UOC
IN3 Internet Interdisciplinary Institute
www.uoc.edu

Documento de trabajo

Política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre delincuencia informática

Óscar Morales (omorales@uoc.edu)
Profesor de Derecho penal (UOC)
Investigador (IN3-UOC)

Working Paper Series WP03-001
Proyecto de investigación: Sociedad de la información y Derecho Penal. Política criminal en el contexto de la globalización (E-crime)
Fecha de publicación: junio de 2003
Internet Interdisciplinary Institute (IN3): http://www.uoc.edu/in3

RESUMEN

La expansión de las tecnologías de la información, y en particular de Internet, favorece el proceso de globalización económica y cultural y, por consiguiente, el desarrollo, pero, al mismo tiempo, abre la puerta a nuevas formas de vulneración de bienes jurídicos, clásicos y emergentes, en la medida en que el propio mecanismo de transmisión de datos se conforma como sector de riesgo. El carácter transfronterizo de este tipo de conductas reclama normas homogéneas en todo el planeta, si no se quiere favorecer la incertidumbre y, con ello, la inseguridad jurídica y la vulnerabilidad de bienes de primer orden. En esta lógica nace lo que hasta el momento es el proyecto legislativo más ambicioso en materia de delincuencia asociada al uso de las tecnologías de la información y la comunicación, esto es, la Convención del Consejo de Europa sobre aspectos relacionados con la delincuencia informática, hecha en Budapest el 23 de noviembre de 2001. En ella, se contienen las bases que deben regir en la creación nacional de normas penales. No contiene, pues, un mandato de transposición literal de una norma, sino un mandato, una vez ratificada la norma, de transposición de sus bases. En definitiva, la Convención contiene un texto articulado que en realidad esconde una valoración político-criminal sobre el uso de las nuevas tecnologías. Dicha valoración deberá ser reestudiada en el momento de la transposición a los diversos estados, que aún tendrán un cierto margen para la asunción de, o la renuncia a, las políticas de máximos que en ocasiones se contienen en la Convención, en una constante tensión entre libertad y seguridad o a veces libertad y control. En el presente trabajo se estudia, básicamente, la primera parte del texto supranacional, relativo a los tipos penales: accesos ilegales, o abusivos, posesión de tecnologías de doble uso, infracciones de contenidos (propiedad intelectual y pornografía infantil), infracciones patrimoniales (falsedades sobre documento electrónico, estafas y daños informáticos) y algunos institutos de la parte general, como la responsabilidad de las personas jurídicas. Se trata, en definitiva, de descubrir las razones que inspiran la creación de tales tipos penales y su adecuación a las reglas del juego de la Unión Europea y los Derechos constitucional y penal españoles.

PALABRAS CLAVE

Convenio sobre delincuencia informática, Convención del Consejo de Europa sobre delincuencia informática, falsedad en documento electrónico, estafa informática, daños informáticos, sabotaje informático, pornografía infantil, denegación de servicio

Para citar este documento, puedes utilizar la siguiente referencia:

MORALES, Óscar (2003). *Política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre delincuencia informática* [documento de trabajo en línea]. IN3 : UOC. (Working Paper Series; WP03-001) [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/in3/dt/20243/index.html>

Política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre delincuencia informática

I. La Convención del Consejo de Europa sobre delincuencia asociada a las tecnologías de la información

La emergencia del fenómeno tecnológico y su generalización, su democratización, si se quiere, ha oscilado entre la libertad como máxima en los momentos iniciales y el intervencionismo actual, cuando la técnica revela posibilidades de control institucional más que sugerentes.[1] Ciertamente, la denominada *sociedad de la información* que nace al abrigo de las tecnologías –no sólo de carácter telemático, sino también de otro tipo, como el cable o la televisión digital– transforma las relaciones sociales y jurídicas de un modo incontestable e impresionante.[2] Los ejemplos que podrían concurrir ahora son múltiples y tal vez sea conveniente apuntarlos sin orden aparente. La confidencialidad de los mensajes mediante sistemas de encriptación invulnerables y la posibilidad de certificar la identidad del emisor de modo tanto o más seguro que mediante los sistemas actuales de certificación[3] (fe pública) ejerce de catalizador en la reflexión sobre el sistema democrático mismo y el sistema de elección de los representantes. Se habla, así, de *democracia electrónica*, queriéndose subrayar con ello el nacimiento de un nuevo modo de concebir la participación ciudadana, no sólo en la elección de los representantes, sino en la toma de decisiones por parte de éstos. La propia especulación sobre el particular genera la necesidad de estudios sociológicos sobre la repercusión que un sistema de participación cotidiano y directo conlleva en el modo de realización política de los principios básicos del Estado democrático. Y si los propios fundamentos del Estado se remueven con la irrupción de tecnologías capaces de comunicar todo el planeta en tiempo real y de acceder a cualquier género de información, las relaciones sociales primarias sufren el mismo efecto. En el ámbito laboral, la posibilidad de ejercer la función, pública o privada, lejos del habitual puesto de trabajo, sin necesidad de desplazamiento, abre un nuevo paradigma de las relaciones laborales, donde apremian las preguntas sobre los nuevos modelos de sindicación, control del desempeño de la actividad laboral,[4] régimen de seguridad social, determinación de nuevas enfermedades laborales, compatibilidad de determinadas situaciones de incapacidad laboral según el sistema clásico con el desarrollo de la actividad desde el domicilio.[5] Del mismo modo, el sector empresarial se ve abocado a la adaptación tecnológica, hasta el punto de que la misma transforma los esquemas clásicos de organización, marketing e intercambio de productos. La supresión de intermediarios en la distribución, la comunicación en línea entre empresas (*business to business*, simbolizado como B2B), o entre particular y empresa, genera nuevas estructuras organizativas y, al mismo tiempo, nuevos ámbitos necesitados de tutela

1. *Vid.* un análisis de la evolución institucional en relación con la expansión tecnológica en MORALES GARCÍA, O. (2001). "Criterios de atribución de responsabilidad penal a los prestadores de servicios de la sociedad de la información". *Revista de Derecho y Proceso Penal*. Nº 5, págs. 140 y sigs., y bibliografía allí citada.
2. La idea en general se desarrolla con amplitud en CASTELLS, M. *La era de la información. Economía, sociedad y cultura*. Vol. I. *La sociedad red*, traducción de Carmen Martínez Gimeno (1997 *passim*.). *Vid.*, entre otros, FERNÁNDEZ ESTEBAN. (1998). *Nuevas tecnologías, Internet y derechos fundamentales*. Pág. XXIII; CAPELLER, W. (2000). *Not such a neat net. Some comments on virtual criminality*. Pág. 3.
3. Sobre el modo en que opera técnicamente la firma electrónica avanzada y la capacidad de garantía de la integridad del documento y la identidad del emisor, véase MORALES GARCÍA O. (2001). "Malversación, estafa informática y falsedad en documento electrónico. Algunas reflexiones sobre la sentencia del Tribunal Supremo de 30 de octubre de 1998". En: *El nuevo Derecho penal español. Estudios penales en memoria del profesor José Manuel Valle Muñiz*. Aranzadi, pág. 1.595 y sigs.
4. Sobre ello, MORALES GARCÍA, O. (2001, octubre). "La tutela penal de las comunicaciones laborales. A propósito de la estructura típica del artículo 197 CP". *IURIS*. Pág. 48 y sigs.; JEFFERY, M. *¿Carta blanca para espiar a los trabajadores?*, en <http://www.uoc.edu/web/esp/art/uoc/0109042/jeffery.html[url1]>.
5. *Vid.* un interesante planteamiento de estas cuestiones en LEONES SALIDO. (2000, marzo). "Razones urgentes para una regulación del teletrabajo en España". *AJA*. Nº 431, pág. 3 y sigs. En profundidad, en THIBAULT ARANDA J. (2000). *El teletrabajo*. Análisis jurídico-laboral. Pág. 125 y sigs.

primaria en el sostenimiento del nuevo modelo organizativo: tráfico de datos, seguridad en las transacciones comerciales, prevención de daños en los centros de comunicación individual y colectivos de la empresa (*v.gr.* frente a programas informáticos como los virus, gusanos, etc.).[6]

Hasta aquí se comprueba cómo la evolución tecnológica permite un incremento cualitativo de la calidad de vida; pero, del mismo modo que se constatan cambios en la estructura y el desarrollo social y económico, a la vez se abre la puerta a nuevas formas de perjudicar los legítimos intereses ajenos, bien sean individuales o colectivos.[7] La cuestión entonces radica en determinar el alcance de los cambios y efectuar prognosis ponderadas sobre los que vendrán y los riesgos que llevarán aparejados, como punto de partida en la fijación de intereses fundamentales en el nuevo marco de relación. Sólo así pueden aventurarse conclusiones sobre la necesidad de intervención del Derecho penal en un sector emergente y de apariencia caótica, en el que aún no han penetrado con decisión los instrumentos primarios de regulación, administrativo, civil, mercantil, etc. Y sólo así sabremos hasta qué punto las normas penales existentes son suficientes o reclaman una tan urgente y demandada modificación y adaptación a las tecnologías existentes.

En esta lógica nace lo que hasta el momento es el proyecto legislativo más ambicioso en materia de delincuencia asociada al uso de las tecnologías de la información y la comunicación, esto es, la Convención del Consejo de Europa sobre ciberdelito, si bien, como veremos a continuación, la ambición de las propuestas originales ha ido cediendo terreno paulatinamente en los diversos borradores hasta plasmarse en una convención político-criminalmente aceptable.

El Consejo de Europa, como institución supranacional que comprende más de cuarenta y cinco países del área continental europea, posee una importante trayectoria en el desarrollo de los derechos fundamentales, cuyo principal exponente sin duda reside en la aprobación de la Convención de los derechos del hombre, en 1950. La superación de la sociedad industrial y la incidencia de las tecnologías en los derechos y libertades individuales en el tránsito hacia la sociedad de la información tampoco han pasado desapercibidas al Consejo, del que han emanado textos con eficacia normativa limitada pero de un indudable peso político, como las Recomendaciones (87) 15, sobre la utilización de datos personales, o la (95) 4, relativa a la tutela de los datos personales en el ámbito de las telecomunicaciones. En línea con esta trayectoria, en noviembre de 1996 "el Comité Europeo sobre problemas penales", es decir, el órgano del Consejo de Europa encargado del diseño de la política criminal de la Institución, en guardia por la vertiginosa evolución tecnológica y las nuevas amenazas a la seguridad y los consiguientes nuevos riesgos para bienes jurídicos de primer orden como la intimidad o el patrimonio, adoptó la decisión de crear un comité de expertos para trabajar sobre el fenómeno de la delincuencia asociada a la tecnología, y ello bajo una máxima sin duda presente en las primeras versiones de la Convención: la dependencia social, económica y cultural de la información contenida en las redes de comunicación, particularmente en Internet, obliga a la tutela de los bienes jurídicos fundamentales que se encuentran en juego; en definitiva, bajo la filosofía según la cual la sucesión histórica del modelo de sociedad, en la que ahora todos podemos ser sujetos activos y pasivos de la información, reclama una regulación (también) penal armónica y global, como global es la sociedad de la información.

En este contexto, el Comité de Ministros nombró un comité de expertos en delincuencia informática en el ciberespacio en 1997, al que estableció como fecha límite para la finalización de sus trabajos y entrega de una propuesta al Comité el 31 de diciembre de 1999, plazo prorrogado luego por espacio de un año. El 27 de abril de 2000 los trabajos preparatorios fueron desclasificados y se hizo pública y abierta a la discusión la versión nº 19, ampliamente modificada hasta llegar a la última y definitiva versión 25.2, aprobada en junio de 2001 por el plenario del Comité de Ministros del Consejo de Europa, y abierta a la firma el 23 de noviembre de 2001, en la reunión del Consejo de Europa en Budapest.

La estructura, contenido y alcance de la Convención puede explicarse cabalmente por la falta

6. *Vid.*, en general, el informe de la KPMG's Assurance & Advisory Services Center. VARIOS AUTORES. (2000, junio). *E-commerce and cybercrime: new strategies for managing the risks of exploitation*, en <http://aci.kpmg.com.hk/docs/evolving issues/ecommerce and cyber crime.pdf[url2]>, pág. 2 y sigs., última revisión 22 de septiembre de 2000.
7. Reflexión genérica que, en relación con la denominada sociedad de riesgos o sociedad postindustrial, puede verse en SILVA SÁNCHEZ. (1999). *La expansión del Derecho penal. Aspecto de la política criminal en las sociedades postindustriales*. Pág. 22.

de iniciativas internacionales o supranacionales en esta materia, lo que en su momento propició la toma de decisiones de especial trascendencia sobre la Convención.

a) En primer lugar, la decisión de trabajar sobre una convención y no tanto sobre una recomendación, vista la necesidad de armonizar la legislación de los diversos países pertenecientes al Consejo de Europa, no sólo en materia penal sustantiva, sino también en el ámbito procesal y de colaboración administrativa internacional, esto es, coordinación de la acción policial, recogida de datos en la investigación criminal, etc.[8] El recurso a una convención permite ampliar satisfactoriamente el conjunto de materias objeto de negociación por los países que intervienen en ella, pero, sacrificando en consecuencia la profundidad y por lo que la firma del texto no significará su inmediata transposición, sino la asunción de compromisos de política jurídica general o política criminal en particular, según los casos, de acuerdo con los marcos generales descritos en la Convención.[9]

b) En segundo lugar, la decisión de abrir a la firma la propuesta a países ajenos al Consejo de Europa, y cuya participación activa ha condicionado, sin duda, parte de la estructura y contenido del articulado,[10] como se explicará inmediatamente.

En efecto, el borrador de propuesta del Consejo de Europa de 27 de abril de 2000 asumió en cada uno de los ámbitos de afectación políticas de máximos en las que la cesión de garantías sobre los poderes públicos fue puesta de manifiesto desde una multiplicidad de instituciones,[11] de modo que se focalizó la atención en los siguientes aspectos:

1. Cesión a las autoridades administrativas de parcelas de autogobierno en el uso de las tecnologías, como el acceso no autorizado a máquinas, a los solos efectos de la investigación criminal, sin concesiones a los aspectos esenciales de preservación de la información. La Unión Europea, a través de la Opinión 4/2001, sintetizó su preocupación en torno a la participación en la Convención de países ajenos al Consejo de Europa y, por lo tanto, a su tradición jurídica.[12] Así, mientras que los países pertenecientes a la Unión Europea transpusieron a su Derecho interno las diversas directivas emanadas del Parlamento sobre la tutela de datos personales, e incluso los países pertenecientes a la órbita del Consejo de Europa han debido asumir la política inherente a las recomendaciones sobre la misma materia, los estados ajenos a la UE o al Consejo de Europa no se encuentran vinculados a dicha normativa. De ahí que, amén de la evidente diversidad filosófica en la tutela de datos personales existente entre Europa y Estados Unidos, nos encontremos ahora con la posibilidad de que cada estado ofrezca a los datos personales obtenidos en un país de la Unión o el Consejo en el curso de una investigación criminal una tutela jurídica muy inferior a la exigida en aquellos entornos territoriales, de modo que se rompa la pretensión armonizadora y se deje a la legislación doméstica la salvaguarda efectiva de los derechos fundamentales. Las amplísimas concesiones en materia de datos de carácter personal se extienden no sólo a los obtenidos en el decurso de una investigación policial, sino a la cesión misma de datos necesaria para la investigación en países ajenos al entorno del Consejo, obligatoria desde el momento en que fueren solicitados por el estado parte de la Convención y cuya elusión sería factible únicamente previa expresa reserva a la eficacia del precepto, basada en motivos de orden público o relativos a la seguridad y defensa nacionales.[13] A mayor abundamiento, la Unión Europea puso de manifiesto cómo del artículo 15 del borrador, en su redacción de 27 de abril de 2000, "podría llegar a generarse la impresión de que la tutela de los derechos fundamentales será observada sólo cuando fuere debida y, en todo caso, de forma sólo 'adecuada'. Más aún, consideraciones sobre la proporcionalidad de los poderes o procedimientos según la naturaleza y circunstancias de la conducta investigada no se contemplan como principio general de

8. En la base de esta decisión, tal y como se reconoce en la exposición de motivos de la Convención, se encuentra el estudio del profesor Kaspersen titulado *Implementation of Recomendation Nº R (89)9 on computer-related crimes*, realizado por encargo del propio comité de expertos. La exposición de motivos puede consultarse en línea en <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm[url3]>.
9. El referente normativo más cercano lo constituyen las directivas de la UE, donde los estados, en el acto de transposición, sólo se encuentran condicionados por las directrices generales, sin que ello afecte necesariamente al instrumento jurídico empleado en la satisfacción del mandato de la Directiva.
10. En concreto, han participado activamente en la redacción de los diversos borradores Estados Unidos, Canadá, Australia y Japón, entre otros.
11. En efecto, mediante escrito de 13 de octubre de 2000, la Global Internet Liberty Campaign, integrada por un conjunto de agrupaciones de carácter civil con peso específico en los procesos de toma de decisiones, como la American Civil Liberties Union o el Electronic Privacy Information Center (EPIC), entre otros, manifestó su desacuerdo con la redacción original del borrador de 27 de abril, justo en el momento en que veía la luz la segunda versión de la propuesta, hecha pública el 2 de octubre de 2000 e inmediatamente rectificada en su tercera versión, de 19 de noviembre de 2000. En el documento emitido, disponible en <http://www.gilc.org/privacy/coe-letter-1000-es.html[url4]>, se pone de manifiesto la política de control excesivo seguida en el borrador, mientras que en los sucesivos se recogen algunas de las demandas y se ignoran otras que en la versión definitiva tampoco han encontrado acomodo.
12. Puede consultarse el texto íntegro de la Opinión 4/2001, adoptada el 22 de marzo de 2001 por la UE, en <http://www.uoc.edu/in3/dt/20243/opinion_4-2001.pdf[url5]>.
13. Opinión 4/2001[url6], página 5.

actuación, sino que serán observados sólo 'cuando sean aplicables'.[14] Si ello se interpreta como una limitación de las garantías y procedimientos, entonces los derechos fundamentales deberán entenderse infralegalmente protegidos, si no absolutamente desprotegidos".[15]

2. Obligación de los prestadores de servicios de la sociedad de la información de registrar la actividad de los usuarios y almacenar los datos resultantes, con el consiguiente riesgo para la intimidad y los datos personales de los usuarios, y el normal funcionamiento de las redes telemáticas, obligación ésta, no obstante, finalmente excluida del texto definitivo del tratado, principalmente por la falta de acuerdo entre la Unión Europea y el Consejo de Europa.[16] La UE, a través de la Recomendación 3/1999 sobre la conservación de los datos de tráfico por los proveedores de Internet, expresó ya antes de la primera versión de la Convención hecha pública por el Consejo de Europa su oposición a medidas de intervención sobre el tráfico de datos. La Recomendación, elaborada por el "Grupo del artículo 29",[17] expresó su preocupación respecto al almacenamiento de datos en los diversos países miembros de la UE. Consciente de la necesidad de controlar los datos que circulan a través de un servidor a los efectos de poder efectuar las oportunas labores de facturación de acuerdo con los datos recabados,[18] el Grupo trata de conciliar, además, las necesidades de investigación criminal en tiempo real,[19] con la indemnidad de los bienes jurídicos subyacentes.[20] De hecho, el Grupo considera en la Recomendación que el hecho de que un tercero llegue a poseer la información derivada del tráfico de datos a través de un servidor implicaría una violación de Derecho fundamental, en general constitutiva de delito, salvo que la medida de interceptación de la comunicación o su contenido[21] cumplan las exigencias jurídicas típicas de la afectación de derechos fundamentales recogidas en las diversas convenciones sobre los derechos del hombre, esto es, proporcionalidad de la medida, sólo adoptable allí donde no existan otros mecanismos alternativos para el desarrollo de la investigación, así como un fundamento claro para su adopción, en el que deberían reflejarse la duración, la finalidad, los medios técnicos que se emplearán y los límites de la interceptación. A idéntica conclusión sobre la política (criminal) en materia de retención del tráfico de datos por los proveedores se llega desde la lectura de la Directiva 200/31/CE, de 8 de junio, del comercio electrónico, en cuyos artículos 12 a 15, ambos inclusive, se contiene el régimen de responsabilidad de los prestadores de servicios de la sociedad de la información.[22] La Directiva, en este sentido, no sólo excluye la obligación de los prestadores de supervisar los contenidos que se alojan o transitan; tampoco se establece una obligación de retención del tráfico, justificada en los considerandos de la norma marco en la garantía del normal desarrollo del comercio electrónico, seriamente en entredicho si los operadores de Internet tuvieran que adaptar sus infraestructuras para poder albergar, más allá del tiempo estrictamente necesario para elaborar los datos de facturación, copia de todo el tráfico de datos circulante a través de sus servidores.[23]

14. Últ. *op. loc. cit.*
15. Opinión 4/2001[url7], página 4. La evolución del texto hasta la versión definitiva, sin embargo, enerva la preocupación apuntada en el texto. *Cfr.*, en este sentido, el contenido de la nota siguiente.
16. Como ha señalado LEZERTÚA, M. "El proyecto de convenio sobre el cybercrimen del Consejo de Europa". En: López Ortega (director). *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, pág. 34 y sigs., existe una evidente distancia entre los primeros proyectos de convención y la versión definitiva; diferencias que, en lo que respecta a las medidas de actuación procesal contra la delincuencia informática y en particular al almacenamiento de datos, su archivo, exhibición, entrada y registro o la interceptación en tiempo real de datos de tráfico o contenido (arts. 15 a 19), permiten un juicio positivo, dado que definitivamente tales medidas se cohonestan con el principio de proporcionalidad como eje cartesiano, así como con el nivel de garantías del Derecho interno.
17. Se denomina así al grupo de expertos para la tutela de las personas en relación con el tratamiento de datos de carácter personal, creado en virtud de lo dispuesto en el artículo 29 de la **Directiva 95/46/CE**, del Parlamento, sobre la tutela de las personas físicas en relación con el tratamiento de los datos personales y con la libre circulación de los datos.
18. El artículo 6.1. *b)* de la Directiva 95/46 permite a los prestadores el tratamiento de los datos personales siempre que dicho tratamiento se encuentre dentro de los límites dibujados por la propia Directiva, es decir, para el control del tráfico y la facturación.
19. Autorizada en cierto modo por el artículo 13 de la **Directiva 95/46**, cuando se refiere al control sobre los datos ejercido por los poderes públicos, previa autorización judicial.
20. Garantizada a través de lo dispuesto en el artículo 6 de la **Directiva 97/66/CE**, del Parlamento, que obliga a la destrucción de los datos o a que los mismos devengan anónimos tan pronto hayan cumplido con las necesidades de facturación, etc., con la finalidad de evitar interceptaciones innecesarias de la comunicación o los datos.
21. Téngase en cuenta, no obstante, que algunas partes de la comunicación son consideradas hoy, en particular a raíz de la Consulta 1/1999 de la Fiscalía, comunicación en sí misma, con la consiguiente proyección a dichas partes de la comunicación (número de teléfono empleado, IP asignada, lugar de destino de la comunicación, duración, etc.) del régimen propio del secreto de las comunicaciones. Sobre ello, *vid.* LÓPEZ MELGAREJO, A. (2002). "Investigación criminal y proceso penal: las directrices de la propuesta del Consejo de Europa sobre *cybercrime* y de la Directiva del comercio electrónico". En: Morales Prats; Morales García (coordinadores). Varios autores. *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*. Actas del congreso celebrado los días 22 y 23 de noviembre de 2001 en el Colegio de Abogados de Barcelona. Pamplona: Aranzadi.
22. Ampliamente, sobre ello, PEGUERA POCH, M. "La exención de responsabilidad civil por contenidos ajenos en Internet". En: Morales Prats; Morales García (coordinadores). Varios autores. *Contenidos ilícitos y responsabilidad*, *op. cit., passim*.
23. Cabe efectuar aquí una prevención, relacionada con la norma de transposición de la Directiva del comercio electrónico, esto es, la Ley de servicios de la sociedad de la información y el comercio electrónico (LSSICE). En trámite de enmiendas en el Senado, el Grupo Popular incluía en la Cámara Alta un número cuarto al artículo 11, con la siguiente redacción: "4. Los operadores de redes y los proveedores de acceso a una red de telecomunicaciones que presten un servicio de la sociedad de la información deberán retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio por un período de doce meses. Estos datos, almacenados de manera automática, relativos al proceso de comunicación serán retenidos, de manera confidencial, a los solos efectos de que pueda ser necesaria su puesta a disposición de las autoridades judiciales o policiales en el marco de una investigación criminal como consecuencia de la comisión de un delito utilizando los servicios de la sociedad de la información". La enmienda, aprobada en el texto definitivo como artículo 12, se justificó, precisamente, en las mismas referencias normativas empleadas por el grupo de expertos del artículo 29 para recomendar la supresión de cualquier propuesta relativa al almacenamiento automático de datos a los fines de la investigación criminal, esto es, a las directivas de 1995 y 1997, sobre el tratamiento de datos personales. En definitiva, ha entrado por la ventana lo que tantos debates había costado echar por la puerta.

3. Tampoco las parcelas de orden sustantivo lograban sustraerse de la vis expansiva latente en la Convención, y particularmente las siguientes:

a) Delitos contra la propiedad intelectual. La propuesta original del Consejo de Europa consistió en hacer tabla rasa en materia de propiedad intelectual: los estados miembros deberían tutelar penalmente todas las infracciones de propiedad intelectual derivadas de las obligaciones asumidas en el Acta de París, la Convención de Berna y los tratados de la OMPI ratificados por los países firmantes. Dicha pretensión, desde luego carente de cualquier reflexión político-criminal, aún se mantiene en la redacción definitiva de la Convención, aunque con la opción de establecer reserva, siempre y cuando se garantice una tutela satisfactoria a través de otros medios jurídicos.[24]

b) Delitos contra la libertad sexual. La constatación del incremento de la difusión de pornografía infantil en las redes telemáticas se ha erigido en motor de una política criminal harto expansiva a la que España no es ajena, rehén de su propia historia legislativa reciente. El incremento de la difusión telemática, en efecto, ha originado un grave problema de discriminación de las conductas más graves que pueden producirse en este ámbito, al objeto de sancionar penalmente las de mayor lesividad, dejando extramuros del Derecho penal el resto. En la base de este incremento de la difusión de pornografía a través de nuevas tecnologías, y en particular de Internet, radica, pues, la causa por la que tanto las instituciones internacionales como las de carácter nacional han elaborado proyectos normativos alarmantemente expansivos sobre esta materia.

No se habla en este contexto de pornografía entre adultos, sino de pornografía en la que aparecen menores. La represión de este fenómeno no ha sido, lamentablemente, una constante en nuestro país. De hecho, el CP 1995 suprimió el delito de corrupción de menores, por las connotaciones que la figura delictiva llevaba aparejadas, con lo que la difusión de imágenes en las que aparecían menores en actitudes sexuales explícitas quedaban al margen de la tutela penal. Al no existir un delito específico que diera cobertura a estas infracciones se recurría a la utilización de menores en espectáculos exhibicionistas, lo que podía ser razonable para la utilización del menor en la captación de la imagen, pero no desde luego para la difusión de la misma, donde no quedaba rastro de vinculación normativa con el concepto "utilización", por más que algún sector doctrinal se empeñara en forzar la letra de la ley contra su tenor literal. En nuestro Derecho interno, por lo tanto, la cobertura penal de la difusión de pornografía infantil se produce sólo a partir de la reforma del CP de 1995 llevada a cabo por LO 11/1999, de 30 de abril.[25]

Por su parte, la Convención del Consejo de Europa hecha en Budapest, en vista de las dificultades para la punición de algunas de las conductas de mayor potencial lesivo y dado que no contiene normas penales sino "recomendaciones" a los estados para que incorporen normas penales en su ordenamiento interno, adoptó una propuesta amplísima sobre la materia, en toda su dimensión (concepto de pornografía y situaciones que la componen, así como conductas en torno a ella).[26]

24. En efecto, el artículo 10 de la Convención dispone en sus dos primeros números que:

"1. Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal, de conformidad con su Derecho interno, las violaciones a la propiedad intelectual tal y como ésta se entienda por su Derecho interno después de contraer las obligaciones derivadas del Acta de París de 24 de julio de 1971, de la Convención de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos comerciales de los derechos de la propiedad intelectual y del tratado de la OMPI sobre la propiedad intelectual, con excepción de cualquier derecho moral conferido por estas convenciones, siempre que esos actos sean cometidos deliberadamente, a escala comercial y mediante un sistema informático.

2. Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal las violaciones de los derechos conexos tal y como éstos se entiendan según su ordenamiento después de contraer las obligaciones derivadas de la Convención internacional para la protección de los intérpretes, ejecutantes, productores de fonogramas y entidades de radiodifusión firmada en Roma (Convención de Roma), del Acuerdo sobre los aspectos comerciales de los derechos de la propiedad intelectual y del Tratado de la OMPI sobre las interpretaciones, ejecuciones y fonogramas con la excepción de todo derecho moral conferido por estas convenciones, siempre que esos actos sean cometidos deliberadamente, a escala comercial y mediante un sistema informático."

25. Clara muestra de la anomia reinante en nuestro país lo constituye sin duda el suceso ocurrido en 1996 en el que dos estudiantes de la Universidad Politécnica de Cataluña distribuían imágenes de pornografía infantil –fotografías tomadas por terceros– desde un servidor ubicado en la localidad de Vic, lo que despertó la alarma social sobre el particular, al no existir figura legal en la que subsumir los hechos, por lo que fue sobreseído el asunto en vía penal. Respondiendo a la alarma social despertada, y en consonancia, por otra parte, con las propuestas de carácter internacional, el legislador introdujo el **artículo 189 *b)* CP**, según el cual: "será castigado con la pena de prisión de uno a tres años: el que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. A quien poseyera dicho material para la realización de cualquiera de estas conductas se le impondrá la pena en su mitad inferior."

La propuesta del Consejo de Europa es sin duda más explícita de lo que hasta ahora lo ha sido el CP español, no sólo porque define el concepto de pornografía (luego concretado al detalle en la amplísima exposición de motivos aludiendo a la conjunción de órganos genitales masculinos o femeninos heterosexual u homosexualmente entre sí, así como a la masturbación o exposición explícita de ano o genitales en solitario o tocamientos de dichas partes entre menores o por mayores a menores), sino también porque define las situaciones en las que tal exposición o tocamientos son pornografía infantil, y porque define, asimismo, de modo más amplio las conductas punibles sobre dicho espectro.[27]

Si en el Derecho español los problemas que se plantean, especialmente en cuanto a las garantías que deba ofrecer el proceso penal, son ya importantes con la punición de la posesión de pornografía infantil con fines de distribución, la transposición del artículo 9 de la Convención (a salvo reserva) o la aprobación del Proyecto de LO de modificación del Código penal introducido en el Congreso puede multiplicarlos. Y, aun cuando la materia es sin duda objeto de especiales sensibilidades, no deben dejar de subrayarse los problemas político-criminales y técnico-jurídicos que se plantean y que pueden resumirse del modo siguiente:

En primer término, suele partirse de la tutela de la libertad e indemnidad sexuales del menor como objeto de protección jurídico-penal en estas normas. Sin embargo, no es la libertad sexual lo que se encuentra en entredicho en la mayoría de conductas. Claramente ello es así en cualquiera de las que se proyecten sobre mayores que simulan ser menores. En este caso se trata de la punición de una tentativa absolutamente inidónea y, por lo tanto, impune, que, para no serlo, el legislador tipifica como delito autónomo. Lo mismo cabe decir, en relación con la denominada pornografía técnica, esto es, pornografía en la que se contienen imágenes realistas que parecen menores en actitudes sexuales explícitas, cuando no existe ningún ser humano en la realidad, mayor o menor.

En segundo lugar, en relación con las conductas de posesión para la distribución, se hace difícil encontrar una lógica en la pornografía infantil similar a la diseñada por la jurisprudencia para el tráfico de drogas. Así, ¿cuántas imágenes deben poseerse para realizar la conducta? ¿Si se excede de un número en concreto puede romperse la presunción de inocencia, como sucede en los delitos de tráfico de drogas? ¿Podrá mesurarse la cantidad en función de la calidad de las imágenes, de la edad de los menores, de la naturaleza homosexual o heterosexual de las mismas, etc.?

Por último, respecto a la conversión en delito de la posesión de pornografía infantil para autoconsumo, los problemas se multiplican. Tal vez se pierde de vista que en la cadena de explotación del menor el principal responsable es, y así debe ser, quien utiliza al menor, quien lo sustrae o quien lo engaña y capta sus imágenes para obtener un lucro con ellas o, simplemente, otro tipo de beneficios. Y tal vez por ello, se confunde igualmente al delincuente con el enfermo. Posiblemente, quien distribuye pornografía infantil es pedófilo (sexualmente aficionado a la sexualidad infantil) además de pederasta (explotador de la sexualidad infantil). Pero de lo que no cabe duda es de que quien únicamente consume, sin contribuir de otro modo a la cadena de explotación sexual, se encuentra, en el estadio cultural en que nos hallamos a escala planetaria, más próximo a la enfermedad o el daño psicológico que al delito, por lo que quizá sean necesarias, para la contención del mero consumo de pornografía infantil, otro tipo de medidas, de diverso tipo a la penal.

Con todo, la represión penal de la explotación sexual de los menores debe constituir un pilar de actuación en el seno de los procesos de transferencia de datos, dado el papel catalizador de Internet en la eclosión de redes de pederastia; aunque ello transite, como ha explicado Morales

26. Dispone así el artículo 9 de la Convención: **Infracciones relacionadas con pornografía infantil**. 1. Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal los siguientes comportamientos cuando sean intencionados y antijurídicos:

a) producir pornografía infantil con la finalidad de difundirla mediante un sistema informático;

b) ofrecer o poner a disposición pornografía infantil mediante un sistema informático;

c) difundir o transmitir pornografía infantil mediante un sistema informático;

d) procurarse o procurar a otros pornografía infantil mediante un sistema informático;

e) poseer pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

27. Por cierto, en sintonía en esta ocasión con la política de la UE, plasmada en la **Decisión del Consejo de 29 de mayo de 2000 relativa a la lucha contra la pornografía infantil en Internet** (2000/375/JAI), DOCE de 9 de junio de 2000, L 138/1 y Anteproyecto de ley orgánica por el que se modifica el Código penal, presentado por el Ministerio de Justicia y en el que se prevé la pena de prisión de tres meses a un año de prisión o multa de seis meses a dos años, para quien poseyera para su propio uso material pornográfico en el que hubieran sido utilizados menores de edad o incapaces. *Cfr.* MORALES PRATS, F. "Pornografía infantil e Internet. Ámbitos de incriminación". En: Morales Prats; Morales García (coordinadores). Varios autores. *Contenidos ilícitos*. *Cit., passim*.

Prats,[28] por multiplicar la capacidad de los delitos contra la intimidad y la imagen personal y familiar contenidos en los artículos 197 y sigs., principalmente para aquellos casos en los que la utilización del menor queda ya lejana y, por lo tanto, también el bien jurídico libertad sexual, entendido como libre desarrollo de su sexualidad. En todo caso, conviene recordar que la versión definitiva de la Convención (artículo 9) permite la formulación de reserva sobre la tipificación del autoconsumo, lo que en todo caso permitirá establecer límites a la distancia entre la lesión de un bien jurídico merecedor de tutela y el hecho penalmente relevante.

c) Concepto de dispositivos ilegales especialmente amplio y por ello distante de un bien jurídico claramente identificado,[29] exceso del cual parece tomar conciencia la propia Convención, obligada a establecer una suerte de interpretación auténtica en la propia configuración del precepto, aclarando que la amplitud de la prohibición no abarcará la producción, venta, etc., de dispositivos ilegales que no se efectúe con la finalidad de cometer alguna de las infracciones descritas en el articulado y llegando al extremo de incluir en el segundo párrafo ejemplos de lo que no deberá entenderse penalmente relevante, con lo que adelanta a la norma lo que debería formar parte, a lo sumo, de la exposición de motivos.[30]

4. Los desequilibrios de la Convención se muestran no sólo en el alcance de las propuestas, sino también en las omisiones, cuya causa, como ya advertí anteriormente, se encuentra directamente vinculada a la presencia de países ajenos al Consejo de Europa. Ninguna referencia se hace en la Convención a la necesidad de tutela penal de los datos de carácter personal frente a las agresiones más graves, o a la apología del terrorismo, el racismo o la xenofobia en Internet, o los delitos de injuria y calumnia, o sobre la responsabilidad de los prestadores de servicios e intermediarios por los contenidos ajenos. La propia exposición de motivos de la Convención[31] pretende aclarar la razón de ser de algunas de estas omisiones, refiriéndose a la falta de disposiciones en materia de delitos relativos a contenidos y, en particular, a la apología del racismo, no tanto por falta de consenso sino por falta de tiempo para la elaboración de una propuesta asumible por todas las partes.[32]

Las objeciones apuntadas y las que se efectuarán a continuación no deben empañar un juicio positivo a la iniciativa del Consejo de Europa. El evidente carácter transfronterizo de la delincuencia informática y la existencia de redes organizadas que utilizan las redes de información y comunicación en la realización de hechos delictivos, aconseja iniciativas legislativas más allá del estricto marco local, que no pueden obviar, sin embargo, las dificultades de armonización que presenta siempre la legislación penal. Ya hemos visto cómo el juego de equilibrios entre la tradición de cada uno de los estados provoca políticas de máximos en algunos sectores (cesión de datos, por ejemplo, o incluso el registro y almacenaje inicialmente previsto en el primer borrador desclasificado) u omisiones más que relevantes (apología, xenofobia, injurias); veremos también cómo esa misma diversidad está en la base de la redacción de las propuestas específicas de incriminación y las alternativas que la propia Convención ofrece.

28. MORALES PRATS, F. "Pornografía infantil e Internet. Ámbitos de incriminación". En: Morales Prats; Morales García (coordinadores). Varios autores. *Contenidos ilícitos*. *Cit.*, pág. 105 y sigs.

29. El artículo 6 de la Convención dispone: **dispositivos ilegales**. 1. Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la comisión dolosa y antijurídica de lo siguiente:

a) La producción, venta, el procurarse para el uso, la importación, distribución o cualquier forma de hacer posible:

1. Cualquier dispositivo, incluidos los programas informáticos, diseñados o adaptados principalmente con el propósito de cometer alguno de los delitos descritos en los artículos 2 a 5.

2. Una contraseña electrónica, código de acceso o datos similares a través del cual un sistema informático o parte de él consigue ser accesible, con la finalidad de ser usado con el propósito de cometer los delitos descritos en los artículos 2 a 5.

b) La posesión de cualquiera de los aparatos descritos en los números 1 y 2 de la letra *a)* con la finalidad de ser usado para cometer los delitos establecidos en los artículos 2 a 5. Las partes deberán establecer mediante ley que sea poseído un determinado número de este tipo de dispositivos antes de la atribución de responsabilidad.

30. El artículo 6.2 establece que el apartado primero del mismo número no debe interpretarse "como imposición de responsabilidad criminal donde la producción, venta, procurarse para el uso, importación, distribución o la facilitación o posesión referidas en el párrafo primero de este artículo no lo sea con la finalidad de cometer los hechos descritos en los artículos 2 a 5 de esta convención, **como por ejemplo para el chequeo autorizado o la protección de un sistema informático**". La prevención llega a ser tan evidente que el precepto se cierra facultando a los estados para el establecimiento de reserva en la transposición del precepto; instrumento éste, la reserva, cuyo uso generalizado podría comprometer la virtualidad de la Convención.

31. Puede consultarse el texto íntegro de la exposición de motivos en: <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm[url8]>.

32. <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm[url9]>, parágrafo 35. Téngase en cuenta, no obstante, que el Tribunal Constitucional de Estados Unidos declaró en 1997 contrarias a la Constitución las disposiciones de la *Decency Act*, relativas a la responsabilidad de los intermediarios por los contenidos circulantes en red, y que la apología constituye en aquel país un problema jurídico íntimamente ligado a la libertad de expresión, lo que explicaría de modo más satisfactorio que en la propuesta no haya sido incluida mención alguna sobre contenidos o responsabilidad por los mismos.

a) Intimidad y protección de datos. Acceso ilegal e interceptación de las comunicaciones

El Consejo parte en los artículos 2 y 3 de la necesidad de tipificar el acceso ilegal a sistemas y la interceptación de comunicaciones, y opta preferentemente, en cuanto a la primera modalidad, por una descripción lo más objetivada posible en lo referente a la conducta, es decir, desnuda de ingredientes añadidos al acceso mismo, de carácter objetivo (con vulneración de medidas de seguridad) o de carácter íntegramente subjetivo (finalidad de conocer la intimidad, por ejemplo).[33] Del mismo modo, la reciente Propuesta de decisión marco del Consejo de Europa de 19 de abril de 2002, sobre los ataques de que pueden ser objeto los sistemas de información, recomienda a los estados miembros de la UE la armonización de la legislación penal en esta materia, tipificando, en materia de acceso abusivo, las conductas consistentes en acceder a un sistema sólo cuando se hayan vulnerado medidas de seguridad, y, cuando éstas no existan, si el acceso se ha llevado a cabo con la finalidad de causar *daños a las personas físicas o jurídicas*.[34] El paralelismo entre la armonización propuesta por el Consejo de Europa y por la UE consiste, pues, en que el Consejo de Europa propone tipificar el acceso ilegal en términos objetivos, aunque permite a los estados reservar la sanción penal sólo a los casos en que exista una vulneración de medidas de seguridad, y la UE, por su parte, propone la tipificación sólo cuando se hayan vulnerado medidas de seguridad.

Ciertamente, en materia de acceso ilegal la decisión político-criminal de tutelar o no penalmente el intrusismo informático sin otra finalidad es compleja. La vertiginosa evolución del mundo de Internet ha eclipsado el romanticismo inherente a aquellas conductas consistentes en acceder a sistemas ajenos e informar al administrador de los déficit de seguridad, y sugiere alternativas para preservar la integridad del sistema frente a posibles ataques; además, cualquiera puede ser ahora un intruso con los programas de entorno gráfico de acceso ilegal que pueden obtenerse gratuitamente en Internet,[35] lo que implicaría la incriminación de un numero elevadísimo de conductas o el recurso a la función promocional del Derecho penal para la educación primaria de los usuarios, es decir, para la creación de una conciencia colectiva de ilicitud del acceso. Pero en tal caso debe quedar claro el bien jurídico que quiere promocionarse. Tanto desde el Consejo de Europa como desde la propia UE (a través de la Propuesta de decisión marco), se asume como tal la seguridad, integridad y disponibilidad de los sistemas de información y los datos informáticos. En tal caso, los delitos de interceptación, pero sobre todo de acceso abusivo, constituyen un adelantamiento de la barrera que separa la intervención penal, puesto que la integridad de los sistemas es ya objeto de tutela a través de los delitos de daños informáticos e interferencia de sistemas de los artículos 4 y 5 de la Convención, o 3 de la Propuesta de decisión marco. Así pues, el acceso abusivo, al constituir en un porcentaje mayoritario el paso previo a la realización de un delito de daños informáticos, pasaría de ser una tentativa cuando el daño no se produce finalmente por causas ajenas a la voluntad del autor, a erigirse en una figura autónoma de consumación. Otros bienes jurídicos fundamentales, como la protección de datos o la intimidad, no tendrían cabida aquí o, si se quiere, sólo muy remotamente, ya que cederían ante el contenido patrimonial del ataque y mostrarían nuevamente la influencia de ordenamientos jurídicos ajenos a la tradición continental, en los que la tutela de la intimidad o los datos personales no encuentra criterios sólidos de merecimiento y necesidad de tutela penal.

Por ello, tal vez sea conveniente formular un concepto de domicilio informático, del derecho a mantener la máquina y su contenido al margen de los accesos no deseados, tal como sucede, *ceteris paribus*, con el domicilio "físico"; concepto, pues, en el que se integren los elementos esenciales de bienes jurídicos con relevancia constitucional, directamente ligados al uso de la tecnología (en el caso del Derecho español, huelgan los comentarios en relación con la ubicación sistemática, el artículo 18 CE, de la cláusula de tutela frente a los peligros de la

33. El **artículo 2** de la Convención establece lo siguiente: **acceso ilegal**. Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal el acceso intencional sin autorización a la totalidad o parte de un sistema informático. Los estados podrán requerir que el hecho haya sido cometido infringiendo medidas de seguridad o con la finalidad de obtener datos u otra finalidad deshonesta o, en relación con los sistemas informáticos, que se encuentren conectados a otros sistemas informáticos.

34. Desde luego la redacción no podía ser más desafortunada desde el punto de vista de las necesidades de tutela. Es evidente que la referencia a las personas jurídicas impide relacionar el daño al que se refiere el subtipo con la integridad física, luego el daño pasa a ser eminentemente patrimonial, en cuyo caso el subtipo es un modo de adelantar la intervención penal respecto a las infracciones patrimoniales, lo que eleva la tentativa de daños a consumación.

35. Entre ellos, quizá el más afamado sea el programa Net Bus. Su funcionamiento es sencillo: dividido en dos subprogramas, uno de ellos debe ser introducido en la máquina a la que se accederá (las formas de introducción son tantas como puedan imaginarse: a través de correo electrónico con la técnica del caballo de Troya, es decir, ejecutando un programa que, a su vez y de modo oculto, ejecuta el subprograma, de Net Bus; mediante un disco flexible, es decir, situándose físicamente ante la máquina, etc.); al ejecutarse, dejará abierta una puerta que será detectada por el otro subprograma. Acceder será entonces tan sencillo como hacer clic con el ratón. Las posibilidades de control de la máquina a la que se ha accedido son absolutas.

informática), de modo que con ello se describa un tipo de carácter objetivo, en los términos recomendados por la Convención, con la pretensión de salvaguardar la esfera íntima del sujeto y sin desdeñar una protección escalonada a través de la creación de subtipos agravados. En cualquier caso, debe tenerse en cuenta que la creación de tipos penales con finalidades trascendentes, de resultado cortado, como sucede con el 197.1 segundo inciso en el CP español de 1995, donde se condiciona la punición de la interceptación de las comunicaciones (o en el 197.2 CP, de la interceptación de datos) a la finalidad de conocer la intimidad o los secretos, sólo puede perturbar la aplicación ordinaria del tipo, de modo que la prueba de dicha finalidad sucesiva (que ni siquiera debe realizarse en un resultado, sino simplemente inspirar la conducta principal de acceso o interceptación) será poco menos que imposible,[36] con lo que permanecerá en la impunidad la mayoría de los accesos ilegales. La creación de subtipos agravados, además de reforzar la tutela de los bienes jurídicos en juego, permitiría mantener la punición del tipo básico cuando los elementos del agravado no concurrieren o no pudieran ser objeto de prueba en el plenario.

b) Delitos patrimoniales

1. Daños

La Convención del Consejo de Europa planea la incorporación en la legislación penal de los estados firmantes de dos figuras delictivas próximas al delito de daños, cuales son los delitos de daños informáticos (artículo 4)[37] y de interferencia de sistemas (artículo 5),[38] tipo este último también sugerido en la Propuesta de decisión marco de la UE. Son múltiples los problemas que concurren en la creación de un tipo de daños informáticos. Si se construye un tipo autónomo, deberá decidirse si, tutelándose la propiedad como tutelan tradicionalmente los delitos contra la propiedad, se establece, no obstante, una cuantía económica mínima como perjuicio para expresar penalmente el desvalor de la conducta. La Convención del Consejo de Europa nada dice al respecto, como tampoco lo hace el Código penal de 1995, porque el artículo 260.4 no deja claro si se trata de una figura autónoma o dependiente del delito base de daños sobre cosa material, que sí contiene esa cláusula.[39] En todo caso, si se establece una cantidad, por ejemplo de 300 euros como mínimo, para que intervenga el Derecho penal a través de un delito –podría mantenerse la existencia de una falta–, el problema radicará en el sistema empleado para la valoración del daño: si se toma como referencia únicamente el valor en sí del dato informático (cuya esencia aún está por describir cabalmente) serán pocos los casos en que se llegue al delito, dado su escaso valor. Si se toma el valor de cambio, lo que vale el contenido, en definitiva, a través de una interpretación funcional, se introduce en el núcleo de injusto un valor propio de la responsabilidad civil derivada de delito, con lo que se amplifica el alcance del tipo penal y en según qué casos, simultáneamente, se recorta, pues la destrucción de datos cuando existen copias de seguridad derivará en tentativa a decidir si posible y punible o imposible e impune, porque el valor de cambio permanecería inalterado.[40]

Por otra parte, se pretende la punición de la mera alteración del funcionamiento de sistemas informáticos, con lo que se previenen los ataques de denegación de servicio,[41] sobre la base de las pérdidas económicas que pueden sufrir las empresas de prestación de servicios y los clientes cuando determinados ataques sincronizados, sin borrar datos, sin destruirlos en términos de inutilización definitiva, impiden, no obstante, su funcionamiento ordinario. Ciertamente la pretensión en este caso excede el ámbito de lo razonable en términos de necesidad; sin embargo, no sería descabellado afirmar la posibilidad de sancionar en el Derecho penal español estas conductas a través de una interpretación extensiva del concepto de violencia contenido en el delito de coacciones, en una operación semejante a la que efectúa

36. Sin duda el caso más claro de acceso ilegal a otro sistema informático fue el denominado "caso Hispahack". Sobre ello *vid.* FERNÁNDEZ PALMA, R.; MORALES GARCÍA, O. (2000, enero). "El delito de daños informáticos y el caso Hispahack. Algunas reflexiones en torno a la sentencia del Juzgado de lo Penal nº 2 de Barcelona de 2 de mayo de 1999". *La Llei*. Nº 283, pág. 1 y sigs.
37. El **artículo 4** de la Convención establece, con el *nomen iuris* **interferencia de datos**: 1. Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la producción intencionada de daño, borrado, deterioro, alteración o supresión antijurídica de datos informáticos. 2. Los estados podrán reservarse el derecho a exigir que la conducta descrita en el párrafo dañe seriamente el contenido.
38. El **artículo 5**, en relación con la **interferencia de sistemas** establece que "los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la obstaculización intencionada del funcionamiento de un sistema informático mediante transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos".
39. Sobre esta problemática *vid.*, ampliamente, DE ANDRÉS DOMÍNGUEZ, C. (1999, febrero). "El delito de daños informáticos". *La Ley*. Nº 4.725; FERNÁNDEZ PALMA, R.; MORALES GARCÍA, O. (2000, enero). "El delito de daños informáticos y el caso Hispahack. Algunas reflexiones en torno a la sentencia del Juzgado de lo Penal nº 2 de Barcelona de 2 de mayo de 1999". *La Llei*. Nº 283, pág. 1 y sigs.
40. Al respecto *cfr.* GONZÁLEZ RUS, J. J. (1997). "Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos". En: *Delincuencia informática, estudios jurídicos, ministerio fiscal*, vol. III.
41. También conocidos como ataques DoS: *Denial of Service*.

la jurisprudencia del Tribunal Supremo, esto es, abarcando en el término violencia también la *vis in rebus* sobre las máquinas inutilizadas.

2. Estafa informática y falsedades documentales

La estafa informática es otro lugar donde la Convención no acierta del todo, en una pretensión recurrente de garantizar la integridad de los sistemas. Así, la literalidad de la letra *a)* no describe una estafa en sentido estricto, sino lo que en puridad no es otra cosa que un delito de daños: causar un perjuicio a otro a través del deterioro o cancelación, etc., de datos informáticos.[42] Por otra parte, el segundo párrafo, que contiene una conducta fraudulenta –colmada con nuestro artículo doscientos cuarenta y ocho segundo párrafo del CP–, no ofrece una respuesta clara a la utilización abusiva de tarjetas, o al modo en que penalmente deban armonizarse el conjunto de conductas que convergen en dicha problemática –uso en terminales punto de venta, en cajeros automáticos con número secreto, en dispositivos automáticos sin número, etc.–,[43] y ello ni aun adoptando un concepto amplio de delincuencia informática referido a *cualquier conducta ilícita realizada en los procesos de transferencia de datos,*[44] puesto que el precepto tan sólo obliga a sancionar penalmente los casos en que se ha producido una interferencia relevante en el sistema, de modo que el riesgo penalmente relevante al que hay que imputar el perjuicio patrimonial debe actuar directamente sobre los datos o el sistema informático, con lo que se consigue una actuación diversa del sistema o igual pero con cambios accesorios –de identidad, cantidad, destino, etc.[45]

Por último, en la parte especial, el artículo 7 de la Convención prevé la punición de las falsedades documentales en documento informático.[46] Si bien no se ofrece un concepto general de documento, o en particular de documento informático, ni se condiciona la sanción penal de la falsedad sobre datos fijados en soporte informático a la certificación de las funciones que el documento debe cumplir para poder ser tenido por tal a efectos penales y ser, entonces, posible objeto de una falsedad, sí que se han tratado de soslayar algunos de los problemas que históricamente condicionaban la subsunción de las falsedades sobre documento informático en los tipos "tradicionales de falsedad". En efecto, la referencia a la irrelevancia de la legibilidad directa del documento esquiva los problemas que especialmente la doctrina alemana[47] subrayaba en torno a la imposibilidad de los documentos electrónicos para garantizar la función de perpetuación, entendida en su aspecto de declaración de pensamiento. Nada se dice en relación con las funciones de garantía y probatoria, mas, al igual que sucede con el cartáceo, deberán inferirse con carácter general para el informático, si no quiere llegarse al absurdo de sancionar la simple alteración de programas informáticos.

Éste es el panorama general que presenta la Convención del Consejo de Europa, visto lógicamente con una pretensión puramente introductoria. Hasta el momento en que la Convención deba implementarse, con la ratificación de al menos cinco estados, tres de ellos pertenecientes *de iure* al Consejo de Europa, será necesario continuar la reflexión político-criminal, con la finalidad de que la transposición del texto sea lo más acorde con el sistema de garantías, al menos, de nuestra nación, entendiendo por tal, ahora, el conjunto de la Unión Europea.

42. El **artículo 8 letra *a)*** de la Convención del Consejo de Europa de 23 de noviembre de 2001 establece que "los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la causación intencionada y antijurídica de una lesión de la propiedad mediante: a) *la introducción, alteración, borrado o eliminación de datos informáticos*".
43. **Artículo 8 letra *b)***: "Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la causación intencionada y antijurídica de una lesión de la propiedad mediante: b) *cualquier forma de atentar contra el funcionamiento de un sistema informático, con la intención de obtener sin derecho a ello un beneficio económico para sí mismo o para otro.*"
44. Así, SIEBER, U. (1986). *The handbook of computer crime*, que recoge la definición de la OCDE sobre la materia.
45. Aunque a mi juicio ello no es posible en términos de estricta legalidad, lo cierto es que el hecho, no obstante, es discutible, como lo demuestra la reciente **sentencia del Tribunal Supremo de 20 de noviembre de 2001**, en la que se equipara la utilización ordinaria de una tarjeta de crédito en un terminal punto de venta con la cláusula indeterminada "artificio semejante" del artículo 248.2 CP. Para ello, el Alto Tribunal entiende que la introducción de la tarjeta en la máquina implica una simulación torticera ante el terminal, que sería entonces equiparable a la manipulación informática. La resolución de instancia, **sentencia de la Audiencia Provincial de Barcelona de 19 de noviembre de 1999**, absolvió al acusado al considerar que, no existiendo en puridad una estafa informática, la ausencia de calificación alternativa impedía la condena por robo con fuerza o, en su caso, hurto.
46. El **artículo 7** de la Convención, relativo a las **falsedades informáticas**, dispone lo siguiente: "Los estados parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la realización dolosa y antijurídica de conductas consistentes en la introducción, alteración, borrado o supresión de datos informáticos, de las que deriven datos inauténticos con la finalidad de que sean considerados como auténticos o de introducirlos con un propósito legal como si fueran auténticos, independientemente de que los datos sean directamente legibles e inteligibles." Los estados podrán exigir por ley que el hecho se cometa para intentar defraudar o con algún elemento subjetivo similar, como requisito añadido para la punición del hecho.
47. *Vid.* una completa descripción de la problemática en VILLACAMPA ESTIARTE, C. (1999). *La falsedad documental. Análisis jurídico penal*. Barcelona. Con carácter previo, SIEBER, U. *The handbook*. *Cit.*

Lista de URL:

[url1]:http://www.uoc.edu/web/esp/art/uoc/0109042/jeffery.html
[url2]:http://aci.kpmg.com.hk/docs/evolving issues/ecommerce and cyber crime.pdf
[url3]:http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
[url4]:http://www.gilc.org/privacy/coe-letter-1000-es.html
[url5]:http://www.uoc.edu/in3/dt/20243/opinion_4-2001.pdf
[url6]:http://www.uoc.edu/in3/dt/20243/opinion_4-2001.pdf
[url7]:http://www.uoc.edu/in3/dt/20243/opinion_4-2001.pdf
[url8]:http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm
[url9]:http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm

Enlaces relacionados:

- Convención del Consejo de Europa sobre ciberdelito (en inglés):
  http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- Versión española de la Convención del Consejo de Europa sobre ciberdelito:
  http://www.uoc/edu/in3/dt/20243/delincuencia_informatica.pdf

Fecha de publicación: junio de 2003