados por algunas de las conductas ciberdelictuales.

### III. 1. 7. Otros problemas procesales

Como dijo Sieber, los delitos informáticos no dejan huellas[31]. Al menos no huellas comparables con los delitos clásicos. Por ese motivo, las dificultades de descubrimiento y

[29] NARESH, S, «Sociedad de la Información: los nuevos pobres», en *Quark: Ciencia, medicina, comunicación y cultura*, nº 17, 1999, págs. 50-51.

[30] RODRÍGUEZ BERNAL, A, «Los Cibercrimenes en el Espacio de Libertad, Seguridad y Justicia», en *Revista de Derecho Informático*, nº. 103, 2007, pág. 6.

[31] SIEBER, U, *op. cit.*, pág. 94.

detección del delito informático se acrecientan significativamente en relación con los delitos tradicionales. Será necesario establecer nuevos métodos de investigación y desarrollar nuevas herramientas de cara a la persecución del delito informático.

Por ello la prueba constituirá un problema muy importante. La recolección de evidencias para los procesos judiciales originará una elevada complejidad. Así, en primer lugar es necesaria la identificación del sospechoso. Y ya se ha dicho lo difícil que puede llegar a ser conocer con precisión quién está detrás de la pantalla. Normalmente se acudirá a los proveedores de servicios, puesto que es relativamente fácil saber a través de qué ISP se está estableciendo el acceso. Parece que en este sentido, en la identificación de los presuntos responsables, se está progresando, pues la legislación mundial más reciente requiere que los ISP's identifiquen a sus usuarios y, en caso de solicitud, que revelen a las autoridades información pertinente sobre ellos[32]. Para esto se necesitará, en principio, una orden judicial[33].

Una vez identificado el supuesto sujeto infractor, cabe que, o bien se tengan suficientes datos para la intervención policial inmediata; o bien, sea necesario un nuevo mandamiento judicial (en este caso ya no existen dudas) para interceptar comunicaciones o bien para acudir al propio domicilio del infractor para revisar «el entorno físico que compone la vida cotidiana del autor»[34].

Como se observa, para evitar que las pruebas queden viciadas y salvaguardar los derechos esenciales de los individuos, es necesario el cumplimiento estricto de la legalidad procedimental, retrasando por ello la eficacia policial. En determinados supuestos serán necesarias multitud de resoluciones judiciales acreditadas para poder acceder físicamente al contenido de los datos, sin que se tenga siquiera la certeza real de haber conseguido un cúmulo de pruebas suficiente para imputar el delito a su autor[35].

En el tiempo que tarda en desarrollarse la reacción policial, ha sido posible la ocultación o la rápida eliminación de los datos mediante la destrucción física de los *discos duros* que les sirven de soporte. Ello sin contar con la posibilidad de encontrar datos cifrados que complica aún más el panorama, haciendo necesario un arduo proceso de descodificación, con elevado coste en tiempo y personal.

De este modo, es necesario propiciar la rápida intervención policial para evitar la destrucción de pruebas, y la mejor forma de lograrlo es mediante la unificación de actuaciones a nivel nacional e internacional[36]. Otra importante dificultad que se presenta, una vez cometido el hecho delictivo, es la paradójica posibilidad de que, ya no las autoridades, sino el propio perjudicado, no tenga conciencia del hecho[37]. Esto es, se trata de un hecho frecuente que el sujeto pasivo se da cuenta del delito cometido contra él mucho tiempo después de su realización, haciendo sin duda mucho más difícil la persecución y

[32] KURBALIJA, J y GELBSTEIN, E, *op. cit.* pág. 20.

[33] Se ha discutido, y aún se discute, acerca de la necesidad de un mandamiento judicial para interceptar la comunicación o para poder solicitar a la operadora ISP los datos del usuario. Finalmente, parece que la sentencia del TEDH 30 de julio de 1998 pacificó en parte dicha controversia, al afirmar que la inviolabilidad de las comunicaciones afecta también a la constatación de la comunicación misma; sin embargo, se han podido ver sentencias posteriores del TS español con una postura sustancialmente distinta (véase STS 22 de marzo de 1999). En general, las distintas legislaciones muestran la tendencia, cada vez más, de omitir el trámite de permiso judicial, especialmente para algunos tipos de delitos.

[34] MORALES PRATS, F y MORALES GARCÍA, O, (coords.), *Contenidos Ilícitos y Responsabilidad de los Prestadores de Servicios de Internet*, Thomson-Aranzadi, Elcano, 2002, pág. 244.

[35] *Ibid.*, pág. 245.

[36] ROVIRA DEL CANTO, E, «Las nuevas pruebas telemáticas y digitales. Especialidades de la prueba en delitos cometidos por Internet» en *Estudios jurídicos*, nº 1, 2003, págs. 286 ss.

[37] MORALES PRATS, F y MORALES GARCÍA, O, *op. cit.*, págs. 238 y 239.

búsqueda del responsable. Por otro lado, los procedimientos penales a menudo no se desean por miedo a que la reputación de las empresas resulte dañada, y se ocultan los delitos a las autoridades[38]. También el asunto se complica porque determinados delitos que pueden cometerse por Internet (art. 287 CP a modo de ejemplo) necesitan la denuncia previa del agravado para poder iniciarse la investigación pertinente, de modo que no basta el mero conocimiento del Ministerio Público para iniciar el proceso.

En la fase judicial encontramos otro problema, pues será obligatoriamente necesaria la asistencia de peritos expertos en el ámbito de las nuevas tecnologías. Es cierto que dependerá del delito cometido, pero desde mi punto de vista se corre el riesgo de llegar en el juicio a un nivel excesivo de abstracción y complejidad en relación con el delito tradicional. Por ello, y a pesar de la necesaria presencia de expertos en la materia, es necesaria la especialización de todos los participantes, tanto abogados, jueces como fiscales, a fin de que todos ellos cumplan su papel con soltura y eficiencia.

Por último, la situación de yuxtaposición de jurisdicciones antes aludida origina multitud de problemas procesales, en la fase previa y posterior a la resolución judicial. Las autoridades policiales tienen serias dificultades para conocer, *a priori*, si les corresponde o no a ellos iniciar la investigación. Igualmente ello puede dar lugar a conflictos positivos y negativos de competencia, con gran dilación de tiempo e ineficiencia, donde el perjudicado principal es la víctima.

Especialmente importante es la cuestión de la extradición. De nada sirve poseer la mejor policía y el mejor sistema para la averiguación de los delitos si finalmente el sujeto activo se protege tras una cortina legal en un Estado al que no es posible acceder. La viabilidad de la respuesta penal contra el ciberdelito depende de la articulación de procesos de diálogo interestatal en esta materia. La cuestión es relativamente sencilla dentro de la Unión Europea, por la existencia de la «euroorden», pero se complica fuera del territorio europeo, siendo necesario recurrir a Tratados bilaterales entre los distintos Estados. Este asunto, por su importancia, será ampliamente desarrollado en el siguiente capítulo.

### III.2. Derecho Penal Informático: tipología y autonomía

Todos los elementos conflictivos anteriormente enunciados están claramente interrelacionados, de manera que se influyen mutuamente, y cualquier solución pasa por una visión conjunta de todos ellos. Son pues las peculiaridades que plantean los nuevos delitos las que justifican su análisis particular; luego es necesario agrupar los tipos con rasgos y problemas comunes para un tratamiento adecuado y armonioso. A estos tipos comunes se les vendrá a llamar «ciberdelitos», y a la parte del Derecho Penal que los estudia, «Derecho Penal Informático».

Se han expuesto por la doctrina numerosas clasificaciones de los delitos informáticos. Desde las calificaciones más simples, como las que los dividen por su carácter económico o lucrativo y afección a la privacidad[39], como puso de manifiesto Sieber, a las más complejas, en función del método informático utilizado para lesionar al bien jurídico en cuestión[40]. Especial interés tiene la clasificación que diferencia si el sistema informático es el objetivo de la acción ilícita o si es tan sólo un instrumento para cometer otros delitos[41].

[38] SIEBER, U, *op. cit.*, pág. 96.

[39] G. SALT, MARCOS, «Delitos informáticos de carácter económico», en *Delitos no convencionales*, MAIER B.J.JULIO, Editores del Puerto, Buenos Aires, 1994, pág. 227.

[40] ACURIO DEL PINO, SANTIAGO, *Delitos Informáticos: generalidades*, publicación en línea, págs. 20 ss. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

[41] Por todos; D. GOODMAN, Marc, «The emerging consensus on criminal conduct in cyberspace», en *International Journal of Law and Information Technology*, vol. 10, nº 2, año 2002, págs. 155 y 156 (en inglés). En el

En torno a esta distinción se articula un controvertido debate acerca de si el concepto «delito informático» está compuesto por ambas categorías o no. Dicho de otra manera, lo que en realidad se discute es si una modalidad criminal consistente en la utilización de un ordenador (como medio) para perpetrar otro tipo delictivo es o no delito informático. Ello porque, se alega, la utilización de un ordenador no añade nada, no modifica la esencia del tipo que finalmente se comete. En esta cuestión, en absoluto trivial puesto que de ella parte el propio concepto de «delito informático», debo posicionarme en contra de la postura anteriormente citada. La autonomía de los delitos informáticos debe ser afianzada y desligada de los tipos comisivos tradicionales. Ello por una razón tanto *teórica* (si bien las modalidades comisivas informáticas pueden asociarse a tipos ya existentes, la función de las nuevas figuras delictuales sería la protección de la información y no del bien jurídico tradicional), como *funcional* (garantizar una adecuada persecución de estas conductas)[42].

Por último, otra clasificación de delito informático que es importante mostrar a efectos de este trabajo es aquella que diferencia entre la criminalidad que se vuelca en Internet y aquella que se desarrolla sobre «aparatos tecnológicos» (ordenadores, teléfonos móviles, etc.). Aquí, por la orientación de este trabajo, nos centraremos especialmente en el ciberdelito cometido en Internet, particularmente a través de la *World Wide Web* y el correo electrónico, dejando de lado otros modos de comunicación en la Red que consideramos de menor importancia.

### III.3. El inevitable expansionismo del Derecho Penal

Teniendo en cuenta lo dicho en el apartado segundo, la novedad y el dinamismo de la nueva sociedad de la información, y la necesidad de proteger a las personas de nuevas conductas perniciosas a través de la Red, es indudable que el Derecho Penal está experimentando una nueva expansión. De hecho, cualquier propuesta de solución de problemas, cualquier intento de mejora de las legislaciones, pasa inevitablemente por una ampliación de las conductas delictivas. Ésta parece ser la única alternativa a la protección de los bienes jurídicos que se vulneran en las distintas modalidades de delitos informáticos.

El expansionismo del Derecho Penal es un fenómeno global que ha penetrado forzosamente en todos los países y en la mayoría de las jurisdicciones penales[43]. Pero en el ámbito informático quizás se agrava y se hace necesario, dada la aparición de modernos bienes jurídicos y del surgimiento de nuevos riesgos. Así el Convenio de Budapest al que nos referiremos en el capítulo quinto, es un buen ejemplo de esta tendencia. Pero no es intención de este trabajo entrar a realizar una crítica al fenómeno del expansionismo del Derecho Penal; baste precisar alguna advertencia. Esto es, se debe tener cuidado con el incremento desproporcionado de los tipos delictivos. Siempre hay que tener en mente el carácter subsidiario y el esencial principio de *ultima ratio* del Derecho Penal. De este modo debemos preguntarnos a la hora de incriminar una nueva conducta si es realmente necesario, o si no bastaría una regulación administrativa o civil que estableciera su desvalor. No hace falta decir que el Derecho Penal sólo debería utilizarse en los ataques más importantes. Y nos consta, sin ánimo de especificar, que algunos de los delitos informáticos presentes en las diferentes legislaciones no responden en absoluto a estos principios. Por

primer caso estaríamos ante un delito genuinamente informático, puesto que se atenta directamente contra el sistema informático, contra la información contenida en él; bien destruyéndola o dañándola o bien vulnerando la confidencialidad de esos datos. En el segundo, se trataría una especie de evolución de los delitos tradicionales, como la estafa, utilizándose el ordenador como mero instrumento para alcanzar esos fines delictivos. Así por ejemplo, robo informático o fraude informático.

[42] En esta línea; AROCENA A., GUSTAVO, «De los Delitos Informáticos», en *Revista de la Facultad de Derecho*, UNC, vol. 5, nº 1, 1997, págs. 44 ss.

[43] MORILLAS CUEVA, LORENZO, «Nuevas tendencias del Derecho Penal: Una reflexión dirigida a la cibercriminalidad», en *Cuadernos de política criminal*, nº 94, 2008, págs. 18 ss.

ello, algunos autores advierten que se corre el peligro de ir hacia un Derecho Penal del Enemigo en materia de delincuencia informática[44]. Huelga decir que la tendencia preferible es la reducción progresiva de la presencia punitiva, pues definitivamente no toda conducta irregular relacionada con la informática ha de incluirse en el ámbito penal.

En definitiva, es innegable que hay un punitivismo ampliamente desarrollado en relación con la cibercriminalidad, pero también debemos tener en cuenta que estamos ante uno de los temas más necesitados de protección penal. Será necesario equilibrar la balanza introduciendo los principios garantistas propios del Estado Social y Democrático de Derecho.

## IV. Cooperación internacional frente al delito informático

### IV. 1. Preliminares

Anteriormente se ha dicho que cualquier medida que se tome en el ámbito ciberdelictual debe tener en cuenta el carácter específico y global al que se enfrenta, y que es necesaria una visión conjunta de los problemas. Pero no basta tan sólo con una indiferente atención a sus especificidades o con la ejecución de políticas diferenciadas. La lucha contra el ciberdelito va mucho más allá.

La dimensión supranacional juega, por tanto, una importancia crucial en el tratamiento de los delitos informáticos. Es imperativa la ejecución de políticas conjuntas, generales, que integren a todos los Estados y sectores de la sociedad.

Desde nuestro punto de vista, establecer una correcta política de cooperación pasa por la elaboración de políticas al más alto nivel, abarcando multitud de Estados. Lo ideal no son los Tratados bilaterales, sino convenios multilaterales que involucren al mayor número de países posible. De este modo sería posible armonizar las políticas regionales en materia de cibercrímenes, logrando una regulación coherente, que no se contradiga y cuya utilización fuera posible a gran escala.

La propuesta, somos conscientes, es muy ambiciosa. La necesidad de un mayor entendimiento entre países y el complejo entramado legislativo existente a día de hoy, hacen muy difícil la consecución de estos objetivos.

### IV.2. Derecho Penal Internacional y Derecho Procesal Penal Internacional

La diferenciación entre ambos constituye sin duda un paso previo fundamental a la comprensión de nuestro problema. Si bien dicha cuestión pudiera resultarnos en un primer momento baladí, es vital su comprensión como premisa ineludible de este capítulo, pues numerosas serán las referencias que se hagan a él *a posteriori*.

El primero de ellos se refiere a las normas sustantivas del *Derecho Penal* que configuran los distintos tipos ciberdelictuales. Estamos hablando de la punición de conductas específicas que se consideran lesivas de bienes jurídicos relacionados con la delincuencia informática.

Ejemplos de ello los tenemos en la elaboración de Tratados internacionales en relación a la guerra, como el Convenio de la Haya (1907) o los Convenios de Ginebra (1949); así como en determinadas materias como piratería, genocidio, tortura, drogas, etc. En todos estos casos, se observa el interés del legislador de alcanzar un cierto grado de

[44] *Ibid.*, págs. 26 a 31.

homogeneización normativa interestatal en la tipificación de determinadas conductas. La propuesta, así como nuestro deseo, es conseguir algo similar en relación con las infracciones penales informáticas. Esto es, lograr una armonización ciberdelictual en el plano sustantivo. Respecto a dicha armonización del Derecho Penal informático, la primera muestra de preocupación que conocemos procede de una recomendación del Consejo de Europa a los Estados de la Unión, en 1989[45]. En ella se invita a tener en cuenta el carácter supranacional del delito informático cuando los Estados procedan a modificar sus legislaciones al respecto, así como recomienda comunicar al Secretario General las experiencias de los Estados en materia de cooperación contra el delito informático.

Por el contrario, cuando hablamos de *Derecho Procesal Penal Internacional*, nos referimos en cambio a la consideración de los procedimientos para hacer efectivo dicho Derecho sustantivo penal. Son las técnicas, medios, facultades, procesos para lograr el efectivo cumplimiento de los diversos tipos delictuales que configura el Derecho Penal informático. Así, podemos referirnos a los procesos de diálogo entre Estados, intercambio de información, negociaciones de extradición (desarrollo particular *infra*), convenios sobre competencia, asistencia mutua, accesos intrafronterizos, articulación de procedimientos procesales subsidiarios, etc. Los ejemplos son numerosos; en este sentido la interminable variedad casuística coincide con la multiplicidad tipológica de dichos acuerdos. Igualmente, consideramos, cuando menos interesante, destacar la progresiva utilización de las tecnologías de la información con estos fines. Su uso, estimamos, es linealmente beneficioso para agilizar los trámites y lograr una sencilla instrumentalización de las técnicas de cooperación; en definitiva, una reducción de los tiempos, tan beneficiosa, como se vio, para la mejora de los derechos de las personas.

El correcto establecimiento de la cooperación internacional en el ámbito de los delitos informáticos necesita de ambas formas enunciadas: tanto la cooperación a nivel operativo entre las administraciones de justicia de los diferentes países y la mejora de las normas procesales, como el desarrollo común de las normas de Derecho Penal Informático sustantivo. En este sentido, el nuevo «Convenio de Budapest» sigue, como se verá en el capítulo quinto, ese camino. El único, entendemos, capaz de garantizar una eficaz lucha contra la ciberdelincuencia.

### IV.3. Modelo europeo: el ejemplo a seguir

Lo cierto es que tanto en materia de Derecho Informático como de cooperación internacional en general, la legislación europea se presenta como adalid indiscutible de las nuevas formas de colaboración entre Estados. En este punto no se hablará sobre el nuevo convenio sobre cibercriminalidad (que no es un proyecto de la UE -Consejo Europeo-, sino del Consejo de Europa), por el contrario, trataremos la visión integradora de las Comunidades Europeas sobre la cooperación en materia delictual en sus Estados miembros. Dicha visión parte de un deseo común de llegar a conclusiones semejantes sobre cuál debe ser el tratamiento adecuado de determinados fenómenos, en aras de una mayor eficacia. En realidad, la puerta a la cooperación en materia penal se abrió definitivamente en el ámbito de la Unión a partir del Tratado de Ámsterdam[46].

[45] Recomendación nº R. (89) 9 adoptada con el Consejo de Ministros el 13 de septiembre de 1989. https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 (en inglés).

[46] ROMÁN PUERTA, L, «Derecho Penal Supranacional y Cooperación Jurídica Internacional», en *Cuadernos de Derecho Judicial*, Consejo Gnal. del Poder Judicial, Madrid, 2004, pág. 35. Como meritorio principal, que afecta a la cuestión que nos ocupa, destacar la aparición del nuevo Título VI del Tratado de la Unión Europea, dedicado a la cooperación policial y judicial en materia penal.

De este modo, existen multitud de acuerdos específicos en materia de cooperación en Derecho Penal que por obvias razones tan sólo nombraremos, sirvan de ejemplo: el Convenio Europeo de Extradición (1957), el Convenio Europeo de la Haya (1970), el Convenio Europeo sobre Traslado de Personas Condenadas (1983), el Convenio de Aplicación del Acuerdo Schengen (1990) o el Convenio Europeo de Asistencia Judicial en Materia Penal (2000). Quizás sea éste último el que revista mayor importancia en relación con el tema objeto de este trabajo. Se dice que este acuerdo *«constituye la culminación de los esfuerzos para maximizar la asistencia judicial entre los juzgados de los países miembros»*[47]. Dicho convenio trata de facilitar la ayuda judicial mutua entre las autoridades competentes de los Estados miembros (policía, aduanas y tribunales), con el fin de que la cooperación penal resulte más rápida y eficaz. Para este propósito se prevén soluciones concretas como son: intercambio de información, equipos de investigación conjuntos, transmisión de documentos, interceptación de comunicaciones, etc. Su incidencia en la persecución del ciberdelito queda, aún a falta de mayor explicación, bien acreditada. Igualmente, no debemos olvidar otras expresiones más que notables de cooperación judicial en materia penal en el ámbito de la Unión Europea, como son la creación de la *Red Judicial Europea*, el *Eurojust* y la *Euroorden*[48].

En cuanto a la primera, se trata de una red de contactos judiciales entre los Estados miembros con el fin de facilitar la cooperación judicial, proporcionar información jurídica y práctica necesaria a las autoridades locales, participar y promover la organización de sesiones de formación en materia de cooperación, constituir un foro de debate sobre los problemas prácticos y jurídicos o encauzar posibles modificaciones normativas y mejoras prácticas. Ello en el marco de la lucha contra formas de delincuencia grave (delincuencia organizada, corrupción, narcotráfico y terrorismo).

El *Eurojust*, por su parte, es un órgano que se encarga de realizar «...*investigaciones y actuaciones relativas a la delincuencia grave que afecta al menos a dos Estados miembros [...] Su papel es promover la coordinación entre autoridades competentes de los distintos Estados miembros y facilitar la cooperación judicial entre ellos*»[49]. Desde nuestro punto de vista su importancia será el apoyo general a las autoridades competentes de los Estados miembros para dar mayor eficacia a sus investigaciones y actuaciones. Cabe decir que tanto la Red Judicial Europea como Eurojust mantienen entre sí relaciones a efectos de colaboración y consulta.

Por último, en cuanto a la orden de detención y entrega europea, más conocida como *euroorden*, supone la evolución natural de la extradición, constituyendo un procedimiento muy avanzado que permite reconocer, *ipso facto* y con escasísimos condicionantes, la petición de entrega de una persona formulada por la autoridad judicial de otro Estado miembro. Su importancia es tal que ha sido reconocida por muchos como la «piedra angular» de la cooperación judicial penal en la Unión Europea[50]. La detención y entrega puede llevarse a cabo para el ejercicio de acciones penales o la ejecución de una pena; igualmente se establecen límites mínimos de condena y circunstancias especiales de rechazo de la extradición. Incluso es posible excepcionar, en determinados casos, el principio de doble incriminación. Todo ello origina, como decíamos, un proceso

[47] HÖPFEL, F, «Nuevas formas de cooperación internacional en materia penal», en *Cuadernos de Derecho Judicial*, nº 7, 2001, pág. 231.

[48] Red Judicial Europea; *vid*. Acción Común de 29 de junio de 1998 adoptada por el Consejo (98/428/JAI) y Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea. Eurojust; *vid*. principalmente Decisión del Consejo, de 28 de febrero de 2002, por la que se crea *Eurojust* para reforzar la lucha contra las formas graves de delincuencia (2002/187/JAI). Euroorden; *vid*. en particular la Decisión marco 2002/584/JAI del Consejo de 13 de junio de 2002 relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros.

[49] http://www.eurojust.europa.eu/about.htm (en inglés).

[50] Consejo Europeo de Tampere, 1999, Conclusiones de la Presidencia http://www.europarl.europa.eu/summits/tam_es.htm

inevitablemente veloz, imprescindible para la adecuada persecución del delito internacional, aún con las posibles costas en materia de Derechos Humanos[51].

Se observará que las normas comunitarias expuestas se refieren a Derecho Procesal Penal Internacional, no a Derecho sustantivo. Podemos preguntarnos si la Unión Europea ha establecido en algún momento normas penales. La respuesta, en principio, debe ser negativa. La materia penal es una parcela que tradicionalmente queda reservada a la soberanía de los Estados y aunque un Estado puede sin duda obligarse mediante directivas o Tratados internacionales, finalmente es el propio país el que debe decidir, como acto soberano, promulgar la norma penal[52].

Por último, el Tratado de la Unión Europea, aun no conteniendo mención explícita del cibercrimen, como viene diciendo Rodríguez Bernal, puede ofrecer marco jurídico suficiente para regular dicho fenómeno. De este modo, el Consejo Europeo, por medio de acciones conjuntas, decisiones, convenios, etc., puede regular una porción importante de la materia, suministrando los instrumentos necesarios para la persecución de los delitos informáticos[53]. Asimismo, existen también importantes Decisiones en el pilar de la Cooperación Policial y Judicial en Materia Penal que afectan cuasi directamente a los delitos que nos interesan[54].

Es importante destacar que si bien la regulación comentada *supra* no se refiere en particular a los delitos informáticos, la mayoría de sus previsiones pueden ser aplicadas a la comisión de éstos, acreditando así el fundamento de la exposición. No obstante la nula tangencialidad de dicha información, algunas normas se refieren con carácter expreso a la delincuencia informática, véase el artículo 4 de la Decisión del Consejo por la que se crea *Eurojust* (28 de febrero de 2002), a modo de ejemplo.

### IV.4. La cooperación penal en el contexto español: especial referencia a la extradición

En cuanto a España, debido a su situación geopolítica, deben tenerse en cuenta las consideraciones sobre la Unión Europea que se han descrito *supra*. Poco más se puede decir que afecte al ámbito de los delitos informáticos. Son importantes las normas internas que se refieren a la cooperación judicial internacional a nivel general, pero tan sólo ciertos preceptos de algunos cuerpos legales atienden en particular a la cuestión penal[55]. Con respecto a la cooperación en sede de la Corte Penal Internacional, en España existe la Ley Orgánica 18/2000 de 10 de diciembre de Cooperación con la Corte Penal Internacional. Dicha normativa es notablemente avanzada, y regula cuestiones clásicas como la detención, entrega, libertad, formas de colaboración, competencia e incluso medidas de reparación. Sin embargo, en este caso la utilidad para el ámbito ciberdelictual es quizás más reducida, puesto que el Tribunal de Justicia Internacional de la Haya juzga determinados delitos que no son susceptibles de ser cometidos a través de la Red, con la excepción quizás del terrorismo[56].Además, resaltar la existencia de convenios internacionales en que forma parte,

[51] LEGIDO SÁNCHEZ, A, «La Euro-orden, el principio de doble incriminación y la garantía de los derechos fundamentales», en *Revista electrónica de estudios internacionales*, nº 14, 2007, pág. 55. El autor pone de relieve el modo de afección de este procedimiento a los derechos de los particulares «*...el modelo instaurado hace prevalecer en todo caso las obligaciones de cooperación sobre los derechos fundamentales...*».

[52] RODRÍGUEZ BERNAL, A, «Los Cibercrimenes en el Espacio de Libertad, Seguridad y Justicia», en *Revista de Derecho Informático*, nº. 103, 2007, págs. 15 a 22.

[53] *Ibid*. págs. 22 a 25.

[54] Véase la Decisión 2000/375/JAI de 29 de mayo de 2000 relativa a la lucha contra la pornografía infantil en Internet o la Decisión 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información.

[55] Arts. 193, 194, 824, 829 LECrim, 276, 277, 278 LOPJ y la ley 21 de marzo de 1985 de Extradición Pasiva.

[56] Véase lo descrito *supra* sobre el terrorismo a través de Internet (final del capítulo segundo).

así como el Convenio de Asistencia Judicial en materia Penal de 1959, en el ámbito de Europa (no de la UE), que sin embargo tendrán aún menor importancia en lo que respecta al objeto que analizamos.[57]

Por último, retomando la cuestión de la extradición, que es *«el modo de garantizar la eficacia de la ley penal material que en virtud de ese fraccionamiento de soberanías puede estar amenazada»*, resta comentar algunos aspectos aclaratorios más allá de los ya comentados[58]. La técnica de la extradición supone, a grandes rasgos, el traslado de una persona acusada o detenida en un Estado a otro distinto, para ser juzgada o ejecutada su pena. Se trata de una materia que continúa dominada por los Tratados bilaterales, con la notable excepción de la UE, y que posee tradicionalmente requisitos generalizados, a saber: doble incriminación y especialización, reciprocidad, voluntad cooperadora y existencia de un núcleo duro insalvable constituido por los delitos políticos y la pena de muerte[59]. En España, además de la normativa comunitaria a la que antes se hacía referencia, y de ciertos artículos de la Ley de Enjuiciamiento Criminal, existe la Ley 4/1985 de Extradición Pasiva, que también debe ser tenida en cuenta. Lo cierto es que la cooperación jurídica internacional en el ámbito procesal (recordemos, Derecho Procesal Penal Internacional) se ha manifestado precisamente, y de forma tradicional, a través del instituto de la extradición[60]. También resaltábamos anteriormente [Cap. 3, epg.1, apr. g)] la importancia que la extradición juega en la persecución del delito informático, dada la universalidad de éste.

### IV.5. La cooperación internacional como paradigma de la solución a la problemática ciberdelictual

Con todo lo dicho hasta aquí, queda clara la trascendencia de la cooperación internacional de cara a la persecución de los delitos informáticos. La cooperación, *in abstracto*, posee una estricta relación con la solidaridad intercultural, con la concurrencia recíproca de ideas y soluciones, con la ayuda mutua, así como con la apertura a otras formas de colaboración transversal que alcance nuevas disciplinas. Esta generalidad es precisamente su mayor ventaja, pero también un inconveniente. Ello por la complejidad y dificultad que supone articular procesos participativos que involucren a gran cantidad de Estados, cada uno de ellos con sus peculiaridades e intereses, así como concordar la gran cantidad de elementos en juego.

Somos conscientes de que dicho instrumento no se trata de una suerte de panacea universal capaz de solucionar *per se* todos los problemas que se presenten. Pero sí entendemos que puede contribuir definitivamente a corregir muchas de sus dificultades, o al menos asentar las bases para llegar a una hipotética normativa que responda efectivamente a gran parte de las contrariedades descritas en el primer apartado del capítulo tercero. Para ello será necesario salvar primero el importante escollo del inherente antagonismo diplomático de los países y forzar a los Estados a tomar decisiones conjuntas de los problemas que les afectan.

Veremos a continuación de manera particular las principales ventajas que, creemos, se desprenden del uso conveniente de la técnica de la cooperación en materia

[57] La cantidad de estos acuerdos es tan elevada que no queremos pretender siquiera nombrar todos ellos. Baste citar algunos: Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes, Convenio Internacional para la Represión de la Financiación del Terrorismo, Convenio para Represión del Apoderamiento Ilícito de Aeronaves, Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas, etc.

[58] PUENTE EGIDO, JOSÉ, «La Extradición, problema complejo de Cooperación Internacional en materia penal», en *Boletín Oficial de la Facultad de Derecho*, nº15, 2000, pág. 209.

[59] Para más información; *ibid*. págs. 215 ss.

[60] ROMÁN PUERTA, LUIS, *op. cit*. pág. 31.

ciberdelictual, sin ánimo alguno de cerrar el paso a otras muchas que también pueden llegar a darse.

### IV.5.1. Mayor intercambio de información

En primer lugar nos referiremos a la información. Como sabemos, se ha dado en llamar a los tiempos actuales, en referencia a la revolución socioeconómica que nos ha correspondido vivir, «Sociedad de la Información»; como tal, la información tendrá un papel fundamental en nuestros días. Por un lado el intercambio de información es lo que da origen a la Red, y por tanto a los ciberdelitos, y por otro lado este mismo elemento es cardinal para el descubrimiento y caza de los infractores. Apuntaremos que los datos que se incluyen dentro del concepto amplio de «información» que estamos utilizando son muy variados: pesquisas, averiguaciones, documentos de todo tipo, exámenes, investigaciones, normativa, procedimiento, cédulas, interrogatorios, etc.

Para un adecuado uso de la información, es necesaria su diversificación en múltiples vías. Debe producirse, en primer lugar, en el interior de un Estado, entre sus diversas instituciones, órganos y autoridades. La información debe fluir eficazmente a todos los niveles y jerarquías; entre fuerzas policiales y de seguridad, órganos jurisdiccionales e instituciones gubernamentales. Éste es el primer escalón. Una vez logrado, mediante políticas meramente internas, es ya posible saltar al plano supranacional y entrar en la cooperación internacional. En ese momento habrá que adoptar políticas entre los diferentes países a efectos de lograr un efectivo intercambio de información. La cooperación en este sentido debe materializarse en normas de Derecho Procesal Penal que articulen los adecuados procedimientos para la transmisión de información, en la línea que se describe a continuación.

Dada la universalidad del delito informático y sus dificultades procesales, como apuntábamos, será muy importante conocer todos los datos acerca de los distintos elementos que configuran el ciberdelito en el tiempo y la forma adecuados. En este sentido la agilidad y rapidez en el intercambio de la información serán aspectos que beneficiarán inmensamente la persecución de los delitos informáticos. Igualmente, será muy importante para dotar de una mayor presteza a la investigación llevar a cabo una simplificación cualitativa de los medios de comunicación. A tal efecto recordamos lo que decíamos *supra* acerca de la utilización de Internet y las nuevas tecnologías (así como los intercambios vía Web) para dotar de celeridad a las pesquisas policiales. En cuanto a la actualidad de las comunicaciones de información, el intercambio debe darse como mínimo después de la comisión del delito, así como una vez realizada la aprehensión del sujeto sospechoso. Sin embargo, entendemos que lo óptimo es que se produzca a lo largo de todas las fases del proceso, tanto en la fase de instrucción como en la de enjuiciamiento y ejecución de la pena, incluso con anterioridad a la perpetración de hecho delictual alguno.

Interesantes propuestas se pueden extraer de la normativa europea antes mencionada en aras de facilitar el adecuado intercambio de información. Véase así el establecimiento de equipos de investigación conjunto o el interrogatorio de testigos o peritos por videoconferencia[61]. Igualmente, de la *Red Judicial Europea* descrita *supra* podría servir de modelo para la creación de una red de juristas de contacto entre diferentes países, en la línea seguida por el avanzado sistema I-24/7 de Interpol para intercambiar información sobre delincuencia informática entre sus países miembros[62].

[61] Convenio de la Unión Europea relativo a la asistencia judicial en materia penal, aprobado por el Consejo Europeo el 29 de mayo de 2000. Véase el artículo 13 en referencia a los equipos de investigación conjunto así como los artículos 10 y 11 en relación con la audición por videoconferencias o conferencias telefónicas.

[62] Se trata de la cooperación operativa entre los países miembros mediante una lista de oficiales de contacto disponibles las 24 horas del día para todo lo relacionado con las investigaciones sobre delincuencia informática.

Facilitar el intercambio de información a todos los niveles es quizás la más importante de las ventajas que puede proporcionar la cooperación internacional, dada su transversalidad, afectando tanto a la alta toma de decisiones como a la actividad administrativa y jurisdiccional común. En este sentido, resulta sencillo advertir que la efectividad de los puntos subsiguientes de este epígrafe depende en cierto modo de la adecuada fluidez de la información.

### IV.5.2. Efectividad en materia policial[63]

La cooperación permite avanzar en el hallazgo y persecución de los delitos que analizamos. Especialmente importante es en este punto la colaboración entre unidades policiales, encargadas de reprimir este tipo de delitos, de los distintos Estados. Dado nuevamente el carácter transfronterizo de los ciberdelitos, no se necesitan demasiadas explicaciones para percibir el modo en que la cooperación beneficia las actividades de las fuerzas y cuerpos de seguridad en la represión de dichos delitos.

Lo ideal es que dentro de los cuerpos policiales comunes existan determinados grupos especializados en la persecución de los delitos informáticos, a fin de una mayor especialización y mejor seguimiento de los casos concretos. En realidad estas unidades policiales deberían tener un funcionamiento similar al resto, excepcionando una específica preparación en el ámbito informático, como resulta lógico. Igualmente entendemos que dichas unidades especiales necesitarán en mayor medida de equipos informáticos e instalaciones modernas, en continua actualización para que los avances tecnológicos no supongan en modo alguna ventaja a favor del delincuente. En definitiva, mayor formación y material avanzado conlleva inevitablemente un elevado incremento del gasto público, lo que en numerosas ocasiones impide que por cuestiones de política policial no sea posible una represión adecuada de las conductas punibles informáticas, especialmente en países subdesarrollados o en vías de desarrollo.

Siguiendo a Antonio López, distinguimos dos vías de cooperación internacional policial: la realizada a través de convenios internacionales y la que se sustancia mediante organizaciones internacionales ya consolidadas como Interpol[64]. La primera vía, caracterizada por los convenios bilaterales entre Estados, es de acción limitada por su inevitable confinamiento a la negociación particular entre muy pocos países, hasta la aparición, claro está, del Convenio sobre Cibercriminalidad. En cuanto a la segunda, hemos de destacar la organización internacional Interpol, cuyo ámbito de acción es prácticamente universal, abarcando hasta 188 miembros. Sus objetivos son el desarrollo de asistencia recíproca entre las autoridades de los diferentes países y el establecimiento de instituciones que puedan contribuir a la prevención y a la represión de las infracciones de «Derecho Común»[65]. Realizará una importante labor en la lucha contra la cibercriminalidad dada su extensión mundial; más allá del mero intercambio de información antes aludido (sistema I-24/7), Interpol favorece enormemente la cooperación entre las fuerzas de seguridad de todo

Esta red de contactos está operativa 24 horas al día y siete días a la semana (de ahí su nombre), y a través de ella se reciben o transmiten datos y solicitudes de asistencia. La existencia de estos puntos centrales de referencia nacionales sobre delincuencia informática constituye un requisito indispensable para el establecimiento de un sistema de alerta rápida. «Más de 120 Oficinas Centrales Nacionales de Interpol han designado ya puntos centrales de referencia».

[63] Este punto y el siguiente suponen las dos caras de la misma moneda que es el tratamiento del delito informático. Es decir, mientras que en este subepígrafe se tratará la cuestión de la cooperación policial previa al ilícito así como la averiguación del delito y captura del culpable, en el siguiente nos centraremos en el enjuiciamiento y posterior ejecución de la posible sentencia condenatoria.

[64] LÓPEZ, A, «La investigación policial en Internet: estructuras de cooperación internacional», en *IDP Revista de Internet, Derecho y Política*, nº 5, 2007, págs. 10 ss.

[65] Artículo 2 del Estatuto de la Organización Internacional de la Policía Criminal-Interpol. Véase su página Web oficial: http://www.interpol.int.

el mundo a lo largo del *íter* policial completo para la indagación del delito y búsqueda del sujeto transgresor. A su vez, permite la *«elaboración de estrategias y tecnologías y la búsqueda de información en relación con los últimos métodos empleados en este tipo de delincuencia». «Interpol ha creado una red de investigadores designados que trabajan en unidades nacionales dedicadas a la delincuencia informática, a los que se denomina puntos centrales de referencia nacionales sobre delincuencia informática, a fin de facilitar el contacto operativo entre los países miembros con la máxima rapidez posible»*[66].

En el ámbito europeo, la cooperación policial alcanza cotas más altas con la presencia del llamado Protocolo Schengen y Europol. El primero es un acuerdo para la supresión real de las fronteras y los controles interiores entre los países signatarios (no coincide con los territorios de la UE). Aún más, incorpora medidas de colaboración policial y judicial y armonización de legislaciones en múltiples materias para la persecución de la delincuencia. En cuanto a Europol, dependiente de la Oficina Europea de policía, tiene por misión la coordinación de las policías europeas, proporcionar apoyo, facilitar intercambios de información, etc., en la lucha contra la delincuencia. En relación con los ciberdelitos, se prevén específicamente «*...tareas de recogida y análisis de información en Internet para contribuir a identificar las actividades delictivas facilitadas por Internet o cometidas a través de Internet*» [67]. Se prevén multitud de sistemas de cooperación tendentes al intercambio continuo de información, por lo que su efectividad en la lucha contra el ciberdelito queda patente. Especialmente conviene mencionar la importancia que ha supuesto la utilización de bases de datos para la persecución de determinado delitos a través de Internet, como son el fichero «*Twins*» y el archivo «*Terminal*»[68].

### IV.5.3. Efectividad en materia procesal

Se ha visto que numerosos son los problemas procesales que se producen en materia ciberdelictual, debido a las características propias de la materia que tenemos entre manos. Estamos ante los problemas más acuciantes y graves, pero a su vez en la zona más pantanosa de la amplia amalgama de la problemática que exhibimos. Por un lado, numerosos y complicados son los problemas que se presentan, con numerosas lagunas de por medio, y por otro, es el espacio más necesitado de regulación. No en vano, la mayor parte de los problemas que observábamos en el epígrafe primero del tercer capítulo eran de tipo procesal: dispersión normativa, múltiples legislaciones y jurisdicciones, amplitud geográfica, responsabilidad de personas jurídicas, recolección de evidencias, vicios del proceso, demoras, ejecución de resoluciones, etc. Al respecto, creemos que éste es precisamente el ámbito en el que más esfuerzos de cooperación internacional deben realizarse. Así lo cree también la doctrina, pues ya solicitaba la pronta armonización de las cuestiones de prueba electrónica a nivel europeo[69]. Igualmente se observa dicha preocupación en la práctica internacional, pues la mayor cantidad de convenios son de Derecho Procesal Penal Internacional, relegando el Derecho Penal sustantivo a un plano secundario.

---

[66] Publicación (Fact sheet) de Interpol nº COM/FS/2008-07/FHT-02 acerca de la delincuencia informática, http://www.interpol.int/Public/ICPO/FactSheets/FHT02ES.pdf.

[67] Decisión 2009/371/JAI del Consejo por la que se crea Europol (art. 5.2)

[68] El primero («*Twins*») es una base de datos en relación con la pornografía infantil, el cual proporciona información y nombres acerca de víctimas y agresores, permitiendo un acceso por todos los Estados involucrados para una eficaz identificación y búsqueda de los sujetos en cuestión. El segundo («*Terminal*») recoge datos sobre estafas electrónicas, en concreto de robo, uso y duplicado de tarjetas bancarias a través de la Red. Ambos son excelentes ejemplos de cooperación policial internacional, cosechando, nos consta, más que notables éxitos.

[69] GARCÍA GONZÁLEZ, N y otros, «Pruebas electrónicas ante los Tribunales en la lucha contra la cibercriminalidad: un proyecto europeo», en *Revista Venezolana de Información, Tecnología y Conocimiento*, nº2, 2008, págs. 146 ss.

No es momento de repetir de nuevo los distintos convenios referentes que se han venido enunciando a lo largo de este trabajo, a ellos nos remitimos, pues, para la complitud del apartado, especialmente a la descripción sistemática realizada en el epígrafe tercero y cuarto de este mismo capítulo.

Como venimos diciendo, a pesar de la existencia de numerosa normativa internacional y de los cuantiosos progresos, siguen existiendo incontables lagunas, la mayoría de ellas originadas en el plano transnacional innato a los ciberdelitos, y por ello no queda sino volcar los futuros esfuerzos en seguir conformando el Derecho Procesal Penal Internacional ciberdelictual así como solucionar aspectos localizados tales como la extradición y el reconocimiento de resoluciones.

### IV.5.4. Armonización sustantiva y mayor planificación

Si anteriormente nos referíamos a las ventajas que una ideal cooperación internacional tiene en el plano del Derecho Procesal Penal Internacional, ahora es tiempo de centrarse en el Derecho Penal Internacional. En este sentido el principal beneficio a obtener es sin duda la armonización normativa del Derecho sustantivo en materia de los delitos informáticos, con todas las mejorías que lleva aparejada.

El principal problema que encontramos es que, al contrario que en el ámbito procesal, resulta más complicado elaborar Tratados internacionales que modifiquen o impongan determinadas normas penales a los Estados. El Derecho Penal es una parcela que tradicionalmente ha sido reservada a la soberanía de los Estados, y como se decía, ni siquiera la Unión Europea puede obligar directamente en este sentido a sus miembros. Por supuesto, la consecuente derivación del principio *pacta sunt servanda* vincula categóricamente a los Estados parte en un Tratado; mas al final son ellos quienes deciden la transposición de dichas normas a su plano interno. Respecto de la citada armonización, la primera gran manifestación a nivel mundial en el ámbito de los delitos informático aparece en el, tantas veces mencionado, Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Más allá, en relación con los hipotéticos beneficios derivados de una armonización de los delitos informáticos, éstos se hacen patentes tanto en el plano material como en el procesal. Dicho de otra manera, una puesta en común supraestatal de los tipos ciberdelictuales proporcionaría una mayor lucidez y racionalidad al tratamiento de éstos. El sistema necesita coherencia y sensatez y no multiplicidad de tipos y penas, con distinta aplicabilidad y entidad, que origina inseguridad. Evitar desigualdades y «paraísos delictivos» por la presencia de lagunas es también uno de los objetivos; en otras palabras, impedir que una misma acción esté penada en un lugar y no en otro.

Por otro lado, la planificación global en todos los sentidos así como la previsión de estrategias mundiales en la lucha contra el cibercrimen es también una importante ventaja que se puede derivar de la cooperación internacional. De este modo es posible no sólo la coordinación de unidades judiciales, policiales o gubernativas, sino la elaboración de políticas al más alto nivel en la prevención del delito informático. Las conferencias preparatorias de los acuerdos o convenios, las reuniones periódicas en el seno de organizaciones internacionales, todas ellas juegan un importantísimo papel que permite sentar las bases dogmáticas que luego servirán para la elaboración de importantes pactos internacionales en materia ciberdelictual. Consecuencia accesoria es asimismo el reforzamiento de los vínculos de solidaridad interestatales, un mayor entendimiento intercultural que sirva no sólo para lograr una colaboración eficaz a lo largo de las distintas etapas del proceso, sino también para estrechar lazos entre países y crear puentes para futuros acuerdos y convenios en materia ciberdelictual.

### IV. 5.5. Beneficios a los particulares

Los individuos son los destinatarios de la Ley en general, y de la Ley Penal en particular, pues ésta última afectará a sus derechos en mayor medida. Es por eso que entendemos que no puede iniciarse ninguna política legislativa criminal, y mucho menos internacional, si no se lleva a cabo pensando en todo momento en los ciudadanos a los que va a ser aplicada: tanto en las víctimas como en los delincuentes. Respecto de los primeros, lograr una adecuada persecución de los delincuentes, medios sencillos de denuncia y comunicación transnacional, construir procesos efectivos de reparación de daños y real punición de los delitos,son los elementos hacia los que una práctica cooperación internacional en esta materia debiera avanzar. En cuanto a la represión del posible delincuente informático, hay que tener siempre presentes las garantías procedimentales que debieran ser congénitas a todo sistema de enjuiciamiento penal, sin perder de vista en ningún caso el respeto de los Derechos Humanos consignados en los distintos Tratados internacionales. Ni siquiera los grandes problemas procesales o probatorios, las necesidades de celeridad, pueden justificar un detrimento de los derechos individuales que deben corresponder como persona. Otro importante beneficio y cuestión en la que se debe trabajar es la necesidad de una mayor información al público en general, tan importante para evitar los problemas que describíamos [cap. III, epg.1, apr. f)].

Por otro lado, obsérvese que una adecuada consecución los puntos señalados anteriormente confluye inevitablemente en beneficios para los justiciables, de modo que un correcto intercambio de información [a)] y una mejora de las condiciones procesales y/o sustantivas [b), c) y d)] permiten el alivio de la problemática que se nos presenta, dirigiéndonos hacia una preciada seguridad jurídica. Así, a modo de ejemplo, el afectado por un ilícito de estas características podrá defender mejor sus derechos si existe una adecuada estructura de competencias legislativas.

### IV.6. ¿Cómo debe ser la cooperación ciberdelictual? Elementos para una adecuada construcción en el plano internacional

Se ha visto la importancia de la cooperación internacional y asimismo su carácter indispensable para solucionar los problemas derivados del carácter supranacional de los delitos informáticos. Para finalizar este capítulo, trataremos de visualizar con carácter esquemático los requisitos que debe investir una adecuada cooperación internacional en materia ciberdelictual para solucionar los problemas analizados en el Capítulo III y poseer algunas las ventajas del epígrafe anterior. A ellos se deben añadir las consideraciones técnicas de Sieber en relación con los delitos contra la «*privacy*», con idéntica superposición para los delitos informáticos[70]. D*e lege ferenda*, hallándonos ante las instancias previas de un hipotético acuerdo internacional, varios son elementos a tener en cuenta, a saber:

[70] SIEBER, U, *op. cit.*, págs. 92 ss. El autor propone un acuerdo sobre los principios básicos de los delitos informáticos, así como el establecimiento de una lista de infracciones. Varios son los principios que para él deben tenerse en cuenta:

1- Utilización preferible del Derecho Civil y Administrativo, a fin de salvaguardar el principio de *última ratio*.

2- Descripciones de los actos prohibidos de forma precisa.

3- Describir los comportamientos incriminados de la forma más clara y comprensible posible.

4- Diferenciación de las infracciones de acuerdo con los intereses afectados.

5- Dichas infracciones relacionadas con los ordenadores sólo deberían ser punibles si el autor actúa dolosamente

6- Los delitos menores sólo deberían castigarse a petición de la víctima.

- *Pensamiento universal*. Para la consecución de los fines que le son propios, la cooperación internacional debe ser, valga así la redundancia, lo más «internacional» posible. Se obliga a abarcar el mayor número de Estados y para ello cosechar el mayor número de avenencias, pues de lo contrario, dado el carácter supranacional de los ciberdelitos tantas veces repetido, en muchos casos quedará frustrada su aplicabilidad[71].

- *Límites formales a la cooperación*. La armonización de las normas sustantivas y/o procesales no puede ni debe hacerse a cualquier precio. En este sentido distinguimos en primer lugar el necesario respeto a las normas y tradiciones propias de los Estados y en segundo lugar el respeto a los Tratados Internacionales.

    - En cuanto al primero, ya sea por el diferente sistema jurídico como por la normativa propia de los Estados, se vaticina un dilatado y complejo entramado de distintos ordenamientos a conformar. Por ese motivo se debe prestar especial atención a esa circunstancia, tratando en la medida de lo posible de unificar intereses y lograr el respeto a los diferentes sistemas jurídicos. La aquiescencia es la única forma de unidad.

    - En segundo lugar, el respeto a los Tratados internacionales ya vigentes no tiene siquiera carácter de recomendación, sino de obligación. Especialmente importante en lo relativo a los Derechos Humanos[72].

- *Límites materiales a la cooperación*. Aquí nos referimos, puesto que los delitos informáticos son materia de Derecho Penal, a la mera constancia de los principios base de éste: principio de intervención mínima, principio de *non bis in ídem*, principio de culpabilidad, principio de humanidad de las penas, principio de legalidad, etc.[73].

- *A todos los niveles*. Para la prevención y represión del delito informático es necesaria la participación de todos los sectores de la sociedad. No basta tan sólo con los propios gobiernos o Administraciones. Se requiere la presencia de Organizaciones Internacionales, asociaciones, expertos, empresas, etc. en

[71] A este respecto se han propuesto diversas formas de alivio de los problemas de la internacionalidad de los delitos informáticos. Soluciones aparentes a nuestro entender, pues ninguna de ellas puede encajar correctamente en el plano internacional. Una de ellas es la creación de Tribunales Internacionales encargados especialmente de la represión de la criminalidad cibernética (Herrero Tejedor) y otra la aplicación del principio de jurisdicción universal en la represión de estos delitos, de modo que cualquier Estado puede conocer de ellos, en principio, sin límites. Todas ellas parten de la institucionalización de una «justicia transfronteriza» para el enjuiciamiento de los delitos, pero nos preguntamos hasta qué punto la «universalidad» de éstos justifica la comprometida decisión.

[72] Véase especialmente Declaración Universal de los Derechos Humanos de 1948 (arts. 1 a 11) y el Pacto Internacional de Derechos Civiles y Políticos de 1966 (arts. 1 a 5). Importancia en el aspecto procesal: *«la investigación y enjuiciamiento de los ciberdelitos plantea no pocos problemas relacionados con la posible vulneración de los Derechos humanos [...] posible violación del principio de legalidad, en tanto que garantía de seguridad jurídica para el ciudadano, cuando se persiguen actos lícitos en el lugar de ejecución, pero delictivos en otros países, por la imposibilidad que tiene el ciudadano de conocer la legislación de todos los Estados. La investigación de los ciberdelitos puede entrar en colisión con los derechos a la intimidad o privacidad consecuencia de actuaciones dirigidas a recabar datos sobre los delitos, como la interceptación de las comunicaciones por parte de las autoridades. Asimismo pueden surgir problemas en el momento de su enjuiciamiento, sobre todo relacionados con el derecho de defensa, como por ejemplo cuando se recurre a pruebas basadas en inteligencia.*» [BLANCO CORDERO, ISIDORO, *Taller sobre cibercriminalidad*, I Conferencia Mundial de Derecho Penal, noviembre de 2007, http://www.penal.org/IMG/Guadalajara-cibercrime.pdf]

[73] Límites del *ius puniendi*, MIR PUIG, S, *Derecho Penal: Parte General*, Repertor, Buenos Aires, 2007, págs.104 ss.

definitiva, es tarea tanto el sector privado como el civil, los cuales deben trabajar conjuntamente en aras de resolver problemas que afectan a todos ellos. Salvando las distancias, tomar a ICANN como ejemplo no es tan disparatado como pudiera parecer, dadas las semejanzas existentes, tanto materiales como formales.

- *Regulación coherente y homogénea*. La técnica legislativa aconseja el cuidado en los aspectos formales de una Ley: no contradicción, complitud, estructuración sistemática, lógica normativa, etc. Sin perjuicio de ello, debe tenerse en cuenta una vez más el carácter especial de los delitos objeto de este trabajo. Así las cosas, está fuera de duda que el ámbito de los ciberdelitos está rodeado de un conglomerado de cientificismos, palabras técnicas incomprensibles para el lego. Por ello creemos que se debe predicar en especial la claridad, a fin de la información llegue a la mayor cantidad de personas posible.

- *Respuesta a todos los problemas*. Las inevitables interconexiones existentes en nuestro espacio de análisis no permiten una respuesta parcial. La lógica nos dice que es inexcusable la regulación afín de todos los tipos penales y análogamente de los mecanismos procesales de persecución; la regulación debe tratar de responder a todas las cuestiones planteadas.

- *Transversalidad*. Los delitos informáticos poseen un carácter interdisciplinar mucho mayor del que se piensa. Es por ello que una adecuada ordenación de dichos delitos requiere prestar también atención al resto del ordenamiento jurídico a efectos de mejor conexión y de evitar contradicciones. Así, se plantea la posibilidad de una regulación conjunta de alguno de los problemas que afectan a varias disciplinas[74].

- *Alta negociación*. Se ha visto que la experiencia histórica sitúa los grandes progresos de regulación en materia ciberdelictual en la Unión Europea. Incluso el nuevo convenio sobre cibercriminalidad hecho en Budapest se sitúa en un ámbito similar (sin perjuicio de las posibilidades de adhesión de otros Estados), pues tiene su origen en el Consejo de Europa (recordamos que no es UE). Sin embargo, entendemos para garantizar la universalidad de aplicación que debieran utilizarse las más altas instancias internacionales para este fin, como es Naciones Unidas. No en vano ha ocurrido así con otras cuestiones transnacionales como la esclavitud, la piratería, la trata de personas, el terrorismo o el genocidio.

- *«Pensar globalmente, actuar localmente» y pensamiento realista*. Tras estas máximas, que operarán aquí como cláusula de cierre, queremos señalar que nunca se debe perder de vista la realidad de los hechos; todas las acciones tomadas en el plano legislativo deben poder llevarse plenamente al escenario existente, pero además deben realizarse pensando siempre en las distintas comunidades a las que finalmente va a ser aplicada.

Dicho esto, es conveniente recordar que para construir una adecuada cooperación internacional de cara a la persecución de los delitos informáticos, no basta con el recurso a

[74] Ejemplos a la vista de la existencia de vínculos con otros órdenes distintos del penal son el Derecho Administrativo, especialmente en lo que respecta a la imposición de sanciones cuya entidad no es suficiente como para llegar a la privación de libertad.

Igualmente, en relación con la rama autónoma del Derecho del Consumo existen muy importantes coincidencias con los delitos informáticos debido a la expansión del «*e-commerce*». La comisión de fraudes varios, estafas y otros delitos bajo la apariencia del *comercio electrónico* alcanza en la actualidad cifras preocupantes.

los Tratados Internacionales únicamente. *De lege data* aún hay mucho por hacer; en palabras de F. Höpfel, *«la simplificación y la agilización de la cooperación no tiene lugar, únicamente, mediante la creación de instrumentos nuevos sino [...] en los fundamentos mismos de los órganos de la Administración de Justicia que han de colaborar mediante una infraestructura mejorada para el tratamiento de casos transfronterizos»*[75].

## V. El nuevo Convenio sobre Cibercriminalidad

### V.1. «El Convenio de Budapest»

Llamamos informalmente «Convenio de Budapest» al Convenio sobre la Cibercriminalidad hecho en Budapest, en el seno del Consejo de Europa[76]. Su importancia es tal que este capítulo quinto, que se centra en él, constituye el final de este trabajo, aún más, su terminación natural. El convenio supone en cierto modo la plasmación positivizada de muchas de las ideas aquí vertidas, la mayor maximización de la cooperación en materia de delitos informáticos existente hoy en día en el plano internacional. En efecto, se trata del primer y único instrumento internacional existente hasta la fecha en esta materia, y su auténtica importancia se hará manifiesta a lo largo de este capítulo. Referente a los Estados que forman parte del mismo, a día de hoy[77] tan sólo treinta Estados han ratificado el Tratado, de un total de cuarenta y seis firmas.

Si bien no existen antecedentes normativos directos, ello no obsta para tratar de completar la perspectiva histórica previa al Tratado. Fugazmente, se describirán así los hitos fundamentales en la creación del Tratado. Rodríguez Bernal sitúa el germen del Convenio de Budapest en 1983, año en el que un grupo de expertos se reúne y recomienda a la Organización para la Cooperación y Desarrollo Económico (OCDE) la necesidad de armonización en los delitos informáticos, lo que finalmente se materializa en un informe tres años después[78]. A partir de entonces el Consejo de Europa toma la iniciativa, y ya en 1989 publica la Recomendación nº 89(9)[79], mostrando la clara tendencia que desembocará en Budapest. Posteriormente, en 1997 se inician las negociaciones, largas y complejas, para la elaboración del Tratado propiamente dicho. El Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, influirá decisivamente en el contenido de éste. Llegarán a existir hasta treinta versiones del proyecto para que pudiera ver finalmente la luz, tal era la dificultad que revestía[80]. En 2000 tiene lugar una reunión en Marsella de los ministros de Justicia e Interior de la Unión Europea, donde deciden volcarse en la labor del Consejo de Europa, dejando a éste la elaboración final del Tratado[81]. Finalmente, el comité del Consejo encargado de redactar el proyecto alcanza un consenso y se publica el «Proyecto de Convención sobre el Delito Cibernético» el 27 de abril de 2000;

[75] HÖPFEL, F, *op. cit.*, pág. 236.

[76] Convenio sobre la Cibercriminalidad de 23 de noviembre de 2001 del Consejo de Europa; CETS nº. 185. España lo firmó el 23 de noviembre de 2001, lo ratificó el reciente 3 de junio de 2010, y su entrada en vigor está prevista para el 10 de octubre de este mismo año (2010). En adelante quedará abreviado como «CB.».

[77] 9 de noviembre de 2010

[78] RODRÍGUEZ BERNAL, A, *op. cit.*, pág. 13.

[79] Véase pág. 28 y nota al pie nº 49.

[80] PAVÓN PÉREZ, J, «La labor del Consejo de Europa en la lucha contra la cibercriminalidad», en *Anuario de la Facultad de Derecho*, nº 21, 2003, pág. 194.

[81] MORENÉS, P, «Nuevas tecnologías y seguridad: el Tratado de Budapest, un paso más», en *Economistas*, nº 91, 2002, pág. 377.

éste debería ser finalizado por un grupo de expertos antes de diciembre del mismo año[82]. Sería finalmente aprobado por el Comité de Ministros el 8 de noviembre de 2001, y abierto a la firma en día 23 del mismo mes.

Asimismo, en el proceso de elaboración del convenio han sido de gran influencia algunas recomendaciones del Comité de Ministros del Consejo de Europa y resoluciones del Consejo de Ministros de la Unión Europea, como el propio Tratado asegura[83].

En cuanto a la estructura del Convenio sobre la Cibercriminalidad, éste consta de 48 artículos y un preámbulo inicial. En concreto encontramos hasta cuatro capítulos, divididos en secciones y títulos. El primer capítulo tan sólo comprende un precepto, referido a la terminología usada en el texto. El capítulo segundo «Medidas que deberán adoptarse a nivel nacional», incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad...) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción...). En cuanto al tercero, se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

Obsérvese no obstante que la totalidad del Tratado, en lo que respecta a los preceptos de aplicación material, se puede dividir, conceptualmente, en dos partes bien diferenciadas: Derecho Penal Internacional, constituido por las disposiciones 2 a 13, y Derecho Procesal Penal Internacional, en los artículos 14 a 35. Más adelante se prestará mayor atención al articulado y el mensaje que encierra el texto legal, baste anotar por ahora que la porción relacionada con el Derecho Procesal es cuantitativamente el doble que la sustantiva.

Observando el preámbulo, vemos que se hace eco de todas las ideas vertidas en los primeros capítulos de este trabajo, así, reconoce la necesidad de «*aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional*». También aboga por intensificar la cooperación internacional para «*una lucha efectiva contra la ciberdelincuencia [...] en materia penal reforzada, rápida y operativa*». Igualmente, subraya que «*el presente Convenio pretende completar dichos Convenios* (en referencia a acuerdos de cooperación en materia penal*) con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos...*».

Finalmente, en palabras de Morón Lerma, el Convenio de Cibercriminalidad persigue básicamente tres objetivos en torno a los cuales se estructura, a saber: armonizar el Derecho Penal material, establecer medidas procesales o cautelares adaptadas al medio

[82] ELHADJ MAME GNING, Lex Electronica, vol. 6, n 2, 2001 (en francés) http://www.lex-electronica.org/articles/v6-2/gning.htm

[83] Recomendaciones nº R (85) 10 en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual, nº R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, nº R (95) 4 sobre la protección de los datos personales en el ámbito de las telecomunicaciones, así como nº R (95) 13 relativa a cuestiones de procedimiento penal vinculadas a la tecnología de la información. Igualmente, Resolución nº 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia, que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales y nº 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia, que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Parte en el Convenio. También es destacable a Directiva 2000/31/CE del Parlamento Europeo y del Consejo (8 de junio de 2000), relativa a determinados aspectos de la sociedad de la información.

digital y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional[84].

### V.2. Ajuste en la normativa estatal

El contexto geopolítico español propició que dicho país estuviera presente en el convenio desde sus negociaciones iniciales. Su pertenencia al Consejo de Europa, como Estado miembro, le lleva a firmarlo el mismo día de apertura a la firma, sin embargo su ratificación se ha demorado hasta hace escasos meses: 3 de junio de 2010.

En cuanto a la legislación española, la presencia de delitos informáticos en el Código Penal data de la creación misma del Código Penal, desde 1995. Así pues, desde el «origen» fueron previstas una amplia gradación de conductas que constituyen los tipos informáticos fundamentales hoy en día. Ello no obsta para que se haya propiciado una comprensible evolución, con el fin de adaptar los tipos a los nuevos tiempos, a través de modificaciones legales del Código Penal[85].

Veamos seguidamente cómo se produce el acoplamiento del Convenio sobre la Cibercriminalidad en el ordenamiento español. Primeramente, respecto de la parte de Derecho Procesal Penal presente en el convenio, todos sus preceptos encajan con relativa soltura en el articulado del Código Penal[86]. Excepción quizás supone el artículo 6, referido a la posesión de dispositivos, códigos de acceso o datos informáticos para la comisión de delitos informáticos, así como la producción, venta, difusión, etc., de dichos elementos. Podría considerarse incluido en los artículos 248.3, 270.3 y 400 CP, pero lo cierto es que ni

[84] MORÓN LERMA, E y RODRÍGUEZ PUERTA, M, «Traducción y breve comentario del Convenio sobre Cibercriminalidad», en *Revista de derecho y proceso penal*, nº 7, 2002, pág. 169.

[85] La normativa modificadora de la Ley Orgánica 10/1995 de 23 de noviembre (Código Penal) es la Ley Orgánica 15/2003 de 25 de noviembre y Ley Orgánica 11/1999 de 30 de abril. Es decir, se han modificado estos delitos en el Código, de facto, en 1999 y 2003.

[86] El artículo segundo y tercero del Convenio sobre la Cibercriminalidad se incardinan en el artículo 197 CP *«el que [...] se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación...»*. No obstante, obsérvese que el Código Penal español establece una intención delictiva específica, esto es, *«para descubrir los secretos o vulnerar la intimidad de otro»*, lo cual no supone inconveniente alguno. En cuanto a los artículos 4 y 5 CB., ambos pueden reconducirse al tipo daños informáticos presente en el artículo 264.2 CP *«...al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos»*. Las conductas descritas en el artículo 7 CB. pueden subsumirse en el título XVIII, en concreto arts. 190 ss., relativos a las falsedades documentales: *«alterando un documento en alguno de sus elementos o requisitos de carácter esencial...Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad...Suponiendo en un acto la intervención de personas que no la han tenido [...] Faltando a la verdad en la narración de los hechos»*. El artículo 8 CB. queda divido en dos apartados. El apartado «a» entra dentro del citado 264.2 CP. Por su parte, el apartado «b» queda contenido en 248.2 CP *«...los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero»*. Por su parte, nuestra opinión es que el artículo 9 CB. se ensambla a la perfección en el artículo 189 del Código Penal: *«el que utilizare a menores de edad [...] para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades...El que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad....El que [...] posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad... el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada»*. Tampoco plantea problema alguno el artículo 10 CB., que se reconduce a los artículos 270 a 272 CP, cuya conducta principal está contenida en art. 270.1*«...quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios»*. No encontramos obstáculo asimismo en relación al artículo 11 y 12 CB., cuyas previsiones pueden alinearse a lo largo del libro I del Código Penal. En concreto, sin ánimo de exhaustividad: arts. 15 y 16 (complicidad), arts. 27 y 28 CP (tentativa) y art. 31 (responsabilidad).

siquiera existe coincidencia parcial. No alcanza ni al delito de daños ni al de interceptación. Sin embargo, según parece, eso no ha sido obstáculo para la ratificación del convenio por España, sin reservas, lo que es, desde nuestro punto de vista, ampliamente criticable.

En cuanto a la parte de Derecho Procesal Penal, presente en el convenio, su encaje en el sistema español no provoca conflictos significativos. De este modo, respecto de los artículos 16 a 21 CB., relativos a los datos informáticos, éstos no generan mayores problemas, siempre que se tenga en cuenta que estas «autoridades» que ordenan conservar los datos, deben ser, obligatoriamente, judiciales (ex. Art. 18.3 Constitución Española y STC 114/84 entre otras). Los artículos 299 ss. de la Ley de Enjuiciamiento Criminal regulan el procedimiento de la instrucción, previendo el uso de medidas cautelares como las que indica el convenio. Las garantías de los artículos 14 y 15 y 28 CB. se pueden enmarcar dentro de los citados artículos y la Ley de Protección de Datos de Carácter Personal[87]. El artículo 22 CB., referido a la jurisdicción, es totalmente compatible con el ordenamiento español, pues los principios de atribución de competencia están contenidos en los artículos 23.1 y 23.2 de la Ley Orgánica del Poder Judicial. Lo mismo puede decirse del artículo 24 CB., relativo a la extradición (arts. 824 ss. LECrim. así como lo relativo a la Euroorden). En cuanto a los artículos 25 a 27 y 29 a 35 CB., consideramos su adecuación al ordenamiento español, sin ser necesarias mayores aclaraciones. Por último, tampoco generan mayores problemas las cláusulas finales de los artículos 36 ss. CB.

### V.3. La satisfacción de las necesidades de cooperación internacional del ciberdelito por el Convenio sobre Cibercriminalidad

En este punto se intentará realizar una visión crítica del texto del Tratado, tenidas en cuenta las recomendaciones sostenidas anteriormente. Esto es, trataremos de responder al interrogante de si realmente es el Convenio sobre la Cibercriminalidad la norma que estábamos esperando para solucionar la problemática de los delitos informáticos. Para llevar a cabo esta tarea, es imperativo realizar primeramente un pequeño análisis del convenio según la reiterada distinción entre Derecho Penal Internacional y Derecho Procesal Penal Internacional.

De este modo, la llamada a la tipificación de determinadas conductas, visible en la primera decena de artículos, supone un enorme paso hacia la armonización del Derecho sustantivo de los Estados parte. Éste, dijimos, es un movimiento fundamental en la lucha contra el ciberdelito, permitiendo aunar los criterios punitivos en torno a dichas conductas. Igualmente, el Convenio sobre la Cibercriminalidad se define por una verdadera plasticidad en los mandatos a los Estados; mantiene abiertas las posibilidades de punición, permitiendo así la aplicación flexible de los tipos. Ello permite trabajar en pos de una lucha común, castigando similares conductas, pero a la vez respetando el ordenamiento jurídico propio de los Estados. Mediante la aludida naturaleza dúctil de los tipos y la utilización de reservas, bajo expresiones del tipo «*cualquier Parte podrá exigir*» o «*cualquier Parte podrá reservarse el derecho*», el Convenio sobre la Cibercriminalidad crea un sistema, no exento de complejidad, que a priori garantiza la conciliación con los más diversos sistemas jurídicos.

Por otro lado, la transversalidad a otras ramas del ordenamiento, más allá del meramente penal, queda patente desde la relativización de las medidas que deben tomar los Estados («*legislativas y de otro tipo*»), así como por la apertura a la responsabilidad administrativa (véase art. 13 CB. para personas jurídicas), lo que redunda en un tratamiento global de la ciberdelincuencia, y en ocasiones, más coherente. En cuanto a la complitud del contenido material del Tratado, no han faltado ciertas posiciones críticas que han afirmado que falta contemplar la problemática de la explotación sexual de la infancia en la Red y la

[87] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

incriminación de actos de naturaleza racista y xenófoba cometidos a través de los sistemas informáticos[88]. Referente a este último, se enmendó la situación a través de un Protocolo adicional[89].

También en relación con esta primera parte del convenio, con las acciones concretas que se tipifican, no podemos dejar de resaltar dos importantes aspectos. El primero de ellos tiene que ver con la problemática de la incriminación de la posesión de programas o datos. Se entra así en terrenos peligrosos, pues no siempre se infiere de la posesión una finalidad estrictamente delictiva. Al respecto, el artículo 6, en su inciso *1.b* contempla la punición de la posesión de dispositivos, códigos de acceso o datos informáticos para la comisión de delitos informáticos. Dada la controversia existente al respecto, así como la variada legislación en los países firmantes, el Tratado permite a los Estados aminorar el ámbito de lo punible en lo concerniente a la posesión, permitiendo que se pueda «*...exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal*».

En el mismo sentido encontramos el artículo 9, relativo a la pornografía infantil. No sólo llama a la punición de la venta, difusión, oferta, puesta a disposición, etc., de pornografía, sino que además establece el castigo de la posesión de datos relativos a ella. Como en el caso anterior, reconoce igualmente el derecho de los Estados a reservarse la aplicación de las partes conflictivas. Al respecto, España sigue desgraciadamente el modelo de la sanción de tenencia privada.

A pesar de la posibilidad de establecer reservas en estos puntos, es del todo criticable la configuración en el texto de la punición de la mera posesión de datos informáticos, expandiendo injustificadamente el Derecho Penal y atentando contra sus principios fundamentales. Especialmente reprochable en el caso de la pornografía infantil, ya que mientras que en el artículo 6 CB. se exige una finalidad especial «*...con el fin de que sean utilizados* (los datos) *para cometer cualquiera de los delitos previstos...*», en el caso del artículo 9 CB., bastaría la mera tenencia para disfrute privado para constituirse en delito. En este sentido coincidimos con la mayor parte de la doctrina española, que aboga por la destipificación de la mera posesión, por no escasas razones[90].

En el capítulo tercero ya se puso en evidencia la necesidad de mantener un equilibrio entre el respeto a los derechos individuales y el uso de la violencia estatal representada por el Derecho Penal[91]. En esta «batalla», nos situamos en el mismo centro ideológico, afirmando la necesidad de proteger ciertas realidades surgidas de las nuevas tecnologías, y a su vez avalando las garantías innegables de los ciudadanos. Con la modernidad, particularmente en relación con los delitos informáticos, se impone irremediablemente la necesidad de proteger nuevos bienes jurídicos, o de ampliar la protección de éstos, si pueden quedar indefensos ante las nuevas circunstancias económico-sociales-tecnológicas. Es pues inevitable que exista una cierta expansión del Derecho Penal. Ahora bien, introducida la racionalidad en el sistema, el proceso pasa por una «expansión razonable», garantizando los derechos de los individuos y utilizando los instrumentos

[88] PAVÓN PÉREZ, J, *op. cit.*, pág. 203.

[89] Tras poco más de un año de vigencia del Convenio sobre cibercriminalidad, el Consejo de Europa alumbra el Protocolo Adicional relativo a la incriminación de actos de naturaleza racista y xenófoba cometidos a través de los sistemas informáticos de Estrasburgo, abierto a la firma el 28 de enero de 2003. Se halla actualmente firmado y ratificado por tan sólo 17 países, entre los que no se encuentra España.

[90] Especialmente; ESQUINAS VALVERDE, P, «El tipo de mera posesión de pornografía infantil en el Código Penal Español: Razones para su destipificación», en *Revista de Derecho Penal y Criminología*, 2ª época, nº18, 2006, págs. 225 ss.

[91] Tradicional discusión entre Derecho Penal mínimo y máximo; FERRAJOLI, L, *Derecho y Razón: teoría del garantismo penal*, Trotta, Madrid, 1995, págs. 105 ss.

penales sólo en lugares indispensables[92]. En este marco, la tipificación de conductas como la mera posesión de datos informáticos antes aludida hace pecar al Convenio sobre la Cibercriminalidad de participar en una desmesurada expansión del_Derecho Penal hacia órbitas que sobrepasan lo estrictamente necesario.

El segundo aspecto a destacar es el referido al artículo 12 del Convenio de Cibercriminalidad, que se refiere a la responsabilidad de las personas jurídicas. Recordando lo que se dijo *supra* [cap. III, epg.1, apr. d)], así como la confusión existente en la materia, afirmamos que el convenio apenas introduce claridad al respecto. No se refiere directamente a la responsabilidad de las personas físicas que estén al cargo de la persona jurídica y además permite a los Estados decidir la entidad de dicha responsabilidad: penal, civil o administrativa. Por este motivo no proporciona ningún añadido de entidad que permita unificar criterios normativos al respecto[93].

En cuanto a la parte de Derecho Procesal Penal Internacional del convenio, constituida por las disposiciones 14 y siguientes, son varios los ítems a destacar. El artículo 22 del convenio se refiere a los problemas de la jurisdicción, de forma que sirve para unificar criterios, al menos parcialmente, al afirmar el principio de territorialidad y el de personalidad para todos los Estados. Sin embargo, como ha indicado parte de la doctrina, serán muy frecuentes los supuestos en que varios tribunales disputen el conocimiento de una causa, debido al mantenimiento de la concurrencia de varios criterios de atribución competencial sin establecer criterios de prelación ni otros sistemas de prioridades[94].

Los artículos 16 a 21 se refieren a la preservación de determinados datos informáticos, medidas procesales tendentes sin duda a la agilización de los trámites y la conservación de información fundamental en torno al ilícito. En concreto, se prevé *«la conservación rápida [...] cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación»* (art. 16 CB.), *«la revelación rápida a la autoridad competente»* (art. 17 CB.), la orden a personas o ISP de comunicar datos relevantes (art. 18 CB.), disposiciones de agilización de registro y confiscación de datos (art. 19 CB.), obtención de datos sobre el tráfico (art. 20 CB.), y la interceptación, para «delitos graves», del mismo contenido de las comunicaciones (art. 21 CB. [95]). Como se observa, se apuesta primordialmente por la rapidez, creando métodos tendentes a la recolección de evidencias para la persecución de los delitos informáticos, algo que es plausible desde el punto de vista de la eficacia policial. Por su parte, los artículos 29 a 34 CB. también se refieren a los datos informáticos, pero esta vez desde una concepción más amplia de cooperación internacional. Se prevén solicitudes de conservación rápida de datos (art. 29 CB.), solicitudes de revelación de datos (art. 30 CB.), solicitudes de obtención o confiscación (art. 31 CB.), acceso libre a datos de fuente abierta (art. 32 CB.) y asistencia mutua para obtención de datos sobre el tráfico e interceptación de comunicaciones (arts. 32 y 33 CB.).

---

[92] SILVA SÁNCHEZ, J, *La expansión del Derecho penal: Aspectos de la política criminal en las sociedades postindustriales*, Civitas, Madrid, 2001, pág. 26.

[93] SILVA SÁNCHEZ, J, «La responsabilidad penal de las personas jurídicas en el convenio del Consejo de Europa sobre cibercriminalidad», en *Cuadernos de derecho judicial*, nº 9, 2002, págs. 133 y 134. El autor aduce *«...dos problemas fundamentales. De entrada, es un modelo formalista, y refleja mucho más el tener de un modelo de responsabilidad civil que penal. [...] Pero es que, además, se suscita la cuestión de si es razonable establecer un modelo único de imputación de responsabilidad a la persona jurídica, dejando simultáneamente abierta la posibilidad de que ésta se configure, en función de la tradición jurídica de cada país...».*

[94] GONZÁLEZ LÓPEZ, J, *La respuesta procesal a la delincuencia informática: especial atención al convenio sobre el cibercrimen*, Noticias Jurídicas publicación electrónica, 2003. http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200309-57551198103225 11.html

[95] Igualmente, nos resulta extraño que el artículo 8 CB. obligue especialmente a los Estados a idear medidas encaminadas a grabar el contenido de determinadas comunicaciones sólo para «delitos graves», sin expresar qué se debe entender por éstos, y dejando a los Estados su concreción. Ello puede llevar a la inaplicabilidad práctica de este precepto, o a su vaciamiento, por las disímiles interpretaciones a que puede dar lugar.

Se evidencia que el convenio ha dedicado gran parte de su texto a la previsión de lo relacionado con los datos informáticos, reconociendo así su importancia en la lucha policial y procesal contra el cibercrimen. Sin embargo, se debe poner de manifiesto la imperante necesidad de conjugar esta colaboración con la protección del derecho a la intimidad y la confidencialidad de ciertos datos. El Grupo de Trabajo sobre Protección de Datos de Unión Europea ya puso de manifiesto la redacción «*con frecuencia demasiado vaga y confusa*» del proyecto de convenio que tuvo que analizar, fórmula que desgraciadamente se repite en la versión final[96]. Si bien se incluyó un artículo 28, relativo a la «*confidencialidad y restricción de la utilización*» de datos, el panorama aún no está claro. Hubiera sido muy interesante, en aras de una mayor garantía de la protección de datos, haber obligado a los países firmantes no pertenecientes al Consejo de Europa la subscrición de Convenio 108 del Consejo o establecer la «*...incriminación por infracción de las normas en materia de protección de datos*», en palabras del citado grupo de trabajo[97]. Desde otra perspectiva, se critica que el convenio no haga referencia a la necesidad de autorización judicial, cuando la injerencia en los datos personales por parte de las autoridades estatales supone una clara intromisión en la esfera privada de los derechos, siendo necesaria una resolución judicial motivada[98]. En cualquier caso, queda fuera de duda la repercusión que muchos de los preceptos del convenio tienen para los Derechos Humanos, especialmente en lo que respecta a la intimidad y la protección de datos. Por ese motivo, dadas las múltiples imprecisiones del convenio, es necesario prestar especial atención a la hipotética vulneración de los derechos individuales, rodeando todo el proceso de las adecuadas garantías presentes en las legislaciones autónomas de los Estados, así como las consagradas internacionalmente y en los Tratados de Derecho Humanos.

Precisamente el propio Convenio sobre cibercriminalidad afirma velar y proteger los Derechos Humanos. Verbigracia el preámbulo afirma la «*...necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en [...] Tratados internacionales aplicables en materia de derechos humanos...*» y por su parte el artículo 15 CB. asevera que «*...el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos...*». Sin embargo, parte de la doctrina considera que tan sólo se trata de «prometedoras frases», que en modo alguno garantizan los derechos individuales. Se ponen así en tela de juicio la proporcionalidad de las medidas de investigación y control del convenio, afirmando que no se garantizan los derechos de los ciudadanos[99].

El artículo 24 CB. se refiere a la extradición, remitiendo en primer lugar a otros Tratados de extradición existentes previamente entre las partes, y supletoriamente, aplicando el Convenio de Cibercriminalidad en lo concerniente a los delitos determinados en la primera decena de artículos. De este modo se establece el marco para garantizar bien el juzgamiento de los sospechosos, bien la ejecutividad de las sentencias en esta materia, siempre bajo el cumplimiento de ciertos requisitos, por lo que no existen en principio objeciones al respecto.

[96] Dictamen 4/2001 acerca del proyecto de convenio del Consejo de Europa sobre el ciberdelito, 5001/01/ES/Final WP 41, 22 de marzo de 2001.

[97] Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

[98] GONZÁLEZ LÓPEZ, J, *op. cit.* Igualmente, el autor critica «*... que estas medidas ofrecen importantes dudas acerca de su legitimidad dada [...] su carácter indiscriminado en cuanto a los sujetos pasivos de la medida (ya que no se especifica que quienes deban padecer la retención de sus datos se individualicen en virtud de la existencia de un procedimiento penal en el que se hallen involucrados), la ausencia de procedimiento penal en curso y el excesivo alcance de la medida para un propósito que se podría obtener a través de otras medidas*».

[99] SÁNCHEZ BRAVO, A, «El Convenio del Consejo de Europa sobre cibercrimen: control vs. libertades públicas», en *Revista jurídica española de doctrina, jurisprudencia y bibliografía*, nº 3, 2002 , págs. 1856 y 1857.

Los artículos 25 a 27 establecen las bases para la cooperación y ayuda entre los Estados (asistencia mutua), así como intercambio de información y fijación de autoridades de contacto, para llevar a cabo las investigaciones y recolección de pruebas. Por su parte, el artículo 35 CB. manda designar a cada parte «*...un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito...*», esto es, establece una red 24/7 de la misma forma que señalábamos en [cap. IV, epg.5, apr. a)]. Al respecto, celebramos dichas previsiones, pues sin lugar a dudas permitirán avanzar hacia una adecuada lucha contra la ciberdelincuencia, haciendo mucho más eficaz la labor policial en la represión de estos delitos. Como contrapunto, tal como se decía respecto al tráfico de datos, será necesario velar por la adecuada protección de los Derechos Humanos en el curso de las investigaciones.

Por último, respecto de las disposiciones finales del Tratado, arts. 36 a 48, éstas constituyen, en su mayor parte, cláusulas generales de los Tratados internacionales elaborados en el seno del Consejo de Europa, por lo que entrará en su concreción[100]. No obstante es de subrayar el art. 46 CB., el cual previendo una vez más la importancia de la constante comunicación y circulación de información, señala la importancia del «*...intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico*» entre los Estados.

En cuanto a la extensión del Convenio sobre Cibercriminalidad, aun tratándose del ámbito del Consejo de Europa, es posible su ratificación por otros Estados (ex. Art. 37 CB.), lo que permite así caminar hacia el nivel de «internacionalidad» necesaria. No obstante, no debemos engañarnos; sin perjuicio de una futura adhesión de nuevos países, a pesar de existir una hipotética «apertura mundial» del Tratado, tan sólo constan treinta ratificaciones hasta el día de hoy, cantidad totalmente insuficiente para garantizar una adecuada respuesta mundial frente al ciberdelito. Será necesario a este respecto implementar mecanismos extra convencionales para facilitar y alentar a la adhesión a dicho texto.

Recapitulando, no son pocos los deslices en los que incurre el Convenio sobre Cibercriminalidad del Consejo de Europa. Desde desaciertos en el articulado hasta potenciales complicaciones de mayor calado en materia de derechos. Pero dichas máculas no vician el resto del Tratado, y no deben desmerecer la importancia que supone la norma tanto en el plano nacional como internacional. Su aparición ha permitido iniciar el decisivo camino hacia la ansiada armonización de los tipos penales ciberdelictuales y la apropiada instrumentalización de las normas procesales y de la colaboración policial en aras de la lucha contra el ciberdelito, especialmente en lo relativo al intercambio de datos e información. Desde el primer momento se puso de manifiesto la necesidad del recurso a la cooperación internacional en el plano de los delitos informáticos. Desde esta perspectiva, el Convenio sobre Cibercriminalidad, única norma internacional en la materia, se nos presenta como un instrumento adecuado para cumplir la función que le ha sido conferida, a pesar de sus problemas y del ingente trabajo que todavía queda por delante.

### V.4. Perspectivas futuras

Una sociedad tan cambiante como en la que vivimos, especialmente en lo que respecta a las nuevas tecnologías, nos hace difícil predecir con exactitud qué ocurrirá en el futuro. Sin embargo, hay algo que sí podemos aventurar, dada la tendencia irrefrenable que muestra la tecnología y el gran acogimiento por parte de la población de las nuevas TIC's.

[100] PAVÓN PÉREZ, J, *op. cit.*, pág. 195.

La aparición de nuevos dispositivos con acceso a la Red, la reducción de la *brecha digital* y el imparable crecimiento de Internet son hechos irrebatibles. El aumento del número de delitos informáticos, como se dijo al principio, también. Así las cosas y, aún más teniendo en cuenta la capitalidad de la cooperación internacional como única solución viable por la afección simultánea de diversas jurisdicciones, no es atrevido pronosticar la tendencia a la inclusión de nuevos Estados en el Convenio sobre Cibercriminalidad.

La propensión a la cooperación no es ilusoria: cada vez hay más países interesados en formar parte del convenio, cada vez mayor cantidad de Estados reforman su Código Penal introduciendo las infracciones informáticas, progresivamente desaparecen los «paraísos ciberdelictuales» y en definitiva, sucesivamente más gobiernos se dan cuenta de la verdadera necesidad de actuar en esta materia. Es pues, no sólo necesario sino gradualmente perceptible, el aumento de la participación en el citado convenio; así se observa en los numerosos esfuerzos a nivel internacional, por parte de diversas Organizaciones Internacionales y Estados, para favorecer la adhesión al Tratado. Verbigracia la 6ª Conferencia Internacional sobre Ciberdelincuencia de Interpol, que recomienda «*que se utilice el Convenio sobre Ciberdelincuencia del Consejo de Europa como referencia en materia de normas internacionales procedimentales y legales mínimas para la lucha contra la ciberdelincuencia...*» instando posteriormente a los Estados a subscribirlo[101]. Del mismo modo, observamos la conferencia titulada «La Cibercriminalidad: un desafío global, una respuesta mundial», la cual tenía por objeto promover la adhesión al convenio entre los Estados americanos, animando encarecidamente «*...a considerar la posibilidad de formar parte de este convenio a fin de utilizar las leyes y los instrumentos eficaces y compatibles para luchar contra la cibercriminalidad...*»[102].

Todas estas manifestaciones que contribuyen indudablemente a garantizar la «internacionalidad» del Tratado debemos verlas con buenos ojos. Por otro lado, también podemos prever posteriores modificaciones del Convenio sobre Ciberdelincuencia, conforme al transcurso de la tecnología y la evolución de los delitos, especialmente en lo que respecta a la inclusión de nuevas infracciones, como ya ocurrió con los actos de naturaleza racista y xenófoba. Resumiendo, movidos por la apremiante necesidad de cooperación internacional en materia ciberdelictual, cada vez más Estados apuestan por refrendar una concurrencia homogénea de normas en esta materia mediante el convenio del Consejo de Europa. En definitiva, el futuro pasa por una mayor cooperación e integración normativa, que en la Unión Europea puede alcanzar una nueva dimensión con la reciente propuesta del Parlamento Europeo de creación de un Tribunal Europeo de Asuntos Informáticos, especializado en cuestiones relacionadas con los delitos informáticos[103].

[101] 6ª Conferencia Internacional sobre Ciberdelincuencia El Cairo (Egypto), del 13 al 15 de abril de 2005. http://www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/ResolutionEs.asp

[102] «La Criminalidad: un desafío global, una respuesta mundial» Casa de América, Madrid, España, 12 y 13 de diciembre de 2005. http://www.coe.int/t/e/legal_affairs/about_us/cooperation/CYB%2 0_2005 _%20Conclusions%20ESP.pdf

[103] Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos • Programa de Estocolmo», 18 de noviembre de 2009, apartado R.