# REFLEXIONES SOBRE LA CIBERDELINCUENCIA HOY (EN TORNO A LA LEY PENAL EN EL ESPACIO *VIRTUAL*)

Mariluz GUTIÉRREZ FRANCÉS

PROFESORA TITULAR DE DERECHO PENAL
UNIVERSIDAD DE SALAMANCA

**s u m a r i o**

I. Aproximación al tema: hacia un nuevo enfoque de la Ciberdelincuencia. II. Problemas de aplicación de la ley penal en el espacio virtual. III. Iniciativas para una actuación globalizada contra la Ciberdelincuencia transnacional. 1. Medidas e iniciativas internacionales para combatir la criminalidad informática en la esfera internacional mundial. 2. Medidas en el ámbito del Consejo de Europa. 3. Medidas en el marco de la Unión Europea. IV. A modo de conclusión (de vuelta al Derecho penal español).

## I. Aproximación al tema: hacia un nuevo enfoque de la Ciberdelincuencia.

Al tiempo de cerrar estas páginas, antes de proceder a su envío (*electrónico*) para su publicación (también *electrónica*) en la *Revista electrónica* de la Facultad de Derecho de la querida Universidad de La Rioja, encuentro en Internet la siguiente noticia:

> Un joven español de dieciocho años ha sido detenido en Málaga el pasado 13 de enero por la Unidad de Ciberdelincuencia de la Guardia Civil, dentro del marco de la «Operación *Navy*», instada por el Servicio de Investigación Criminal Naval del Departamento de Defensa de los Estados Unidos. Al parecer, al joven se le imputa el haber dañado gravemente el funcionamiento y la seguridad de un dique seco de mantenimiento de submarinos nucleares, al haber accedido subrepticiamente por Internet a los ordenadores de la base naval de Point Loma, San Diego. En la investigación fueron detenidas otras cuatro personas más acusadas de haber comprometido la seguridad de un centenar de sistemas informáticos, provocando daños superiores a cuatrocientos mil euros.

Aunque aún parecen provocar cierta alarma social y perplejidad, noticias como esta han dejado de sorprenderme tras casi media vida ocupándome de los problemas de la llamada «Criminalidad informática». Cada vez es más frecuente hallar en la página de sucesos algún hecho ilícito, por lo general de dimensión espectacular, en el que esté presente, de algún modo, el uso abusivo o pervertido de las altas tecnologías de la información. (Sin necesidad de retrotraernos más allá de la última semana, por citar sólo otro ejemplo, seguro que aún sigue en el recuerdo de todos la reciente desarticulación por la Policía española de una red de tráfico de pornografía infantil a través de Internet)[1]. Sin embargo, por tentador que resulte prolongar el listado de supuestos con que ilustrar estas páginas (hoy ya no tendríamos que irnos más allá de nuestras fronteras para encontrarlos), creo preferible a estas alturas, con la perspectiva que nos ofrecen dos décadas de historia, plantear de partida una serie de reflexiones:

1º. Eran ciertas las palabras de TIEDEMANN[2] cuando advertía en los años ochenta que la criminalidad mediante computadoras no es un fenómeno genuino y exclusivo de las sociedades más evolucionadas o con un mayor desarrollo económico, tecnológico o industrial, sino que surge en todo entorno que se haya incorporado a la «era de la informática». Y si esta afirmación ya era cierta entonces, con mayores argumentos lo es a principios del siglo XXI, en pleno proceso de *globalización*. Es verdad que hasta fechas muy próximas sólo se descubrían casos en aquellos países más sensibilizados y con mayores y mejores medios para su adecuada investigación[3], (los más desarrollados, claro está). Sin embargo, en la actualidad, no es infrecuente que algunas de las redes internacionales de criminalidad a través de Internet posean importantes conexiones con países menos desarrollados (bastante habitual en supuestos de pornografía infantil, como el citado en el párrafo anterior). En suma, estamos ante una materia que concierne a toda la Comunidad internacional. Todos los países están de algún modo involucrados, sin excepción.

2º. Por lo mismo, cabría afirmar que todos y cada uno de nosotros, individual o colectivamente, estamos implicados en el «gremio de afectados». Ninguno de los ciudadanos de una sociedad incorporada al tren de la *era digital* puede considerarse «no aludido» en este tema. (En la medida en que realizamos todo tipo de actividades usuales como adquirir bienes en supermercados que fijan sus precios en códigos de barras, es decir, electrónicamente, por ejemplo, podemos ser víctimas de fraudes informáticos; en la medida en que usamos teléfonos con tarjetas electrónicas, eventualmente podemos ser víctimas de manipulaciones en las mismas para que se nos cargue mayor costo en cada llamada; en la medida en que usamos Internet, podemos estar siendo víctimas de programas espías contra nuestra intimidad, o podemos sufrir las consecuencias de un *virus* informático que dañe

[1] La detención de más de treinta personas, entre ellas, maestros, médicos, educadores, sacerdotes, etc., ha generado gran desasosiego a la sociedad: se empieza a sentir que cualquier ciudadano, aparentemente honesto y bien integrado socialmente, (aquel que contacta a diario con nuestros hijos en clase o en la catequesis...), puede aparecer eventualmente implicado en una de estas noticias. Como quiera que en los últimos meses se han producido varias operaciones policiales de índole similar (todas ellas, exitosas operaciones de las Brigadas de Delitos Tecnológicos de la Policía Judicial en cooperación con las Policías de otros Estados).

[2] TIEDEMANN, *Poder económico y delito*, trad. Mantilla Villegas, Ariel, Barcelona, 1985, p. 121.

[3] Baste recordar que prácticamente todos los primeros casos detectados procedían de los Estados Unidos y Alemania. Vid los primeros estudios comparados de SIEBER, a quien con todo merecimiento cabe atribuir un extraordinario protagonismo en las iniciativas para la armonización internacional en materia de criminalidad informática. Por todos, cfr. *The International Handbook on ComputerCrime,* John Wiley & Sons, Chichester, N.Y., Brisbane, 1986, por todos si bien el propio autor ha seguido recopilando esta clase de información ampliando la muestra de Estados. Vid. *Computer Crime and Criminal Information Law. New Trends in the Internatinal Risk and Information Society,* publicado en la p. Web de la Universidad de Wüerzburg en 1998, con actualizaciones posteriors: \www.jura.uniwüerzburg.de\sieber.

todo nuestro sistema, o destruya nuestra valiosa información... etc.) Y, lo más grave es que podemos estar siendo la víctima en este instante de un ilícito mediante el uso abusivo de la modernas tecnologías, e ignorarlo absolutamente (en este mismo momento alguien puede estar entrando electrónicamente en nuestra historia clínica informatizada, incluso cambiando datos de la misma en nuestro perjuicio, y no podemos saberlo; por no mencionar fraudes informáticos a los consumidores ya conocidos, como el de las gasolineras, que nunca llegaremos a saber si estuvimos o no entre el grupo de afectados). En resumen, urge superar viejos tópicos sobre los *autores* y las *víctimas* de la criminalidad informática. Las víctimas no lo son sólo las grandes empresas multinacionales, bancos, Administraciones Públicas. Lo somos cualquier ciudadano, consumidor y usuario habitual de la sociedad actual.

3º. Ahora que ya hemos comprobado que el uso perverso de las tecnologías de la información puede servir a delitos de muy diversa índole, cuando la experiencia tristemente no ha puesto de relieve que no exageraba BEQUAI al decir que todos los delitos, a excepción de algunos especialmente violentos, como la violación, pueden cometerse sobre o por medio de la Informática, es hora de replantearse si tiene sentido seguir abordando esta materia como algo excepcional, con sustantividad propia y en los términos en que se planteaba hace dos décadas en los primeros estudios sobre *Computercrime*. (En tal sentido, después de leer algunos de los casos de asesinato por medio de manipulación informática de programa de una aeronave, por ejemplo, recogidos por el autor citado, sorprende que todavía en el año 2000, en la reunión de París del Grupo de los Ocho, sólo se advirtiese como una «posibilidad» de futuro que un *terrorista mate a través de la pantalla de un ordenador*[4]. Con toda evidencia no estamos ante un *futurible*, y así se explica que la criminalidad vía Internet se la considere como la «tercera gran amenaza para las potencias, después de las armas químicas, las bacteriológicas y nucleares»[5]).

4º. Sin ninguna duda, hemos integrado en la cotidianeidad de nuestras vidas la *computer dependency*[6], pero, del mismo modo, también «lo informático» se ha incorporado a la *normalidad* del comportamiento criminal actual, abriendo un extraordinario abanico de posibilidades al delincuente (facilita, agiliza la comisión de hechos ilícitos, favorece su ocultación y la expansión ilimitada de sus efectos, sin olvidar las dificultades para su persecución). Y si el reto que tuvieron que afrontar inicialmente los ordenamientos jurídicos en su conjunto y, de modo especial, la esfera penal, fue el de modernizarse para encauzar una nueva realidad (regulando, desde las diversas parcelas jurídicas concernidas, los aspectos conflictivos y hasta entonces desconocidos que generaba la irrupción de la Informática en prácticamente todas las dimensiones de nuestra vida)[7], al tiempo presente, sin embargo, conviene reconducir el problema a sus justos términos. A mi modo de ver, el gran reto del Derecho Penal ante las altas tecnologías de la información ahora, superados en gran medida retos previos, viene a conectar con lo verdaderamente genuino y específico que en la actualidad comporta su uso ilícito. Me estoy refiriendo, claro está, al proceso de transnacionalización de la delincuencia que la revolución cibernética ha propiciado, con una singularidad de nuevo cuño: sus más graves manifestaciones tienen lugar en un nuevo ámbito espacial, el *espacio virtual*. A poco que se observe la realidad, se coincidirá conmigo en que, más allá de lo afortunado que haya estado el legislador en la aprehensión en

[4] Cfr. el trabajo Rómulo DE ANDRADE MOREIRA, «Globalización y crimen», publicado en http://revistapersona.4t.com/13Moreira.htm.

[5] *Ibidem*.

[6] En este sentido ya me pronunciaba desde mi trabajo *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, pp. 621 ss.

[7] Sobre los diversos «modelos» de adaptación legislativa a una realidad para la que no había previsión en las legislaciones tradicionales, vid. GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, cit., pp. 119 ss.

Derecho positivo de todas o algunas de las «modalidades *informáticas*» de algunos delitos, una tarea crucial pendiente hoy, fruto del gran impacto tecnológico en la esfera penal, es *la investigación, prueba, persecución y aplicación de la ley penal a la delincuencia informática transnacional que se proyecta, se desarrolla y expande sin límites sus efectos en el Ciberespacio*.

En suma, sin cuestionar el interés que puedan seguir ofreciendo otras perspectivas de análisis de la «Criminalidad mediante el uso pervertido de la Informática», de las que, por lo demás, he tenido ocasión de pronunciarme en otras sedes, las próximas líneas las pretendo orientar al examen de los **problemas de aplicación de la ley penal a las manifestaciones criminales cometidas en el *Ciberespacio***.

Ya en los primeros estudios sobre *Delincuencia informática*, hace casi dos décadas (PARKER, NYCUM o BEQUAI, en los años setenta del siglo pasado)[8], se apuntaba el riesgo que podía representar el uso pervertido de las altas tecnologías de la información, al posibilitar la separación espacio/temporal de hechos ilícitos y resultados (aspecto que facilitaba la comisión y suponía un obstáculo adicional para su detección, prueba y persecución). Casos célebres, como el llevado a cabo desde Alemania por el llamado *Chaos Computer Club*, sirvieron entonces para poner de relieve que el problema (en aquel supuesto, *hacking* o intrusismo informático en los sistemas de la NASA por un grupo de jóvenes desde Alemania, conductas de espionaje y fraude postal a distancia) era particularmente grave cuando los hechos adquirían una dimensión transnacional, posibilidad que aún parecía, no obstante, bastante remota y excepcional.

Sin embargo, la vertiginosa implantación mundial y la evolución de los sistemas de almacenamiento, tratamiento, proceso y transmisión electrónica de información y de datos han transformado ese potencial peligro en una inquietante realidad de consecuencias imprevisibles. Hoy se coincide en afirmar que el *Cibercrimen* se mueve en la práctica impunidad de un *espacio virtual* y sin fronteras, el espacio que suministra Internet, la Red de redes[9]. Los intentos en la Comunidad internacional orientados a aprehender el *Computercrime*, en sus inicios[10] no excedieron de la «encarecida recomendación» a los Estados para que adaptasen sus legislaciones internas a fin de evitar lagunas de impunidad y la aparición de «paraísos informáticos». Pues bien: la sola armonización legislativa, al tiempo de escribir estas líneas, se muestra claramente insuficiente. Lo que en realidad se impone es la superación efectiva de las fronteras nacionales para la represión, con un mínimo de eficacia, de esta clase de delincuencia (hasta ahora sólo han representado un serio obstáculo), preservando cuotas irrenunciables de soberanía de los Estados, y sin sacrificar, con la coartada de la *seguridad*, las más elementales garantías individuales. Este es, a mi juicio, el ambicioso proyecto que la sociedad moderna globalizada tiene ahora pendiente.

En dicha línea se está trabajando desde el Consejo de Europa, con particular reflejo (aunque no sólo, como se verá) en el Convenio sobre *Cibercrimen*, de 23 de noviembre de 2001, con un Protocolo Adicional de enero de 2003, donde se prevén una serie de medidas para la cooperación internacional en dicha materia. No obstante, los pasos más serios se

[8] El primer estudio, de carácter criminológico, es de sobra conocido, la famosa monografía de PARKER, *Crime by Computer*, Charles Scribner's Son, N.Y., 1976. Sus trabajos posteriores y una muy extensa bibliografía producida en los años siguientes en Estados Unidos sobre el tema pueden consultarse en GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, cit., *passim*.

[9] Un minucioso estudio muy reciente de las diversas modalidades de comportamientos ilícitos en Internet, cfr. la monografía de HILGENDORF/ FRANK/ VALERIUS, *Computer– und Internetstrafrecht*, Springer, Berlín, Heidelberg, 2005.

[10] Cfr. la recopilación de estas primeras iniciativas internacionales en ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002, pp. 281 ss.

están dando dentro de la Unión Europea. Así, expresamente se incluyen los *delitos informáticos*[11] en el catálogo de *eurodelitos*, que no sólo habrán de tratarse armónicamente en el plano legislativo interno, sino que, además, contarán con una cooperación y coordinación policial y judicial «privilegiada» en el incipiente «espacio judicial único europeo». A la espera del pleno desarrollo del mismo (proceso lento por las reticencias de los Estados miembros a renunciar a parte de su soberanía)[12], las legislaciones internas inician su andadura para la implantación de la *Euroorden*, la puesta en marcha de *Eurojust*, con la creación paralela de equipos conjuntos de investigación y la práctica supresión de los mecanismos clásicos de extradición en el seno de la UE. En estas claves deben ser consideradas algunas normas relativamente recientes en nuestra legislación, como la Ley 3/2003, de 14 de marzo, sobre la orden europea de detención y entrega, la L.O./4/2003, de 21 de mayo, o la L.O.12/2003, de 21 de mayo, donde hallamos notable avance en materia de cooperación judicial internacional, con enorme incidencia en las manifestaciones transnacionales de la *criminalidad informática*, como tendremos ocasión de comprobar.

Evidentemente, las necesidades vinculadas a una respuesta *globalizada* y transnacional para combatir las más graves manifestaciones de ciberdelincuencia en la Red no quedan satisfechas en el plano regional europeo, ni siquiera en el nivel del llamado *Primer Mundo,* como pareció ignorarse hasta el terrible atentado terrorista contra Las Torres Gemelas. Aun después de aquella fecha, en el seno de la Comunidad internacional, particularmente entre los países más ricos y desarrollados, se aprecia una cierta *miopía* en el modo de afrontar el fenómeno, pues, de poco sirve ya hoy que algunas (o una) de las grandes potencias logren un cierto control (unilateral, unidireccional) del ciberespacio en aras a combatir todas las expresiones de la delincuencia en la Red si no se poseen, de forma paralela, los resortes y apoyos mínimos en los diversos Estados en los que aquellas extienden sus tentáculos.

Por volver con el caso que nos sirvió de introducción a estas líneas, cabría apostillar que el Departamento de Defensa de los Estados Unidos, aún habiendo detectado los actos de «intrusismo informático» en sus sistemas, pero llevados a cabo desde España, ha precisado de una activa cooperación policial y judicial en nuestro territorio hasta materializar la detención del *hacker* y, en tanto sean depuradas sus eventuales responsabilidades, a cuyo efecto es preciso que tales hechos sean *delito* en España. Es decir, que al menos se precisa una adecuada relación entre los países, cristalizada en una serie de Acuerdos, una disposición a colaborar de nuestro país y la no menos importante «capacidad» para colaborar (esa capacidad, obviamente, no la tienen todos los países, porque se precisa una cualificación técnica mínima en equipos especializados dentro de los Cuerpos y Fuerzas de Seguridad del Estado y en muchos países este puntal falta). Por último, todo lo anterior deviene inútil si en España no están tipificadas como delictivas las conductas que se pretender reprimir, cuestión harto complicada por la insuficiente y poco meditada contemplación del *intrusismo informático* en nuestro Código Penal vigente[13].

---

[11] Expresión que tendré oportunidad de criticar más adelante, reiterando la posición que he defendido en varios trabajos. Por todos, «En torno a los fraudes informáticos en el Derecho español», *Actualidad Informática Aranzadi*, nº 11, abril de 1994, pp. 7 ss.

[12] Una clara expresión de estas reticencias la encontramos en el reciente pronunciamiento del Tribunal Constitucional Alemán declarando, por Sentencia de 18 de julio de 2005, la oposición de la *Euroorden* a la Ley Fundamental de Bonn en el punto concerniente a la «entrega de nacionales» (B.VefG18.07.05). Como consecuencia, por Acuerdo del Pleno de la Audiencia Nacional de 21 de julio de 2005, la Euroorden no es de aplicación en los procedimientos que los Tribunales españoles tengan con los alemanes y viceversa.

[13] Es sabido que la cuestión de más difícil consenso en orden a la comprensión armónica y homogénea en Derecho positivo de las diversas manifestaciones de la criminalidad informática es precisamente el *hacking* o mero intrusismo. A mi modo de ver, la polémica no siempre se plantea en

Resta una última observación para cerrar estas líneas introductorias: No podemos olvidar que, entre tanto, en el otro platillo de la balanza, y siempre en ese permanente equilibrio inestable con la *eficacia* y la *seguridad*, están las garantías individuales, la libertad, la intimidad y la dignidad de las personas, constitucionalmente consagradas en las sociedades modernas, pero cada vez más en entredicho «por razón *superior de seguridad nacional*» en los últimos tiempos. La revolución tecnológica ha potenciado (propiciándola) la delincuencia transnacional, globalizada, sin fronteras, y urge una respuesta globalizada, no unilateral e individualizada. Pero no puede ser una respuesta a cualquier precio. El otro gran riesgo de la sociedad cibernética concierne más directamente al hombre en sus más íntimos y personalísimos bienes: el ciudadano *transparente* controlado en todas sus dimensiones y actividades por el ojo, siempre atento e implacable, del Estado[14].

En suma, nuestra propuesta inicial de replantear el estudio de la criminalidad informática desde una nueva óptica aconseja prestar atención, no ya a cualquier hecho criminal mediante el uso abusivo o pervertido de las altas tecnologías de la información, sino a los problemas que en la actualidad presenta la criminalidad transnacional en el *espacio virtual*. Esto remite al replanteamiento de una cuestión clásica en Derecho penal, que experimenta la necesidad de un profundo cambio para adaptarse a la *era digital*, y todo ello, en permanente conflicto con las garantías individuales, tan en precario en el presente como se acaba de apuntar.

## II. Problemas de aplicación de la ley penal en el *espacio virtual*.

El último párrafo de la Exposición de Motivos de la Ley 3/20003, de 14 de marzo, sobre la orden europea de detención y entrega, establece:

> «Se trata, (...), de una ley que introduce modificaciones tan sustanciales en el clásico procedimiento de extradición que puede afirmarse sin reservas que éste ha desaparecido de las relaciones de cooperación judicial entre los Estados miembros de la Unión Europea. El procedimiento de entrega que se aplicará en su lugar permitirá a partir de ahora que esta forma de cooperación judicial directa opere de manera eficaz y rápida, entre Estados cuyos valores constitucionales se basan en el respeto de los derechos fundamentales y en los principios democráticos».

Tras una primera lectura de todo el articulado de la Ley citada (cuyo objeto, según el propio legislador, es cumplir con las obligaciones que la Decisión marco de 17 de julio de

---

los términos adecuados, y con la aparente cobertura de un pretendido *garantismo*, en no pocas ocasiones sólo se simplifica burdamente la cuestión hasta un grado inaceptable. Por lo que puedo entender, el debate remite a la eventual aparición de un nuevo interés social muy valioso para la vida hoy en sociedad (está claro que hablamos en clave de «bien jurídico», vinculado a la revolución tecnológica y a la dependencia informática moderna). Más extensamente, con referencias ilustrativas de Derecho comparado en mi trabajo «El intrusismo informático (*Hacking*): ¿Represión penal autónoma?», *Informática y Derecho. (Actas del II Congreso Internacional de Informática y Derecho)*, vol. II, UNED (Centro Regional de Extremadura), Mérida, 1996, pp. 1163 ss.

[14] Una representativa corriente de juristas, dentro y fuera de nuestras fronteras se muestran especialmente sensibles ante este grave riesgo de nuestro siglo, problema que se ha agravado de forma ostensible desde el atentado del 11–S en Nueva York, dolorosa coartada para el Gobierno de los Estados Unidos en su despliegue ilimitado de mecanismos de control por todo el Orbe. Vid. el interesante trabajo de mi colega argentino Marcelo RIQUERT, titulado: «Protección de datos y lucha contra el crimen», texto manuscrito, gentilmente cedido por el propio autor, a la espera de su inminente publicación.

2002 establece para los Estados miembros de la Unión Europea para hacer efectivo el «espacio judicial único»), bien podría afirmarse que se produce un avance sin precedentes en relación con la efectiva represión de un importante elenco de delitos (entre los que se mencionan los «delitos de alta tecnología, en particular delito informático»). Sin embargo, como pronto tendremos ocasión de comprobar, el cambio, siempre en este entorno de la Unión Europea, no se ciñe sólo a la simplificación o supresión de ese paso final que representa el procedimiento de extradición (con la inserción del principio de reconocimiento mutuo, que permite la ejecución prácticamente automática de las resoluciones dictadas por las autoridades judiciales de los demás Estados). Las características de la criminalidad en nuestros días imponen, en no pocos casos, que ya la cooperación, la coordinación, la actuación conjunta y el reconocimiento mutuo tengan lugar desde momentos anteriores a la existencia de una concreta resolución judicial. Y es por eso por lo que la actuación conjunta se prevé en todas las fases a través de las que se materializa el ejercicio del *ius puniendi*. Una puntual colaboración en la actuación policial o judicial, o la armonización legislativa, por sí mismas, ya se han mostrado insuficientes. Se impone una meta mucho más ambiciosa: alcanzar efectivamente un *espacio penal* (policial, legislativo y judicial) único[15]. Este es el proceso extraordinariamente complejo en que en que hoy estamos inmersos, y al cual, de forma periódica, se vienen añadiendo eslabones (v.gr.: además de otros instrumentos de auxilio judicial de fechas precedentes, de manera destacada en materia de blanqueo de capitales y criminalidad organizada, con un ámbito más genera,l destacan la L.O.11/2003, de 21 de mayo, reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea, o la L.O.12/2003, de la misma fecha, de prevención y bloqueo de la financiación del terrorismo; en idéntica orientación, reuniones conjuntas como el Congreso de EUROPOL celebrado en Alicante del mismo año, en busca de una aplicación armónica y organizada de la nueva normativa).

Evidentemente, no está en nuestro ánimo (ni en nuestras posibilidades) proceder a un análisis serio de este complejo marco jurídico. En las próximas líneas sólo intentaremos aproximarnos a lo que ello significa desde la perspectiva de esa manifestación de la criminalidad que aquí nos interesa, vinculada al uso pervertido de la altas tecnologías de la información y la comunicación electrónica (ATI), el llamado *Cibercrimen*. Se trata, en último término, de conocer en qué medida el impacto de las ATI incide o conmociona las líneas maestras de una materia clásica: eficacia de la ley penal en el espacio y competencia jurisdiccional de los Tribunales en el orden penal.

I. Hace sólo muy pocas décadas, el tema del «ámbito de validez espacial de la ley penal» se consideraba, dentro de nuestra disciplina, relativamente residual. Los delitos, por lo general, se circunscribían a un entorno limitado dentro de las fronteras de un Estado sobre el cual éste ejercía el *ius puniendi* como indiscutida expresión de su soberanía. (Una característica histórica del hecho estatal viene marcada, como es sabido, por la posibilidad de ejercicio de la potestad punitiva dentro del propio territorio: detentar el *ius puniendi* y ejercitarlo sin ninguna limitación o concesión a otros Estados). El principio de territorialidad, con sólo muy pocas excepciones (por lo general, relacionadas con la necesidad del Estado de proteger determinados intereses que le son propios prescindiendo, incluso, del lugar en que sucedan o de la nacionalidad del atacante), resolvía de forma satisfactoria y suficiente las eventuales dificultades que podía plantear, ante un caso

[15] Para un acercamiento a esta normativa, sus exigencias, mecanismos que articula, limitaciones y deficiencias, me ha resultado de gran ayuda el trabajo monográfico de CALAZA LÓPEZ, *El procedimiento europeo de detención y entrega*, Iustel, Madrid, 2005, con una amplia bibliografía actualizada. También de interés para comprender diversos enfoques sobre la *Euroorden*, el tomo colectivo FERRÉ OLIVÉ (VV.AA), *Cooperación policial y judicial en materia de delitos financieros, fraude y corrupción*, Ediciones Universidad de Salamanca, Salamanca, 2003.

concreto, la solución a los interrogantes clásicos: ¿qué ley penal resulta de aplicación y qué tribunales son competentes para conocer, juzgar y, en su caso, castigar al autor? Por lo demás, pese a la existencia de cuestiones «calientes», muy conflictivas y de difícil acuerdo (tenemos ejemplos bien próximos, como la definición de «delitos políticos»), un *cierto* consenso en la Comunidad internacional en punto a los requisitos y condiciones mínimas de extradición, quedaba materializado en una serie de Acuerdos y Tratados internacionales, bilaterales o multilaterales, dirigidos a resolver los problemas de impunidad más importantes con los que se podían topar los tribunales en la práctica.

Es posible que, al menos en el plano teórico, los postulados anteriores sigan resultando válidos. Sin embargo, no se nos esconde la simplificación que estas afirmaciones conllevan, habida cuenta de que no es posible desconocer, en la línea apuntada por MORALES PRATS[16], que aún estamos muy lejos de alcanzar ese mínimo de semejanzas políticas y sociales imprescindible para el propósito de lograr que la solidaridad entre naciones se manifieste también en lo penal; pero es que el planteamiento en tales términos, además, resulta en exceso simplista, ya que se muestra insuficiente para aprehender satisfactoriamente la compleja realidad de la criminalidad «globalizada» de nuestros días, así como el complejo, también, entramado de relaciones entre los Estados en la actualidad.

No vamos a cuestionar, desde luego, que sigue existiendo un importante segmento de delincuencia que podríamos llamar «doméstica», limitada espacio–temporalmente, cuantitativamente de gran relieve y que incide de forma muy directa en la sensación de seguridad (inseguridad) de los ciudadanos. Sin embargo, incluso muchos de esos supuestos que cabría incluir en la delincuencia tradicional más local, ya se ven, con frecuencia, salpicados, favorecidos o condicionados por la nota de la *globalización* o *mundialización* (según expresión que aún prefieren algunos) que, de una parte, favorece la movilidad de un país a otro, eludiéndose más fácilmente la acción de la justicia de un Estado, al tiempo que, de otro lado, extiende las posibilidades de actuación sobre el territorio de varios países al mismo tiempo, o respondiendo a un plan criminal único. En efecto, una violación, un asesinato, una estafa o un delito de cohecho, por ejemplo, son delitos tradicionales, clásicos, y nadie cabalmente los mencionaría como expresión de las «nuevas formas de criminalidad». No obstante, en el presente ya podría cualquiera de ellos precisar para su descubrimiento, su investigación policial o su represión, alguna suerte de cooperación internacional o actuación que superase los límites geográficos de un Estado. (En la mente de todos, seguro que están presentes supuestos que pertenecen a la historia negra más reciente en España, con el «caso *Stephen King*», o el «caso de la *estafa nigeriana*», según expresión empleada por el propio portavoz de la Policía). Es decir, que ya hoy no necesitamos apelar a supuestos extraños, casi de laboratorio, como los que se describían en antiguos Manuales y Tratados de Derecho Penal (v.gr.: el que dispara desde la misma frontera de los Pirineos) para comprender que la «eventualidad» de la dimensión transnacional de la delincuencia moderna, ya ha dejado de ser sólo «eventualidad». (Somos muchos los que nos hemos preguntado, a propósito del referido «caso *King*», si hubiera podido evitarse tanta tragedia con una cooperación policial previa más eficaz. En la sociedades modernas se reclama que, del mismo modo que los *delincuentes* no encuentran obstáculo en las fronteras nacionales, tampoco estas sean el obstáculo para la investigación de los delitos y para su represión).

Pero lo que verdaderamente parece la enseña de las manifestaciones más modernas de la criminalidad no es la *vinculación incidental* con las ATI, sino el dato de que en su uso pervertido y abusivo se halla el punto de inflexión, el origen del transito desde la delincuencia local, limitada y controlable, a una delincuencia ilimitada de carácter

[16] Cfr. MORALES PRATS, en QUINTERO OLIVARES, *Manual de Derecho Penal, Parte General,* 3ª ed. revisada y puesta al día, Aranzadi, Navarra, 2002, pp. 174 ss.

transnacional[17]. En efecto, el rasgo más diferenciador de la criminalidad más grave de estos últimos tiempos reside en que se ha visto favorecida por todas las ventajas que reporta el fenómeno de la *globalización* (v.gr.: rapidez, facilidad de comisión, separación espacio/temporal del resultado, carácter transfronterizo, potenciación ilimitada de sus efectos, favorecimiento de organizaciones internacionales y grupos no estables sin contacto previo personal, posibilidad de eliminación fáctica de cualquier rastro del hecho ilícito...) Y, sin embargo, no se ve contrarrestada por una paralela *globalización* suficiente en las actuaciones legislativas, policiales y judiciales dirigidas a su represión.

En estas coordenadas, el tema del ámbito espacial de la ley penal ya no puede estimarse marginal. La enorme escala en que se mueven las más diversas actividades económicas y culturales contemporáneas desborda ampliamente los límites nacionales como hace ver MILITELLO[18]. Y no vemos acertado desconocer o minimizar el extraordinario protagonismo que la revolución de las ATI ha jugado en esta transformación. La llamada «revolución cibernética» es uno de los motores esenciales de la nueva cara de la criminalidad moderna. Según hemos expresado en otro lugar, no cabe la comprensión del fenómeno de la delincuencia organizada transnacional moderna sin una íntima conexión con el *cibercrimen*[19], en tanto que expresión emblemática de dicho fenómeno. La realidad criminal moderna más preocupante para la Comunidad internacional en el presente se desarrolla en un «lugar» indeterminado, que denominamos *ciberespacio*, en unas coordenadas temporales difíciles de aprehender y la magnitud de sus efectos nos resulta, con frecuencia, desconocida. Coincidimos con quienes advierten de la necesidad de un replanteamiento de los postulados más tradicionales de instituciones bien consolidadas en nuestra disciplina. Bien puede decirse que en dichos postulados hoy difícilmente hallamos la solución al problema de «dónde» y «cuándo» se entiende cometido un delito, a los efectos de la ley penal aplicable o el órgano jurisdiccional competente[20]. (El ámbito espacial de las más graves y nuevas formas de delincuencia es, justamente, el «ciberespacio», un espacio global, virtual, ajeno a los conceptos «territorio nacional», «soberanía estatal», según ya se apuntó. Mas no se olvide que tampoco será sencillo la comprensión de categorías dogmáticas como la tentativa, el delito continuado y delito masa, imputación objetiva, autoría y participación, por citar sólo algunos ejemplos, si bien desbordan el objeto de las presentes líneas).

Llegados a este punto, hemos de detenernos a examinar en qué medida está llevando a un replanteamiento de los principios de la eficacia espacial de la ley penal por mor del impacto tecnológico (lo que venimos denominando en términos de «eficacia de la ley penal en el *espacio virtual*»), con especial atención a nuestro entorno más próximo: el Derecho español en el ámbito de la Unión Europea.

---

[17] Cfr. GUTIÉRREZ FRANCÉS, «Las altas tecnologías de la información al servicio del blanqueo de capitales transnacional», Separata de «Aquilafuente», nº 38, Ediciones Universidad de Salamanca, Salamanca, 2003.

[18] Cfr. MILITELLO, «Iniciativas supranacionales en la lucha contra la criminalidad organizada y el blanqueo en el ámbito de las nuevas tecnologías», *Derecho Penal, sociedad y nuevas tecnologías*, Colex, (Coord. Zúñiga, Méndez y Diego Díaz–Santos), Madrid, 2001, pp. 177 ss.

[19] GUTIÉRREZ FRANCÉS, «Las altas tecnologías de la información al servicio del blanqueo de capitales transnacional», cit. p. 211.

[20] En el mismo sentido, ANARTE BORRALLO, «Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información», Separata de *Derecho y conocimiento. Anuario jurídico sobre la sociedad de la información*, Vol. I, Universidad de Huelva, Huelva, 2001, pp. 191 ss.

II. Comenzaremos este epígrafe haciéndonos eco de una crítica que ya hemos reiterado en otras sedes (Congreso de la AIDP, en Wüerzburg, en 1993, o en el Encuentro sobre «Cooperación judicial y policial en materia de delitos financieros, fraude y corrupción», Programa Grotius II, en Lisboa en 2002), crítica que ahora ya empezamos a advertir en otros penalistas, como MILITELLO[21]. Se trata de poner de manifiesto, una vez más, la gran confusión con la que se pretende atajar las modernas formas de la criminalidad fruto del proceso de *globalización,* confusión que atribuimos, en buena medida, a los problemas que todavía en nuestros días plantea la delimitación del *Computercrime* (empleamos deliberadamente la expresión anglosajona, huyendo, de momento, de otra fórmula en castellano menos apropiada, como se explicará). Sirvan como ejemplo estas dos pequeñas muestras:

1º. La Decisión del Consejo de la Unión Europea de 28 de febrero de 2002 (por la que se crea *Eurojust* para reforzar la lucha contra las formas graves de delincuencia), cuando en el art. 4 se ocupa del «ámbito de competencia general de Eurojust», indica que abarcará, además de las competencias que tenga Europol (art. 2 del Convenio de Europol de 26 de julio de 1995), otros «tipos de delincuencia». Y en este punto se cita, en primer término, «la delincuencia informática». La sorpresa surge cuando, al propio tiempo, se citan categorías delictivas como: fraude, corrupción y cualquier infracción que afecte a intereses financieros de la Comunidad Europea, el blanqueo de capitales, participación en una organización delictiva, y otras infracciones cometidas en conexión con las anteriores.

2º. La Ley española citada al iniciar este apartado, de 14 de marzo de 2003, a mayor abundamiento, en ese largo listado de delitos que darán lugar a la entrega de la persona reclamada sin control de la doble tipificación de los hechos (art. 9.1), incluye, al mismo nivel que los supuestos de fraude, corrupción, blanqueo de capitales, explotación sexual de niños y pornografía infantil o falsedades (por citar algunos), los «*delitos de alta tecnología, en particular delito informático*».

Hemos seleccionado estos dos ejemplos para encabezar nuestra crítica porque en ellos podemos contemplar esa confusión apuntada, derivada de la difícil (además de inútil e innecesaria) delimitación del llamado *Computercrime*. El «delito informático» no existe como tal. No es una categoría más del elenco de delitos. Desde luego, pretender a estas alturas la existencia de «algo» con entidad propia que deba llamarse «delito informático», resulta desde cualquier punto inaceptable. Pudo tener sentido inicialmente (y aún hoy, pero siempre en otros términos) abordar conjuntamente y en clave de «problema», los problemas que las ATI vienen planteando al sistema punitivo[22]. Pero «lo informático» (su uso pervertido o abusivo) no puede tener entidad suficiente para mutar la naturaleza de cualquier delito, cuya esencia estará siempre en la naturaleza del bien jurídico cuya afección se pretende evitar. Es decir, lo sustantivo del hecho ilícito no está determinado por la presencia (o no) de «lo informático», por grandes que sean las dificultades que tal aspecto represente para su efectiva represión. Así, por ejemplo, unas amenazas a través de la Red, o el blanqueo de capitales, o el atentado contra la seguridad de Estado..., no verán modificada su esencia, se realicen o no mediante manipulación informática subrepticia, recaigan o no sobre elementos o sistemas informáticos.

Adviértase, en la línea que aquí se sigue, que algunos textos jurídicos ya reflejan la normalidad de lo que pudiéramos llamar «versión informática» de ciertos delitos. Tomamos

[21] Cfr. MILITELLO, ult. cit.

[22] Cfr. He mantenido esta criterio desde mis primeros trabajos sobre el tema (por todos, cfr. GUTIÉRREZ FRANCÉS, «En torno a los fraudes informáticos en el Derecho español», *Actualidad Informática Aranzadi*, abril, 1994, pp. 7 ss). En contra, sin embargo, en el mismo número de la misma revista, vid. BUENO ARÚS, «El delito informático», cit., p. 1 ss.

ahora como ejemplo la Decisión Marco del Consejo de la Unión Europea de 13 de junio de 2002, sobre lucha contra el terrorismo. En la definición que se acoge de los delitos de terrorismo en el art. 1, se incluye específicamente como posibilidades comisivas las «destrucciones masivas en instalaciones gubernamentales o públicas, sistemas de trasporte, infraestructuras, incluidos los sistemas informáticos...» Parece fuera de duda que un delito de terrorismo no deja de serlo para convertirse en un «delito informático», (de otra naturaleza, como pudiera ser un «sabotaje informático»), sólo por realizarse sobre «sistemas informáticos». Por lo mismo, tampoco debe merecer un tratamiento distinto y diferenciado[23].

En suma, hay que denunciar ese afán por marcar la *sustantividad* de una categoría que carece de ella, que es heterogénea y plural, y que sólo se justifica por su funcionalidad desde una perspectiva criminológica (y en tanto siga siendo de alguna utilidad). Porque lo deseable es que las legislaciones modernas sean capaces de hacer frente a las múltiples manifestaciones de la llamada *criminalidad informática* mediante la «no exclusión expresa» de lo informático (es decir, la inclusión sin atentar al principio de legalidad penal) en la configuración de los tipos penales. Debe evitarse el error de volver a una normativa casuística, descriptiva y farragosa, en la que se vayan incluyendo, una vez más de modo precipitado, como añadidos explicativos, los nuevos medios que se descubran o los nuevos objetos que lleguen a surgir. Supondría desconocer todo lo que significó en el siglo XIX el movimiento codificador y el avance que representó en racionalidad, seguridad jurídica, economía legislativa y concisión.

La cuestión no es meramente formal. Por el contrario, encierra una confusión incomprensible, que, en la práctica, está conduciendo a una duplicidad innecesaria de esfuerzos en el orden internacional, a la superposición de Convenios, Acuerdos y actuaciones internacionales y que, en último extremo, redunda en una pérdida de *energía* en la represión de las formas más graves de la criminalidad moderna. Con un planteamiento crítico similar al que aquí hemos expuesto, MILITELLO[24] denuncia esa tendencia, de modo especial entre los países occidentales: Por un lado, se observa en la mayoría de las legislaciones contemporáneas la dedicación de un esfuerzo muy importante del sistema penal para luchar contra la criminalidad organizada y las diversas formas ilegales en que se manifiesta, pero, por otra parte, al mismo tiempo, se está desarrollando una legislación específica, casi siempre con disposiciones de naturaleza penal, dedicada a la materia informática. Y, como él mismo denuncia, lo llamativo es que los dos sectores carecen de una adecuada conexión recíproca, sin la cual las diversas respuestas nacionales a las mencionadas manifestaciones de la criminalidad moderna, a duras penas podrán afrontar la importancia y los caracteres cada vez más peculiares de dichos fenómenos. Pensemos en la sucesión de Convenios orientados a una actuación coordinada para luchar contra el tráfico de drogas, el blanqueo de capitales, los fraudes y la corrupción, últimamente, el terrorismo internacional... La mayoría de las conductas criminales de entidad transnacional tienen un trasfondo económico: necesitan dinero para financiarse y/o se realizan por dinero. Sea como fuere, el control de las transacciones económicas internacionales, el seguimiento ajustado de los circuitos financieros, como expresa nuestro legislador en las reformas de 21 de mayo de 2003, posibilita acercarse a los más graves delitos. Reconocer esto nos lleva, a renglón seguido, a aceptar que la mayoría de tales hechos encuentran en los sistemas informáticos el cauce idóneo para, o bien financiar, o bien perpetrar el delito, o desplegar sus efectos, o bien, ocultar, invertir o presentar como de origen lícito sus beneficios. No se entiende que la *criminalidad informática* sea abordada en otro nivel, como

[23] Vid. al efecto, en la línea propuesta por GARCÍA RIVAS, RIQUERT, M.A., «Protección de datos y lucha contra el crimen», cit., *passim*.

[24] Vid. MILITELLO, «Iniciativas supranacionales en la lucha contra la criminalidad organizada y el blanqueo en el ámbito de las nuevas tecnologías», cit., pp. 177 ss.

si de una realidad criminal autónoma se tratara. Más al contrario, es el impacto de la revolución cibernética y su empleo perverso lo que determina el salto, la transformación de algunos de los delitos «domésticos» clásicos hasta erigirse en grandes protagonistas de la criminalidad organizada transnacional más peligrosa hoy.

Tras estas reflexiones críticas, se entenderá sin dificultad nuestro rechazo al planteamiento de nuestro legislador cuando en la Ley de marzo de 2003 arriba citada menciona, como si de una figura autónoma se tratara, «el delito informático» (del mismo modo que en su día nos pareció desacertado presentar el Código Penal español de 1995 alabando su «modernidad» por incorporar el «delito informático»)[25]. Ahora bien, ¿significa eso el desconocimiento de la incidencia que la revolución cibernética viene representando hasta el presente al sistema punitivo? En modo alguno. Entendemos que aún tiene sentido analizar conjuntamente algunos de los problemas que plantean las nuevas manifestaciones de la criminalidad cuando se aprovechan de las múltiples ventajas que reportan las ATI. Sólo en ese contexto cabe hablar de *Computercrime, Cibercrime* o *Criminalidad cibernética*. Y su punto realmente diferenciador y unificador lo hallamos justo en su dimensión transnacional, lo que explica esa radical transformación en materia de «eficacia de la ley penal en el espacio». La necesidad de una revisión profunda de este tema, insistimos, no deriva de la presencia de «lo informático» en las modernas manifestaciones de la criminalidad, sino en esa dimensión transnacional (o supranacional) nueva de la delincuencia actual, facilitada, potenciada o propiciada por la revolución de las altas tecnologías de la información y comunicación electrónica.

¿Y dónde se halla, para nosotros, lo esencial de la radical transformación del problema de la ley penal en el espacio? A nuestro entender, se concreta en lo siguiente: Hasta ahora, las claves para afrontar los problemas de *cuándo* y *dónde* se entendía cometido un hecho delictivo, *qué ley penal* era de aplicación y *qué tribunales* se consideraban competentes para conocer del mismo, estaban previstas para delitos que eventualmente traspasaban las fronteras (geográficas) de los Estados (en su dinámica comisiva, en sus efectos o en su ocultación) y para delincuentes que pudieran desplazarse (físicamente) a otro territorio nacional. Ahora, en cambio, el planteamiento y las claves para la solución del problema han de ser distintos. La novedad es que ni delito ni delincuente traspasan fronteras, porque *no existen fronteras*. No existe uno o varios «delitos informáticos», a combatir mediante la adecuada armonización legislativa entre los Estados, sino que existe una delincuencia que se despliega eficazmente y con gran impunidad en la «aldea global». Y combatir el *Cibercrimen*, que se realiza en un espacio virtual, al margen de las fronteras convencionales de los Estados, no puede pretenderse desde las coordenadas convencionales de la soberanía en el territorio nacional.

En las próximas líneas vamos a ocuparnos de los principales pasos que se han dado para hacer frente a estos problemas, que, a nuestro juicio, en buena medida no son sino la expresión desorganizada de una multiplicidad de esfuerzos sin la coordinación racional de un proyecto eficaz y realista común. No vemos otra forma de valorar iniciativas superpuestas desde distintas esferas (Naciones Unidas, Consejo de Europa, Unión Europea...), referidas, unas veces a combatir el *Cibercrimen*, pero otras, sobre el terrorismo

[25] Tal fue la expresión que recogieron numerosos medios de comunicación que, aquí sí, reproducían textualmente las palabras del entonces Ministro de Justicia, siendo así que la novedad más importante que en tal materia aportaba el texto legal era (es) la «no exclusión de lo informático» en la normal previsión de las conductas prohibidas: v.gr. blanqueo de capitales (sin excluir «por medios informáticos»), falsedades documentales (sin excluir las electrónicas), apropiación indebida, delitos societarios, estafa, fraude fiscal..., etc., se realicen o no mediante artificios electrónicos. (Sobre tales novedades del Código Penal de 1995, GUTIÉRREZ FRANCÉS, «Delincuencia económica e informática en el nuevo Código Penal», *Cuadernos de derecho Judicial. Ámbito jurídico de las tecnologías de la información*, CGPJ, XI, Madrid, 1996, pp. 247 ss.)

internacional, o sobre el crimen organizado, o sobre el fraude y la corrupción, cuando no, sobre el blanqueo de capitales internacional.... Con todo, a pesar de la falta de coordinación de algunas de estas iniciativas, hemos de ocuparnos de ellas, en especial de aquellas que más directamente incidan en nuestro ordenamiento punitivo.

## III. Iniciativas para una actuación globalizada contra la Ciberdelincuencia transnacional.

Aunque existen manifestaciones en la Comunidad Internacional a nivel global de esos esfuerzos por hacer frente de forma coordinada a los nuevos retos de la moderna delincuencia transnacional, bajo los auspicios de Naciones Unidas (pensemos, por ejemplo, en la represión del blanqueo de capitales y en las actuaciones orientadas a combatir el terrorismo internacional), las iniciativas más relevantes y significativas pueden citarse en el ámbito europeo, al que vamos a prestar una mayor atención. En efecto, de una parte, en el seno del Consejo de Europa, pero, sobre todo, en el ámbito más homogéneo de la Unión Europea, ya desde el Tratado de Ámsterdam (firmado el 2 de octubre de 1997, y en vigor desde el 1 de mayo de 1999) se busca efectivamente crear un «espacio de libertad, seguridad y justicia», objetivo al que desde entonces se están orientando los esfuerzos de los Estados miembros, en orden a la adopción de las medidas necesarias para potenciar la cooperación en la lucha contra las formas más graves de delincuencia. En las próximas líneas haremos referencia a aquellas medidas de mayor trascendencia en la materia que nos ocupa, al tiempo que se apuntarán las vías para su incorporación en nuestro Derecho interno. Y, como tendremos ocasión de demostrar, en su mayoría son cauces «*informáticos*» de luchar contra diversas expresiones de la dimensión pervertida de la Informática. Dicho en otros términos, se empieza a vislumbrar que una mejor y más coordinada utilización de las altas tecnologías de la información y la comunicación electrónica de datos, ha de ser el cauce para combatir una delincuencia que no conoce fronteras en el espacio virtual.

Debe considerarse, en todo caso, que las dificultades para poner en marcha todos estos mecanismos (en gran medida ya formalizados hoy jurídicamente), aún en el espacio más limitado y, en principio, más homogéneo de la Unión Europea, son grandes: como señala MUÑOZ CONDE[26], pese a la existencia de numerosos principios de carácter jurídico, esta materia presenta frecuentes connotaciones políticas, que se hacen patentes especialmente en materia de extradición. La cesión a otros Estados de parte del ejercicio de la potestad punitiva propia no se acepta siempre fácilmente. Y, tal como está previsto, la puesta en marcha plena del sistema articulado en el Convenio relativo a la asistencia judicial en materia penal, de 29 de mayo de 2000, la Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la Orden Europea de Detención y Entrega, o la Decisión del Consejo, de 28 de febrero de 2002, por la que se crea EUROJUST para reforzar la lucha contra las formas de delincuencia más graves, el instituto de la extradición, al menos en su configuración clásica, se debiera haber superado, al menos en teoría, en el ámbito de la Unión Europea. No obstante, ya se ha indicado más arriba que en los últimos meses se ha presentado un escollo muy serio, al quedar excluida la República Federal Alemana tras el pronunciamiento del 18 de julio de 2005.

[26] Cfr. MUÑOZ CONDE, GARCÍA ARÁN, *Derecho Penal. Parte General*, 6ª ed., Tirant lo Blanch, Valencia, 2004, pp. 162 ss. También de interés, CUERDA RIENZU, *De la extradición a la euro orden de detención y entrega. Con un análisis de la doctrina del Tribunal Constitucional español*, Ed. CEURA, Madrid, 2003.

Comoquiera que en líneas anteriores hemos advertido la falta de coordinación en las medidas para la represión de la *Ciberdelincuencia*, esto mismo dificulta una exposición más ordenada y coherente. En todo caso, se intentará establecer un cierto orden abordando, en primer término, las iniciativas específicamente orientadas a combatir la llamada *Criminalidad informática*, en los diversos niveles internacionales, para mencionar después otras actuaciones con tanta o mayor repercusión en esta materia, pero que no se destinan de forma específica a la represión del *Computercrime*.

1. Medidas e iniciativas internacionales para combatir la *criminalidad informática* en la esfera internacional *mundial*:

En este primer nivel más amplio, no podemos ser muy optimistas con carácter general. Muy serias diferencias políticas, culturales y sociales arrastradas desde siglos imposibilitan las condiciones mínimas para la cooperación en todos los planos de la represión penal internacional. (Las dificultades con las que está topando la implantación del Tribunal Penal Internacional no son sino el reflejo de las divergencias de fondo, entendemos que de momento insalvables). Es por eso que los pasos para una coordinación en la lucha contra las formas más graves de delincuencia de carácter transnacional se ven reducidos a Convenios bilaterales o multilaterales entre los Estados, y cuya efectividad depende, en última instancia, de la «buena voluntad» de estos en la concreta plasmación de las medidas en las legislaciones internas respectivas. Sin embargo, en materia de represión del *Computercrime*, acaso por la falsa impresión de que se trata de una problemática de carácter meramente técnico, sin implicaciones políticas, las dificultades de aproximación no han sido tan grandes. La evolución en el proceso que se ha seguido hasta nuestros días, de sobra conocida, podríamos resumirla en los siguientes términos:

Desde la segunda mitad de la década de los setenta, en los Estados Unidos (como ya avanzamos en el epígrafe introductorio) se empezó a tomar conciencia del peligro que podía representar el «abuso informático», y ya de aquellos años datan los primeros estudios criminológicos sobre el *Computercrime* (ya citados), donde se ponían de manifiesto las dificultades que podrían plantear estos supuestos para su detección, prueba y persecución. Se empezaba entonces a vislumbrar, en efecto, la dimensión que las altas tecnologías de la información ofrecían como *factor criminógeno* de primera magnitud, al potenciar de forma casi ilimitada el abanico de medios comisitos, generar nuevos, y con frecuencia muy vulnerables objetivos criminales, dificultando, al tiempo, su descubrimiento y represión. No se ha de olvidar, no obstante, que en aquella etapa inicial los pocos casos descubiertos, aunque llamativos, eras burdos, poco sofisticados en cuanto a su dinámica comisiva, y limitados desde la perspectiva de sus efectos (supuestos de intrusismo informático, daños en los sistemas, manipulación de datos, fraudes...). Si volvemos a aquellos primeros estudios, sin embargo, observamos que no revelan una especial preocupación por la potencial dimensión transnacional de la llamada *delincuencia informática*. Es decir, su eventual carácter trasfronterizo era sólo eso: un *eventual* riesgo, lejos aún de percibirse como un peligro real y serio. (Como se puede suponer, el proyecto «*The Ribicoff Bill*» que se pretendió introducir en 1978, aunque sirvió de modelo a posteriores reformas legislativas en diversos estados miembros, no abordó cuestión alguna sobre la peculiar dimensión transfronteriza de estas nuevas formas de delincuencia).

A partir de la segunda mitad de los ochenta, en cambio, y ya sin duda desde la década de los noventa, ese riesgo potencial se actualiza, estalla de forma inesperada, y la *delincuencia informática* adquiere una nueva dimensión, abandonando los moldes del ámbito doméstico. No vamos a entrar aquí en el debate acerca de la conveniencia o no de

distinguir una primera *revolución informática* de una segunda *revolución cibernética* (en tal sentido, MORÓN LERMA o ROVIRA DEL CANTO)[27], pero lo que no cabe desconocer es que la irrupción de los ordenadores personales en las sociedades contemporáneas y su vertiginosa extensión y popularización, no han representado más que el preámbulo o la antesala de una revolución más trascendente, si cabe, con la entrada en la *era digital*, por la difusión masiva de las comunicaciones telemáticas. (Aunque en opinión de los expertos Internet está en su infancia, habida cuenta de que parece que aún ni se ha desarrollado el 20% de su potencial, lo cierto es que ni los más optimistas llegaron a intuir la celeridad de su expansión. Si la televisión necesitó trece años para llegar a 50 millones de hogares, Internet alcanzó esa cifra en tan sólo cinco años. Así, por ejemplo, de 180 millones de internautas en diciembre de 1998, se ha pasado a más de 600 millones a principios del presente 2003, según *NUA Internet Services*.).

La referencia que se acaba de apuntar no es una mera curiosidad a los efectos del tema que nos ocupa, sino que más bien fija el punto de inflexión en la evolución desde el *localismo* a la *globalización*, evolución a la que no ha permanecido inmune el mundo del delito. Sin embargo, la trascendencia de dicho tránsito no fue percibida en el mundo jurídico, al menos en nuestra disciplina, desde el primer momento. Desde luego, en materia de *criminalidad informática*, desde los años ochenta se pone de relieve la necesidad de alguna suerte de cooperación entre los Estados. Varias reuniones de expertos[28] en el tema auspiciados por la OCDE, el Consejo de Europa o la AIDP, trataron de buscar cauces para una eficaz represión del *Computercrime* (tarea en la que ya se observaba insuficiente e ineficaz cualquier iniciativa aislada de un Estado determinado; ni siquiera era suficiente la actuación coordinada entre los países más desarrollados). ¿Cuál fue el fruto de estos primeros encuentros internacionales? Formalmente, cuajaron en varios textos de Recomendaciones a los Estados en orden a adaptar sus respectivos sistemas punitivos para llenar las lagunas que se venían detectando en las legislaciones tradicionales. (En tal sentido, las Recomendaciones de la Comisión de Expertos de la OCDE, firmada en París, en 1986; o las Recomendaciones de la AIDP tras el encuentro sobre *Computercrime*, Würzburg, 1993). Es decir, aún no se percibía la necesidad de un nivel más amplio de cooperación, en la idea errónea de que los instrumentos clásicos de los principios de eficacia de la ley penal en el espacio, con la legislación interna ya adaptada, eran adecuados para resolver problemas de posible impunidad.

Con todo, el mayor logro de estas actuaciones iniciales de carácter internacional se concreta en su extraordinaria labor de sensibilización en todas las instancias nacionales, internas, a quienes compete directamente el ejercicio del *ius puniendi* (Policía, jueces, juristas, legisladores) sobre los riesgos de las ATI.

## 2. Medidas en el ámbito del Consejo de Europa.

Hay que esperar hasta el 2001 para encontrar un Convenio internacional donde se cristalicen tales recomendaciones. El Consejo de Europa, la más alta institución activa en la escena europea en el sector de la cooperación en materia penal, confirmó su efectivo interés en este tema a través de la elaboración del Convenio sobre el *Cibercrimen*, de 23 de noviembre de 2001, abierto a la firma también a Estados no pertenecientes al Consejo de Europa[29]. Dicho texto, que nace precisamente debido a la exigencia de superar los límites

[27] Sobre el debate, cfr. por todos, ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, cit., pp. 18 ss.

[28] Para una visión global, vid. ROVIRA DEL CANTO, ult. cit. pp. 283 ss.

[29] Cfr. HILGENDORF/ FRANK/ VALERIUS, *Computer– und Internetstrafrecht*, cit., pp. 16 ss.

derivados de la naturaleza transnacional del fenómeno de la delincuencia vinculada al uso pervertido de las ATI, ya refleja una preocupación seria por resolver los problemas de aplicación de la ley penal en el nuevo *espacio virtual* (a tal efecto, desde el Preámbulo se declara prioritaria una «política criminal común» contra el *Ciberdelito*, en el marco de una «mayor, más rápida y eficaz cooperación internacional» en la materia). Sin embargo, ya merece ser destacado otro paso previo relevante: El 19 de marzo de 1998, el Consejo invitó a los Estado miembros a adherirse a la *Red de información del G8* (accesible durante veinticuatro horas) para la lucha contra la delincuencia en el ámbito de las altas tecnologías de la información. Con esta *Red*, configurada en sus pilares básicos durante la reunión de Ministros de Justicia e Interior de los G8 de Washington en 1997, aunque prevista también para incluir a terceros países, se permitirá a los Estados adherentes tener una visión global de aquellas manifestaciones de la *criminalidad informática* que se desarrollan simultáneamente en varios territorios nacionales. Creada en el periodo 1998 a 2000, la *Red* integra en la actualidad a los siguientes países: Australia, Brasil, Canadá, Dinamarca, Finlandia, Francia, Alemania, Italia, Japón, Países Bajos, Rusia, España, Suecia, Reino Unido y Estados Unidos de América. Pues bien, una comunicación permanente de información en esta línea se halla prevista con carácter general para todos los países que se adhieran al Convenio sobre el *Cibercrimen* de 2001 citado anteriormente. El art. 35, en concreto, cuando prevé el llamado «24/7 *Network*», de alguna forma puede decirse que institucionaliza esta fórmula como una vía de cooperación internacional en la represión de las formas más graves de delincuencia.

Aunque el Convenio del Consejo de Europa sobre el *Cibercrimen* no será aquí objeto de estudio más detallado, en el tema que ahora nos ocupa daremos sólo un pequeño apunte:

- ❖ No se puede olvidar que, más allá de lo que el texto establece respecto a la jurisdicción competente cuando un *cibercrimen* presenta carácter transfronterizo (art. 22), y de las reglas previstas en los arts. 23 y siguientes sobre cooperación internacional y principios de extradición en estos supuestos, en última instancia todo va a depender: primero, de la firma y ratificación del Convenio por los Estados y, sobre todo, de la voluntad que estos reflejen en su orden interno (la armonización legislativa y la efectiva cooperación judicial y policial). Es, por tanto, muy importante esa fase ulterior, a cuyo albur queda la eficacia del Convenio. Es por eso que, al tiempo presente, su virtualidad es ciertamente limitada.

- ❖ Respecto al establecimiento de las reglas de atribución de competencia jurisdiccional, no se resuelve gran cosa, siendo así que es uno de los temas más conflictivos en estas nuevas manifestaciones de la criminalidad. Quizá hubiera sido una buena oportunidad para superar el tradicional criterio del «lugar donde se ha cometido el delito» (que obliga a plantear dónde ha de entenderse *cometido* un delito), ofreciendo unas pautas realistas para los hechos simplemente cometidos *en la red*, en el *ciberespacio*.

- ❖ Se exhorta a los Estados a procurar los medios para una más amplia cooperación en las investigaciones y procesos referidos a infracciones de las que se recogen en los arts. 2 al 11 (ahora se han de completar con las incluidas en el Protocolo Adicional al Convenio, de 28 de enero de 2003), fijándose unos principios mínimos de extradición, en defecto de otros Convenios más específicos entre los Estados. En este punto, no podemos olvidar que ya los países miembros de la Unión Europea, con un nivel de cooperación judicial y policial muy superior, como veremos, estuvieron representados en el Convenio de forma única (posición común adoptada por el Consejo el 27 de mayo de 1999 en GUCEL 142 de 05/06/99) y que, por lo que a nosotros concierne, es en este ámbito más reducido donde hallamos el centro obligado de referencia. De cualquier modo, en materia de extradición es donde más

evidentes se manifiestan los problemas de yuxtaposición de iniciativas análogas no bien coordinadas.

❖ Habida cuenta de que los avances tecnológicos que comporta la Sociedad de la Información, de acuerdo con el Convenio, se ponen a disposición de la Justicia penal (debieran ofrecer mayores y mejores posibilidades en la persecución y lucha contra la criminalidad, no sólo *cibernética*), tampoco se ignora en el texto que tales instrumentos conllevan graves riesgos para los derechos y libertades individuales. Por eso no se descuida la implantación de mecanismos para intentar neutralizar de algún modo tales «efectos secundarios» sobre las libertades de los ciudadanos. Aunque, de nuevo, tal *autocontrol*, exigencia ineludible del Estado de Derecho, queda sujeto a las concretas limitaciones que se incorporen en el concreto orden interno.

3. Medidas en el marco de la Unión Europea.

El entorno que para nosotros es más próximo, por razones obvias, y en el que de modo verdaderamente significativo vemos comprometidas y conmocionadas en el presente las líneas maestras tradicionales sobre competencia jurisdiccional y eficacia de la ley penal en el espacio es, sin duda, el entorno de la Unión Europea, con ese ambicioso proyecto de creación de un «espacio judicial único». Vamos a ocuparnos ahora de los aspectos más relevantes, señalando los pasos que se están dando para la consecución de tal objetivo:

❖ En primer término, se debe aclarar que resulta excesivamente limitado plantear el tema que aquí nos ocupa circunscribiéndolo a los «mecanismos de cooperación para la represión del *Cibercrimen* en el ámbito de la Unión Europea». Y no significa que en este nivel supranacional falten específicas iniciativas para una actuación conjunta, armónica y coordinada en la lucha contra esta clase de delincuencia. Pero difícilmente pueden comprenderse desgajadas del proyecto citado del «espacio judicial único», dentro del cual los problemas de *Ciberdelincuencia*, más que un capítulo autónomo, se incrustan el casi *todos* los capítulos. De cualquier modo, la atención que las instituciones europeas vienen prestando a los peligros inherentes a la *revolución cibernética*, está fuera de toda duda, como ahora destacamos a través de algunos ejemplos, antes de abordar el alcance de la Decisión Marco de 13 de junio de 2002.

❖ Ya el Parlamento europeo, en una resolución de 28 de octubre de 1997 sobre el «Plan de Acción contra la criminalidad organizada», confirmaba la importancia de una cooperación judicial, policial y aduanera más intensa entre los Estados miembros de la Unión Europea para salir al paso de las transformaciones sufridas por la «actividad criminal después del advenimiento del mercado interno único y de la irrupción de las modernas tecnologías de la información». Se denuncia en el texto el retraso en el conocimiento del modo en que se desarrolla la «criminalidad de alta tecnología», al tiempo que se exige sacar cuanto antes a la luz las «posibilidades de blanqueo de los efectos procedentes de la comisión de delitos a través de Internet», de los «fraudes en las transacciones comerciales electrónicas», o se advierte del peligro del «espionaje (económico) informático».

❖ El 18 de diciembre de ese mismo año, el Consejo de la Unión Europea, al tiempo de establecer las prioridades asignadas a la cooperación en materia de justicia, pone de relieve la necesidad de combatir el «uso de las altas tecnologías con fines delictivos», con la correlativa necesidad de que también sean utilizadas eficazmente en la lucha contra la criminalidad. El compromiso es asumido igualmente después de

la entrada en vigor de la nueva versión del Tratado de Ámsterdam: una de las materias en las que se prioriza el objetivo de la consecución de un espacio de «libertad, seguridad y justicia», es la «criminalidad de alta tecnología» (n.48 de las conclusiones del Consejo de Tampere, Finlandia, 16 de octubre de 1999).

❖ En reunión de 28 de febrero de 2003 pasado año, los Ministros de Justicia acordaron la necesidad urgente de aproximar las legislaciones internas de los Estados miembros, a fin de evitar en lo posible lagunas legislativas, y al mismo tiempo se fijan criterios para establecer la competencia jurisdiccional en casos de *ciberdelitos* de carácter transnacional: en primer lugar, tendrá preferencia el lugar desde donde se ha cometido el ataque, la nacionalidad del presunto autor, así como el país donde tenga su sede la persona jurídica a la que se pueda imputar el ataque. Si el hecho afectase a varios países, deberán llegar a un acuerdo para que el proceso se desarrolle en un solo Estado.

En este rápido repaso, según se habrá observado, hemos centrado la atención en las iniciativas *específicamente* orientadas a la lucha contra el *Cibercrimen* en el ámbito de la Unión Europea, listado de iniciativas que debe completarse con la ya mencionada Posición Común (CE) 1999/364/JAI, de 27 de mayo de 1999, adoptada por el Consejo sobre la base del art. 34 del Tratado de la Unión Europea, relativa a las negociaciones del proyecto de Convenio sobre *Cibercrimen* del Consejo de Europa. Sin embargo, bien podría decirse que sólo son a modo de «llamadas de atención» respecto a la dimensión pervertida y abusiva de las ATI y respecto a la necesidad de facilitar la cooperación internacional ante las modernas formas de delincuencia. Porque, como venimos reiterando, paralelamente a este camino de sensibilización hacia los riesgos de la Sociedad de la Información, se viene siguiendo un largo y complejo proceso para hacer realidad los objetivos de un *espacio judicial único* en la Unión Europea que resulta mucho más esclarecedor. Dicho *espacio judicial único*, en el sentido previsto por el Tratado de Amsterdam, debiera suponer, en el futuro, un sistema judicial sin fronteras en la Comunidad, con un Derecho común o muy próximo, aplicable indistintamente por los órganos jurisdiccionales de cualquiera de los Estados miembros. Es evidente que la tarea no es sencilla, no obstante lo cual, ya se han dado algunos pasos relevantes, que a continuación trataremos de presentar de modo muy simplificado[30].

La creación de un sistema judicial único y sin fronteras dentro de la Unión ha de pasar por varios niveles, que resumiríamos así:

❖ Armonización legislativa o aproximación de normas jurídicas aplicables en cada territorio nacional: Este deseo de armonización está permanentemente presente en toda la actividad de las instituciones de la Unión Europea en la práctica totalidad de las ramas del ordenamiento jurídico. Sin embargo, la cuestión es más difícil en la materia penal porque, como es de sobra conocido, estamos en una disciplina eminentemente valorativa y que se manifiesta como la más sensible a los cambios políticos, sociales y de orientación ideológica. La homogeneidad en la defensa de los valores tendentes a la consecución de un sistema democrático parlamentario, pluralista y respetuoso de los derechos humanos y las Libertades Fundamentales,

[30] Mucho menos optimista, seguro que a causa de su mayor conocimiento sobre el tema, CALAZA LÓPEZ, *El procedimiento europeo de detención y entrega*, cit., pp. 259 ss. , donde critica el «confucionismo» al que lleva el sistema, con la superposición del cauce fijado por la *Euroorden* y el clásico de la extradición, según la voluntad legislativa de nuestros vecinos comunitarios. Explica, adicionalmente, otros argumentos que apoyan la crítica (como la creación o potenciación de «paraísos delictivos», o la adaptación «incondicional» de toda suerte de regulaciones). Con todo, parece que no puede negarse su valor como «primer intento» serio en la consecución de una Europa sin fronteras en la represión de las más graves formas de delincuencia.

debiera facilitar la armonización legislativa. En tema de *Ciberdelincuencia*, adicionalmente, acaso por la impresión de que no posee la carga ideológica de otras formas de criminalidad, los representantes de los Estados miembros han llegado a postura común consensuada (la que se defendió en las sesiones preparatorias del Convenio del Consejo de Estado). Con todo, esa posición común consensuada no se ha materializado en idénticas soluciones jurídicas en el orden interno. Para solventar tales escollos, se recurrió, en primer término, a la simplificación de los mecanismos de extradición en este entorno, y ahora ya se da un paso más: desaparece el clásico procedimiento de extradición y es sustituido por un procedimiento ágil, sencillo y estrictamente judicial de entrega en las relaciones de cooperación judicial entre los Estados miembros de la Unión Europea. En lo que ahora interesa, por lo que concierne a la armonización legislativa, este sistema recoge una importante novedad: cuando se implante el mismo, quedará en el seno de la Unión Europea incorporado el principio de reconocimiento mutuo. Respecto al amplio catálogo de categorías delictivas establecida en la Decisión marco de 17 de julio de 2002, ya no se precisará la exigencia de doble incriminación. La trascendencia que esto tiene en materia de *criminalidad informática* es grande, porque en hechos como el denominado *hacking* o intrusismo informático, no se ha alcanzado acuerdo acerca de la procedencia de una tipificación autónoma. En todo caso, es una solución que puede terminar con desajustes y falta de coincidencia entre el Derecho penal de cada país[31]. No obstante, a todas luces ha sido insuficiente la supresión del requisito de la «doble incriminación» en la parcela que aquí más nos interesa, habida cuenta de que, sólo en los últimos dos años se han sucedido varias disposiciones, directivas y recomendaciones del Parlamento europeo y del Consejo relativas a diversas parcelas de la *Ciberdelincuencia*[32], al tiempo que se crea la Agencia Europea de Seguridad de las Redes y de la Información[33].

❖ Otro nivel imprescindible de cooperación para la consecución del objetivo de crear un «espacio judicial único» es el de los organismos judiciales de lucha contra la Delincuencia. En este plano, puede afirmarse que el grado de coordinación es elevado, si bien está llamado a avanzar sustancialmente con la efectiva puesta en marcha de todo el sistema proyectado. En un apretado repaso a las principales líneas de cooperación judicial, debe mencionarse:

1º. Acerca de la posibilidad de comunicación directa entre las autoridades judiciales de los distintos Estados miembros, ya desde la llegada del Convenio de aplicación del Acuerdo de Schengen, de 19 de julio de 1999, se incluía como novedad relevante dicha opción a la hora de solicitar o remitir peticiones de

[31] *Ibidem*.

[32] Merece, a mi juicio, ser destacadas dos dimensiones que no son sino los dos lados de la moneda, en el sentido en que nos referimos al principio: Por una parte, existe una gran preocupación por evitar que los mecanismos arbitrados para la mayor eficacia en la represión de las formas más graves de delincuencia terminen con todo un valioso (y costoso) entramado de garantías individuales. En estas coordenadas hay que entender, por ejemplo, el tenor (garantista) de las Normas del Reglamento interno de Eurojust relativas al tratamiento y a la protección de datos personales, aprobado por el Consejo el 24 de febrero de 2005(2005/C 68/01); por otra parte, se pone de relieve el interés por fomentar un uso más seguro de Internet y las nuevas tecnologías en línea (al efecto, merece citarse la Decisión Nº 854/2005/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a esta cuestión), y el tema tan sensible de la explotación sexual de los niños y pornografía infantil (Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra aquellos delitos).

[33] Cfr. Reglamento (CE) Nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

asistencia judicial (sin seguir la tradicional vía diplomática). El Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, de 29 de mayo de 2000, contempla con carácter general como medio principal de transmisión de solicitudes el contacto directo entre las autoridades judiciales, aunque con excepciones. No obstante, se permite también el envío de solicitudes y respuestas a través de las autoridades centrales de los Estados miembros (por ejemplo, en casos complejos o en casos en que la solicitud se envía a más de una autoridad competente del Estado miembro requerido). Además de otros relevantes aspectos novedosos, en el texto se incluyen previsiones acerca del intercambio espontáneo de la información que cada respectivo Estado miembro haya obtenido en el ámbito penal, y ello sin que sea preciso la solicitud de la autoridad judicial. (Ante los riesgos que para los derechos y libertades fundamentales de las personas puede representar, por mor de las modernas tecnologías, este intercambio permanente de información, el Convenio presta una especial atención al problema de los límites en el uso y transmisión de datos de carácter personal).

2º. Para facilitar los cauces de cooperación en este extremo, se han arbitrado, adicionalmente, otros instrumentos como los *Magistrados de enlace*, creados por la Acción común de 22 de abril de 1996, adoptada por el Consejo, para facilitar el intercambio de magistrados de enlace y mejorar la coordinación en su actuación; además, la *Red Judicial Europea*, que es, en realidad, otra institución articulada en la Decisión del Consejo de 28 de mayo de 2001 dentro del mismo proyecto de ayuda judicial mutua entre los Estados, pero que centra su actividad en los diferentes aspectos de la prevención de la delincuencia a escala de la Unión, además de apoyar las acciones de prevención de la delincuencia a nivel local y nacional (la *Red Judicial Europea* se compone de las autoridades centrales de cada Estado miembro responsables de la cooperación judicial internacional y de uno o varios puntos de contacto en cada Estado miembro; se prevé, en todo caso, la posibilidad de asociar a la misma a los *magistrados de enlace*).

3º. El proyecto de cooperación en el plano judicial se completará con la puesta en marcha de *Eurojust*, unidad creada por Decisión del Consejo de 28 de febrero de 2002 con el objeto de intensificar la lucha contra las formas más graves de delincuencia organizada. Integrado por jueces, fiscales y funcionarios de policía de los estados miembros, tiene asignadas muy amplias competencias, tanto en la investigación y actuaciones por hechos delictivos que afecten a dos o más Estados miembros, como en casos que afecten a uno sólo o a un Estado miembro y un tercer país (a petición de la autoridad competente del país miembro afectado). El marco de competencias es tan amplio, como ya se ha referido en otro lugar, que ya incluiría cualquiera de las formas más graves de *Ciberdelincuencia* transnacional aunque no hubiese específica alusión a la misma. El art. 42 exhorta a los Estados miembros a la adaptación de sus legislaciones internas para que *Eurojust* esté en marcha desde el 6 de septiembre de 2003.

4º. El último paso en el ámbito de la Unión Europea, aún en el nivel de la cooperación judicial, lo hallamos en la tan citada *Euroorden*, con la plena judicialización de todo el procedimiento de detención y entrega de procesados o sentenciados requeridos por un Estado miembro a otro. Se pone fin a la intervención y decisión última de instancias políticas de los Estados, para convertirse en un procedimiento simple de comunicación entre autoridades judiciales. Junto al importante avance que esto implica, no debe olvidarse otro principio tradicional en materia de extradición que también se conmociona definitivamente con la implantación de la *Euroorden*. Nos estamos refiriendo, desde luego, al principio de «no entrega de los nacionales», que ya se había intentado

superar para los Estados miembros de la Unión en el Convenio de Extradición de 1996, si bien desde entonces ya dejó de concebirse como un principio incondicional.

❖ El tercer gran puntal para lograr el *espacio judicial único* lo constituye el plano de la cooperación policial en el ámbito de la Unión Europea. Sin duda, estamos ante un eslabón imprescindible, como ya queda reflejo en el mismo Tratado de Maastricht, donde se acordó la creación de EUROPOL. Con sede en La Haya, EUROPOL inició sus actividades el 3 de enero de 1994 como «Unidad de drogas EUROPOL», con operaciones limitadas en esta clase de delincuencia. Posteriormente se añadieron otros ámbitos importantes de criminalidad, hasta perfilarse en sus competencias actuales por el Convenio de Europol, que entró en vigor el 1 de octubre de 1998, y entró plenamente en funcionamiento en julio de 1999. La Oficina Europea de Policía es la organización de cumplimiento de la ley en la Unión Europea que gestiona la información criminal. Su principal objetivo es mejorar la efectividad y cooperación de las autoridades competentes de los Estados miembros en la prevención y lucha contra la delincuencia organizada grave internacional. Habida cuenta de la extensa lista de delitos cuya prevención e investigación se puede encargar Europol, puede afirmarse que en la actualidad tiene competencia sobre la totalidad de manifestaciones de la criminalidad moderna transnacional (ni las figuras delictivas más clásicas, como homicidios, lesiones, secuestros...) llegan a escapar de su conocimiento si así se le encomienda, como establece el Anexo al Convenio). A esta relevante institución debe añadirse, tras la creación de *Eurojust* y la *Euroorden*, la creación de los ya citados *Equipos conjuntos de investigación*, que han de actuar sometidos a la legislación del Estado donde desarrollen sus funciones.

Para completar estas rápidas pinceladas sobre el diseño del nuevo modelo proyectado para la represión de las formas más graves de la delincuencia de carácter transnacional surgidas o potenciadas por el impacto de las modernas tecnologías deberíamos ahondar, a continuación, en el proceso que paralelamente viene siguiendo para la cooperación judicial en otras materias, como el «Crimen organizado y lavado de activos en el marco de la *globalización*» y el terrorismo internacional (mecanismos de cooperación internacional para su prevención y represión, incluyendo la vigilancia, el control y bloqueo de las fuentes de financiación). Como esa tarea desborda con creces las posibilidades de la presente intervención, cerramos ahora el apartado reiterando nuestras críticas por la ausencia de una coordinación más seria entre tantas iniciativas, muchas de ellas yuxtapuestas y redundantes.

## IV. A modo de conclusión (de vuelta al Derecho penal español).

Terminamos estas líneas volviendo a nuestro punto de partida, circunscribiéndonos ya al Derecho español. No perdemos de vista que la problemática que debíamos afrontar se refería a la vigencia de la ley penal en el *ciberespacio*. Detectado y denunciado uno de los llamados *ciberdelitos* ante los Tribunales españoles, ¿quién y cómo conoce, investiga y lleva la iniciativa de las actuaciones? ¿A qué autoridad judicial corresponde resolver y conforme a que Derecho?

Con carácter general, en la línea que ya se indicó anteriormente, nuestro ordenamiento jurídico acepta con nitidez el principio de territorialidad de las leyes penales en el art. 8.1 del Código Civil, donde se establece: «Las leyes penales, las de policía y las de seguridad pública obligan a todos los que se hallen en territorio español». Tal

pronunciamiento sobre la vigencia espacial del Derecho punitivo español, con independencia de la nacionalidad del infractor, encuentra su adecuado complemento en el art. 23.1 de la Ley Orgánica del Poder Judicial (LOPJ), referida a la competencia de los órganos judiciales españoles: «En el orden penal, corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español, o cometidos a bordo de buques o aeronaves españolas, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte». El precepto se completa con las excepciones al referido principio de territorialidad (supuestos en los que los Tribunales españoles son declarados competentes para aplicar la ley española a hechos cometidos en el extranjero, por virtud de los principios, también de aceptación internacional, ya conocidos: principio personal, principio real o de protección y principio de justicia universal. (Sobre las exigencias y requisitos legalmente previstos, véanse los números 2, 3, 4 y 5 del citado art. 23 LOPJ, reformado por la LO 11/1999, de 30 de abril, por la se pretende compatibilizar la legislación interna con tratados internacionales o «actos normativos de una Organización internacional de la que España sea parte»).

Como se ha defendido más arriba, la utilización pervertida y abusiva de las altas tecnologías en la dinámica comisiva de un hecho ilícito no cambia ni la naturaleza de éste (el delito seguirá siendo, por ejemplo, una estafa, o un delito de falsedad documental, o de blanqueo de capitales o fraude fiscal...) ni las reglas tradicionales de vigencia espacial de la ley penal. Evidentemente, pueden plantearse problemas adicionales de detección, prueba y persecución, pero no se modifican con carácter general los criterios clásicos.

Sin embargo, cuando se ponga en marcha el Convenio del Consejo de Europa sobre la Ciberdelincuencia (que España hasta el momento sólo lo ha firmado), las reglas que fija dicho texto operarán con carácter supletorio en defecto de otro Convenio bilateral o multilateral más específico.

En el espacio supranacional más reducido de la Unión Europea, adicionalmente, habrán de tenerse en cuenta los principios en que se materializa el proyecto del *espacio judicial único europeo*, en el sentido y con los mecanismos que en breve resumen hemos mencionado. A tal efecto, conviene ahora recordar que las manifestaciones de *criminalidad cibernética* dentro de la Unión, al menos las más relevantes, entran en el plan, parcialmente en marcha, de máximo nivel de cooperación judicial (además de mencionarse de forma expresa, según se indicó, la *Ciberdelincuencia*, estaría de forma implícita incluida a través de la «versión *cibernética*» de cualquiera de los delitos más graves y preocupantes hoy, especialmente las tipologías delictivas subsumibles en el llamado *Crimen organizado transnacional*). Esa cooperación privilegiada, con la superación efectiva de las fronteras nacionales en la represión de la delincuencia moderna, ya se viene desarrollando con un grado notable de eficacia, particularmente en el orden policial y judicial, con flujo permanente de información, con la actuación de Europol y grupos específicos de investigación conjunta y, en suma, tratando de equilibrar los riesgos de la Sociedad de la Información mediante la utilización racional de las modernas tecnologías también en la lucha contra la delincuencia.

De momento, dentro de nuestro Derecho interno, se están colocando los pilares imprescindibles para la implantación del complejo y ambicioso proyecto de la Unión Europea en material de auxilio judicial, pero, como ya sabemos, su verdadera eficacia está al albur de la adopción o no de la *Euroorden* por los países vecinos. Destacamos, por su trascendencia en la materia que estudiamos y su proximidad:

- ❖ Ley 3/2003, de 14 de marzo, sobre la orden europea de detención y entrega, donde se viene a incorporar a nuestro ordenamiento jurídico el procedimiento ágil y estrictamente judicial de entrega en el seno de la Unión Europea, de acuerdo con la Decisión marco de 2002, poniéndose fin, entre los Estados miembros, el instituto

clásico de la extradición. (Cuanto se apuntó anteriormente respecto a la superación del principio de doble incriminación y del principio de no entrega de los nacionales, es ya una realidad en España, siempre en este contexto europeo, y sólo respecto a los Estados miembros que también hayan adaptado sus legislaciones a la Decisión marco, según se indica en la Disposición transitoria segunda).

❖ De la misma fecha, la Ley Orgánica 2/2003, de 14 de marzo, complementaria de la Ley sobre la orden europea de detención y entrega, adapta la LOPJ para ampliar las competencias de la Sala de lo Penal de la Audiencia Nacional y de los Juzgados Centrales de Instrucción en relación con la tramitación de expedientes de ejecución de las ordenes europeas de detención y entrega.

❖ Mención especial merece, a nuestro juicio, la Ley 11/2003, de 21 de mayo, reguladora de los equipos conjuntos de investigación en el ámbito de la Unión Europea. Con ella se pretende, según expresa el legislador en su Exposición de Motivos, incorporar al Derecho español los mecanismos necesarios para la implantación de estos equipos en el sentido proyectado por la Decisión marco, contribuyendo así a acelerar el proceso hasta su puesta en marcha. La lectura detallada del texto nos permite inferir que se da carta de naturaleza con carácter general a un sistema que desborda la idea misma de «cooperación», para entrar en la «actuación conjunta» en la prevención e investigación criminal.

❖ Finalmente, también deben ser consideradas otras disposiciones próximas con trascendencia en la creación del *espacio judicial único europeo*, en la medida en que arbitran mecanismos para la cooperación internacional en la lucha contra las más graves formas de delincuencia a través del seguimiento y control de las transacciones financieras electrónicas: nos referimos en concreto a la Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo. Este texto, dentro del específico Plan de Acción contra el Terrorismo (objetivo prioritario de la Unión Europea según se decidió por el Consejo extraordinario de Jefes de Estado y de Gobierno de 21 de septiembre de 2001), se integra en la línea continua de políticas de prevención de formas especialmente graves de delincuencia, como el blanqueo de capitales y tráfico de drogas. Es por eso que debe conectarse con otros textos legislativos, como la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, o la Ley 40/1979, de 10 de diciembre, sobre régimen jurídico de control de cambios, instrumentos todos de prevención y evitación del delito desde la perspectiva de su financiación.

La situación actual en nuestro país, como se puede inferir de este rápido repaso, se caracteriza, como en toda la Unión Europea, por su provisionalidad. La idea de que es imprescindible superar barreras tradicionales para afrontar el fenómeno de la delincuencia moderna está cada vez más viva en nuestro entorno más próximo. Pero la idea de la *globalización* (en todas las vertientes, incluida la criminal), exige como correlato la *solidaridad*. Los países más avanzados que están impulsando la *globalización*, cada vez son más conscientes de que, en esa *aldea global*, la seguridad pasa por la cooperación y la solidaridad. Es imprescindible evolucionar hacia cotas más altas de cooperación en *toda* la Comunidad internacional. Los pasos en el marco europeo hacia un *espacio judicial único* son sólo el «prólogo» de una historia que acaba de empezar.

La utilización pervertida de las altas tecnologías reportan al delincuente, sin duda, un abanico amplio de medios para facilitar la comisión, incrementar sus efectos, y propiciar la impunidad, con el recurso adecuado a vías de enmascaramiento y ocultación. Pero ya es una realidad incuestionable incrustada en las expresiones más graves de la delincuencia

moderna. La llamada *Ciberdelincuencia*, que ha sacado máximo rendimiento al desarrollo y expansión de las nuevas tecnologías, y que ha encontrado un espacio desconocido, ilimitado e incontrolable, el *espacio virtual*, sólo podrá ser combatida con las mismas armas: aprovechando las nuevas posibilidades que ofrece la Sociedad de la Información en la prevención, investigación, prueba y represión del hecho criminal, superando las trabas que representan las fronteras de los Estados. Sin embargo, el gran reto de la Justicia penal en las democracias actuales consiste en alcanzar, una vez más, el máximo posible en seguridad y eficacia, con la mínima restricción de garantías y libertades fundamentales de los ciudadanos (el difícil equilibrio en que opera el Derecho Penal, tan sensible a los eventos políticos y sociales, y que en el momento presente, sobre todo desde el atentado del 11 de septiembre de 2001 en Nueva York, se inclina peligrosamente a favor de la seguridad, con grave sacrificio para las garantías).