Cibercrimen

Computer Crime

ALVARO SÁNCHEZ BRAVO

Doctor en Derecho. Professor de Filosofía do Derecho da Faculdade de Direito da Universidade de Sevilha (Espanha); Professor de Política Criminal do Instituto Andaluz Interuniversitario de Criminología (Sección Sevilla).

RESUMO

O artigo analisa a resposta internacional à delinqüência informática, a partir da Convenção do Conselho da Europa sobre a cibercriminalidade.
Palavras-chave: *Criminalidade informática, Direito internacional, Direito europeu.*

ABSTRACT

Based on the European Council Convention on computer crime, the article analyses the international response to computer delinquency.
Key words*: Computer crime, International law, European law.*

1. LA NECESIDAD DE UNA REFLEXIÓN SOBRE LA DELINCUENCIA INFORMÁTICA

Los modernos sistemas de información y comunicación presentan, frente a innegables avances, riesgos de que no deben soslayarse.

Las tecnologías de la sociedad de la información pueden utilizarse, y de hecho, se utilizan, para perpetrar y facilitar diversas actividades delictivas.

A medida que nuestras sociedades se vuelven cada vez más interconectadas informáticamente, aumenta exponencialmente la posibilidad de

que la nueva infraestructura de la información y el conocimiento se vuelva un blanco apetecible de grupos o individuos que a través del terror quieran lograr sus fines, cualquiera que éstas sean[1]. Como ha señalado la propia Comisión Europea, "en manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades delictivas que pongan en peligro o atenten contra la vida, la propiedad o la dignidad de los individuos o del interés público"[2].

Respecto al alcance de estas actividades ilícitas, no existen estadísticas fiables sobre la magnitud del fenómeno de la delincuencia informática. Así se estima que el número de agresiones detectadas y comunicadas hasta el presente, subestima, con mucho el problema. Todavía la limitada experiencia y la ausencia de una conciencia crítica de muchos administradores y usuarios del sistema hace que muchos ataques aún no se detecten.

Además, todavía numerosas empresas no denuncian muchos de los ataques para no crear alarma entre sus potenciales clientes, y por la propia perdida de credibilidad ante una publicidad negativa.

No obstante, se espera que el número de actividades ilegales crezca a medida que se dispara el uso de ordenadores y redes[3].

Ahora bien, estas actividades delictivas pueden adoptar una gran variedad de formas y pueden cruzar muchas fronteras. Al menos inicialmente, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Es por ello, que se evidencia como imprescindible una acción eficaz, tanto a nivel de las legislaciones internas, como de la cooperación internacional, para luchar contra la delincuencia informática.

---

[1] de 1987. Cfr. FALCIONELLI, E., "Cyber-terrorismo, el nuevo rostro del miedo", en delitosinformaticos.com/ cyber/ cyberterrorismo/shtml.

[2] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, *Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos*, COM(2000) 890 final, Bruselas, 26.01.01, p. 6.

[3] Así se manifestó el Jefe de la Unidad de Delitos Tecnológicos de la Policía Nacional, en su intervención en el I Congreso Internacional sobre Ética en los Medios de Comunicación e Internet, donde manifestó como los delitos tecnológicos que se cometen en la red seguirán creciendo ante la falta de legislación internacional, "al no haber una ley ágil e inmediata para que una vez conocido el delito además de prevenirlo podamos erradicarlo". Vid. Delitosinformaticos.com/noticias/17.10.01.

Para ello, amén de políticas legislativas, se requiere la definición de un nuevo marco de seguridad, que garantice infraestructuras de información seguras y fiables, y basadas en las necesidades reales de los usuarios, y la constante renovación tecnológica[4]. Pero para eso será necesario determinar, con carácter previo, a que nos estamos refiriendo cuando hablamos de delincuencia informática.

2. DELIMITACIÓN CONCEPTUAL DE LA DELINCUENCIA INFORMÁTICA

Diferentes son las expresiones que se utilizan para designar este fenómeno. Así suelen utilizarse indistintamente los términos "cibercrimen", "delincuencia informática", "delincuencia relacionada con la informática", y "delincuencia de alta tecnología".

Pero, realmente, ¿de que estamos hablando?. Como ha señalado Pérez Luño, "la ambigüedad e indeterminación de las situaciones de criminalidad informática se refleja en los planteamientos doctrinales tendentes a su teorización. Determinados enfoques subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo, con los ordenadores. Desde otras ópticas teóricas incluso se llega a negar cualquier tipo de sustantividad al delito informático, al considerar que se trata de tipos delictivos tradicionales sin otra nota distintiva que la de estar relacionados con los ordenadores. Como contrapunto a quienes niegan la criminalidad informática, habrá quien postule que todos los delitos pueden ser informáticos, en cuanto que las conexiones entre los actos criminales y las computadoras son prácticamente ilimitadas"[5].

Camacho Losa, lo conceptúa como "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para sus autores, o que, por el contrario, produce un beneficio

[4] Sobre el déficit en materia de seguridad en el ciberespacio y las soluciones apuntadas desde la Unión Europea, vid. SÁNCHEZ BRAVO, A., "Una política comunitaria de seguridad en Internet", en *Diario La Ley*, n° 5414, 8 de noviembre de 2001, pp. 1-8.

[5] Cfr. PEREZ LUÑO, A. E., *Manual de Informática y Derecho*, Ariel, Barcelona, 1996, p. 70 y la bibliografía allí citada.

ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la victima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas"[6].

Por su parte, en una clásica y amplia definición el Departamento de Justicia norteamericano: "delito informático (*computer crime*) es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación o persecución"[7]. Otros autores, restringen, a sensu contrario, el concepto de criminalidad informática al campo de lo patrimonial.

Ahora bien, más relevante que establecer una definición cerrada de que sea el cibercrimen o delito informático, será poner de manifiesto sus concretas peculiaridades.

Siguiendo nuevamente a Pérez Luño, "la regulación de la criminalidad por o contra el ordenador presenta determinadas peculiaridades debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan"[8].

Entre las mismas, pueden citarse:

1. la criminalidad informática puede suponer una nueva versión de delitos tradicionales, o, en la mayor parte de los casos, la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías, lo que obliga a revisar los elementos constitutivos de gran parte de los tipos penales tradicionales.

2. Es un sector sometido a constantes cambios y variaciones lo que determina una inestabilidad en sus categorizaciones.

3. La criminalidad informática viene caracterizada por los problemas que plantea su descubrimiento, su prueba y su persecución.

[6] Cfr. CAMACHO LOSA, L., *El Delito Informático*, Madrid, 1987., p. 25.

[7] Cfr. U.S. Departament of Justice, *Criminal Justice Resource Manual on Computer Crime*, National Criminal Justice Information and Statistics Service, Washington D.C., 1979, p. 2. Tomo la referencia de ROMEO CASABONA, C. M., *Poder Informático y seguridad jurídica*, Fundesco, Madrid, 1988, p.. 42.

[8] Cfr. PEREZ LUÑO, A. E., *Manual de Informática y Derecho*, cit. , pp. 74-77.

4. La ya apuntada precariedad y anquilosamiento de los sistemas penales lleva a numerosos afectados a no denunciar los hechos, para evitar la alarma social o el desprestigio que para sus intereses pudieran producirse[9].

5. La insuficiencia de los instrumentos y mecanismos penales para prevenir y reprimir estas conductas.

Todas estas cuestiones, nos llevan a la necesidad de establecimiento de unos instrumentos jurídicos sustantivos y procesales eficaces aproximados a escala mundial para protegernos frente a la delincuencia informática. Pero no debe olvidarse que las comunicaciones personales, la protección de los datos personales y la intimidad, y el acceso y la difusión de la información, son derechos fundamentales en los modernos sistemas democráticos.

Así pues, como ha señalado la Comisión Europea, será necesario contar con la disponibilidad y el uso de medidas eficaces de prevención, para reducir la necesidad de aplicar medidas de ejecución. Cualquier medida legislativa que pueda resultar necesaria para abordar la delincuencia informática ha de alcanzar un equilibrio entre estos importantes intereses[10].

3. LA NECESARIA RESPUESTA INTERNACIONAL FRENTE A LA DELINCUENCIA INFORMÁTICA

La delincuencia informática se comete en ese "lugar" indeterminado que se conoce como ciberespacio, pero cuyas magnitudes se desconocen.

[9] En Estados Unidos, las autoridades policiales han constatado el aumento de las denuncias en los casos de atentados informáticos. Los elevados costes que suponían para las empresas la contratación de abogados y consultores de seguridad, así como el cambio de actitud hacia los efectos de publicidad negativa que podría conllevar una denuncia ante los fiscales federales, ha supuesto un notable incremento respecto a años anteriores .

A sensu contrario *en Gran Bretaña, un reciente estudio de la CBI (Confederación de la Industria Británica) donde se evidencia que un tercio de las firmas británicas fueron victimas de "cibercrimen", constata igualmente que aunque el 69% de las empresas que realizaron el sondeo dijeron que las pérdidas financieras eran insignificantes, dijeron temer que su reputación pudiera verse empañada.*

[10] Cfr. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, *Creación de una sociedad de la información más segura...*, cit., p. 15.

Prima facie, puede perpetrarse desde cualquier lugar, y contra cualquiera, no deteniéndose ante ninguna frontera.

A nivel nacional, no existe en muchos casos planteamientos globales, y con vocación internacional, frente a los nuevos desafíos de seguridad y delincuencia informática.

A pesar de los esfuerzos realizados dentro de la cooperación internacional, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias. Corresponde a los Estados nacionales la definición de lo que sea o deba considerarse como ilícito. Surgen así dificultades prácticas para la aplicación de las legislaciones represivas en los supuestos en que determinados actos son punibles con arreglo al Derecho penal de un Estado, pero no de otro[11].

Además la naturaleza internacional de los servicios audiovisuales y de información, puede posibilitar que los autores o suministradores de contenidos abusen de esta situación utilizando determinados países – los denominados paraísos informáticos – donde ciertos comportamientos se consideren *legales*, o cuando menos alegales, como plataforma para reproducirlos y perpetrarlos en países donde sean punibles.

Incluso, aunque una legislación prohíba contenidos o comportamientos ilícitos y establezca la apertura de una causa criminal, puede ocurrir que el autor, el suministrador de contenidos o el de servicios de ordenador central queden todos fuera del ámbito de aplicación de la ley penal y de la competencia de los agentes de orden público, sometidos a a los límites de la aplicación territorial de la aplicación de la ley penal[12].

Se manifiesta, por tanto, la necesidad de reforzar la cooperación internacional entre los Estados con el fin de luchar eficazmente contra la delincuencia informática, estableciendo determinadas pautas comunes en las legislaciones para evitar lagunas o discrepancias que propicien el desarrollo de actividades delictivas.

Todo ello en un contexto de evidente conflicto de intereses, que se ha visto agravado a raíz del ya tristemente famoso 11-S en New York y Wa-

[11] Así, tomando como ejemplo la Unión Europea, en materia de pornografía infantil ésta está cubierta en unos países por legislaciones específicas y por normas generales sobre obscenidad en otros. Vid. Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de la información, COM(96) 483, pp. 41-43.

[12] Cfr. SÁNCHEZ BRAVO, A., *Internet y la Sociedad Europea de la Información: Implicaciones para los ciudadanos*, Publicaciones de la Universidad de Sevilla, 2001, p.86.

shington. Por un lado, la industria de la información y comunicación que exige la libre circulación de datos y contenidos, pues cualquier control excesivo puede incidir sobre el desarrollo del mercado. Por otro, el de los Estados, que exigen una circulación controlada y restringida en aras de una peculiar interpretación de la seguridad y el interés nacional[13].

Y en medio, los usuarios que oscilan entre el temor a ciberataques a su intimidad y al resto de sus intereses, y la preocupación por verse sometidos a un control estatal que les inhabilite para el correcto ejercicio de sus derechos.

A escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, desarrollándose numerosas iniciativas en este campo.

Los Ministros de Justicia e Interior del G8 adoptaron en diciembre de 1997 un conjunto de principios y un plan de acción de diez puntos, aprobado en la Cumbre de Birmingham en junio de 1998, y que actualmente se está aplicando[14].

La ONU y la OCDE también se han implicado en esta reflexión, y asimismo se está discutiendo en foros internacionales como el Diálogo Empresarial Global y el Diálogo Empresarial Trasatlántico[15].

---

[13] De todos es sabido como a raíz de dichos atentados terroristas se ha producido una oscilación casi universal hacia posturas que postulan una intervención de Internet, y un control sobre los usuarios y sobre la información que envían o consumen.

Así, con motivo de la aprobación en el Senado de la nueva ley antiterrorista que limitará los poderes en la Cámara, una de las enmiendas de urgencia impulsadas tras los atentados permitiría a la fiscalía instalar en los proveedores de acceso a Internet sistemas de vigilancia de los servicios de mensajería electrónica. De hecho, unos horas después de los atentados agentes de la Oficina Federal de Investigación (FBI) se presentaros en las oficinas de los proveedores AOL, Earthlink y Hoptmail para instalar en sus servidores el programa "Carnivore", *que permite interceptar las comunicaciones de sus clientes.*

Ahora bien, esta cuestión no constituye, por otra parte, ninguna novedad, como lo demuestra la existencia hace tiempo de la red de espionaje Echelon, *cuya existencia ha sido confirmada plenamente por el Parlamento Europeo.*

[14] http://ue.eu.int/ejn/index.htm. Cfr. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, *Creación de una sociedad de la información más segura...*, cit., p. 7.

[15] Naciones Unidas elaboró un "Manual sobre la prevención y el control de la delincuencia informática", que se ha actualizado recientemente. En 1983 la OCDE inició un estudio sobre la posibilidad de aplicar a escala internacional y armonizar los derechos penales para abordar el problema del abuso informático o de la delincuencia informática. En 1986, publico el informe "Delincuencia informática: Análisis de las medidas jurídicas", donde se examinaban las leyes y propuestas existentes para la reforma en varios Estados miembros y se recomendaba una lista mínima de abusos que los países deberían prohibir y penalizar con leyes penales. Finalmente, en 1992, la OCDE elaboró un conjunto de directrices para la seguridad de los sistemas de información, que deberían en principio proporcionar una base sobre la cual los Estados y el sector privado pudieran construir un marco para la seguridad de los sistemas de información. Cfr. ID., p. 8, y especialmente p. de p. 9.

La Unión Europea, por su parte, ha adoptado medidas legislativas en los campos del derecho de autor[16], la protección de datos[17], el comercio electrónico[18] y la firma digital[19], entre otros.

Igualmente ha adoptado varias medidas no legislativas, entre las que merecen destacarse, el plan de lucha contra los contenidos ilícitos y nocivos en Internet[20], la pornografía infantil[21] y la interceptación legal de las comunicaciones.

La preocupación comunitaria por el problema de la delincuencia informática ha cobrado carta de naturaleza específica, recientemente con la elaboración por parte de la Comisión de una Comunicación donde se aborda la necesidad y las posibles formas de una iniciativa política amplia en el contexto de los objetivos más amplios de la sociedad de la información y de la libertad, seguridad y justicia, con el fin de mejorar la seguridad de las infraestructuras de información y luchar contra la delincuencia informática[22].

El Consejo de Europa, no podía ser ajeno a esta global preocupación, cuyos trabajos han desembocado en la reciente Convención sobre la cibercriminalidad, cuyo examen será objeto de nuestras próximas consideraciones.

[16] Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la harmonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, DOCE n° L 167/11, 22.6.2001.

[17] Vid. SÁNCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Publicaciones de la Universidad de Sevilla, 1998.

[18] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de la sociedad de la información, en particular el comercio electrónico (Directiva sobre el comercio electrónico), DOCE n° L 178/1, 17,7.2000.

[19] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica.

[20] Vid., a este respecto SÁNCHEZ BRAVO, A.,. "La regulación de los Contenidos Ilícitos y Nocivos en Internet: una propuesta desde la Unión Europea", en *Informática y Derecho*, Vol. 27-28-29, UNED. Centro Regional de Extremadura, Mérida, 1998, pp. 361-387, y la bibliografía allí citada.

[21] Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información, COM (96) 483.

[22] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, *Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos*, COM(2000) 890 final, Bruselas, 26.01.01.

4. LA CONVENCIÓN DEL CONSEJO DE EUROPA SOBRE LA CIBERCRIMINALIDAD [23]

Durante cuatro años, el Consejo de Europa ha estado elaborando una Convención capaz de responder a los desafíos que plantea la criminalidad informática. Este texto constituye el primero a nivel mundial que pretende, ante todo, garantizar la seguridad de la red y de sus usuarios.

El texto y las propuestas originales no fueron objeto de pacífica aceptación, lo cual obligó en numerosas ocasiones a una rebaja de los niveles represivos previstos inicialmente por el Proyecto. Así la mayoría de los países se manifestó en contra de la propuesta inicial de crear una "ciberpolicía" internacional y de otorgar a los jueces de cada país una competencia universal para juzgar este tipo de delitos.

Por otra parte, para evitar la desaparición de pruebas, el Proyecto preveía la obligación de que los Proveedores de Servicios de Internet (ISP) conservaran sistemáticamente todos los datos de conexión de sus clientes durante cierto tiempo. Sin embargo, esta iniciativa, fue también rechazada, y no se incluyó en el texto final[24]; si bien se han adoptado otras no menos lesivas, que veremos posteriormente.

El texto ha sido objeto de una abierta impugnación por parte de numerosas asociaciones de internautas y por los propios proveedores de Internet. Éstos, por el temor a convertirse en vigilantes obligados de los contenidos que se publican en las webs que alojan. Aquellos por el temor a que el Convenio de vía libre a la invasión de la privacidad de los usuarios de Internet y su consiguiente control por parte de los gobiernos[25].

El Convenio ha sido firmado por 31 Estados[26], y su aprobación se ha

[23] http://conventions.coe.int/Treaty/FR/projets/FinalCybercrime.htm

[24] http://www.delitosinformaticos.com.noticias.23-11-01.

[25] Vid a este respecto las actuaciones del Center of Democracy and Technology (www.cdt.org) y la Global Internet Liberty Campaign (www.gilc.org/privacy/coe-letter-1200-es.html).

[26] La Convención fue abierta a la firma el día 23 de noviembre de 2001 en Budapest. Firmaron 26 Estados Miembros del Consejo de Europa: Albania, Alemania, Armenia, Austria, Bélgica, Bulgaria, Croacia, Chipre, España, Estonia, Finlandia, Francia, Grecia, Holanda, Hungría, Italia, Moldavia, Noruega, Polonia, Portugal, Reino Unido, Rumania, Suecia, Suiza, la "ex república yugoslava de Macedonia", y Ucrania. Canadá, Estados Unidos, Japón y Sudáfrica, que participaron en su elaboración, han firmado igualmente la Convención. Malta ha firmado el convenio en Estrasburgo el 17 de enero de 2002.

visto condicionada por dos características de Internet: la oposición entre la dimensión universal del "cibercrimen" y la actividad policial, subordinada a las fronteras nacionales, y el riesgo de desaparición de infracciones en la Red.

Como indica en su Preámbulo, su objetivo es "impulsar, prioritariamente, una política penal común, destinada a proteger la sociedad de la criminalidad en el ciberespacio, especialmente mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional"[27].

La propia Convención autojustifica su elaboración en "ser necesaria para prevenir los actos que atenten contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de estos comportamientos, tal como se describen en la presente Convención, y la adopción de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la investigación y persecución, tanto en el plano nacional, como en el internacional, previendo disposiciones materiales con vistas a una cooperación internacional rápida y fiable".

Abordemos, llegados a este punto, y sin ánimo de ser exhaustivos, las principales aportaciones de este Convenio.

a) Modalidades de criminalidad informática.

Las infracciones reseñadas en el articulado del Convenio, son todas sometidas a un previo doble requisito para que la responsabilidad criminal sea determinada: los comportamientos deben ser realizados de manera "intencional" y "sin derecho". Las infracciones se agrupan en cuatro categorías:

a1. Infracciones contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos.

[27] Para el Portavoz del Ministerio de Asuntos Exteriores de Francia, el objetivo es triple: proveer una definición común de la cibercriminalidad,; fortalecer el arsenal jurídico de los Estados en materia de procedimientos; y adaptar las reglas clásicas de las Convenciones del Consejo de Europa en materia de extradición y ayuda mutua represiva de 1959 y 1957, que constituyen importantes elementos del patrimonio jurídico penal del continente europeo.

- Acceso Ilegal: acceso a todo o parte de un sistema informático (art. 2).

- Interceptación Ilegal: interceptación efectuada por medios técnicos, de datos informáticos, con ocasión de transmisiones no públicas, con destino, provenientes de, o, en el interior de un sistema informático, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte tales datos informatizados (art.3).

- Atentado a la integridad de los datos: la acción de dañar, borrar, deteriorar, alterar o suprimir datos informatizados (art. 4).

- Atentado a la integridad del sistema: la interferencia grave, del funcionamiento de un sistema informático, por la introducción, daño, borrado, deterioro, alteración y supresión de datos informatizados (art. 5).

- Abuso de dispositivos: 1. la producción, la venta, la obtención por utilización, la importación, la difusión o cualquier otra forma de modo de utilización de un dispositivo, que comprenda un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los arts. 2 a 5. Se equiparan a estas acciones las actividades descritas anteriormente cuando tengan por objeto una clave, códigos de acceso o datos informáticos que permitan el acceso a todo o parte de un sistema informático. 2. La posesión de uno de los elementos descritos con anterioridad con el fin de cometer alguna de infracciones establecidas en los arts. 2 a 5. (art. 6).

a2. Infracciones informáticas.

- Falsificación informática: introducción, alteración, borrado o supresión de datos informatizados, generando datos no auténticos, con la intención de que estos sean tenidos en cuenta o utilizados con fines legales como si fueran auténticos, independientemente que ellos sean o no directamente legibles e inteligibles (art. 7).

- Fraude informático: el hecho de causar a otro un perjuicio patrimonial mediante la introducción, alteración, borrado o supresión de datos informatizados; o mediante cualquier otra forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictuosa, de obtener sin derecho un beneficio económico para sí o para otro (art. 8).

a3. Infracciones referidas al contenido: pornografía infantil. *(art. 9).*

- Producción de pornografía infantil con vistas a su difusión a través de un sistema informático.

- El ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático.

- La difusión o la transmisión de pornografía infantil a través de un sistema informático.

- El hecho de procurarse o procurar a otro pornografía infantil a través de un sistema informático.

- La posesión de pornografía infantil en un sistema informático o sistema de almacenamiento de datos informatizados.

Pero en esta materia el Convenio va más allá, no limitándose a una mera enumeración de las conductas punibles, sino que establece dos delimitaciones cruciales. La primera, determinar que se entiende por pornografía infantil cuando de delitos informáticos estamos hablando. La segunda, también capital, establece el límite de edad para considerar a una persona como menor.

Respecto a la primera cuestión se entiende por pornografía infantil todo material pornográfico que represente de manera visual: a) a un menor realizando un comportamiento sexual explícito; b) a una persona que aparezca como un menor realizando un comportamiento sexual explícito; c) imágenes realistas que representen a un menor realizando un comportamiento sexual explícito.

Como se observa ha optado el Convenio por una amplia definición de supuestos, lo cual casa con las modernas orientaciones de política criminal en la materia, pero que no obvian algunos problemas de calificación jurídica dada su indeterminación. Tal es el caso del supuesto c) donde

puede producirse una colisión[28], entre el derecho a la libertad de expresión (concretado en este caso en la libre creación artística) y la legítima represión de comportamientos que, aún no contando con un referente real, si muestran actitudes que repugnan, y que, bajo ningún pretexto, deben ampararse. No obstante, serán las legislaciones nacionales[29] las que tengan que asumir estos supuestos en aplicación del Convenio, y conformar de acuerdo a sus principios jurídicos y políticos la prelación entre los intereses en conflicto.

Respecto a la segunda cuestión, se determina la minoría de edad hasta los 18 años. No obstante, se establece la posibilidad (¡sorprendente!) de rebajarla hasta los 16 años, lo cual nos parece una total incoherencia dado que si no se les estima el pleno ejercicio de sus derechos civiles hasta los 18 años, sin embargo si se les considera mayores a efectos de represión de conductas, beneficiando injustificadamente al autor de las misma, que atentan contra el libre desarrollo de su personalidad, su libertad y su dignidad.

A4. Infracciones referidas a atentados a la propiedad intelectual y derechos conexos.

- Atentados a la propiedad intelectual y derechos conexos, cuando tales hechos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático (art. 10).

[28] Los Estados nacionales otorgan, con arreglo a sus peculiaridades culturales y jurídicas, una importancia variable al principio de libertad de expresión. Así la jurisprudencia se ha decantado erráticamente por la protección de unos u otros intereses al albur de determinados intereses y presiones. Así en Estados Unidos, el 11 de junio de 1996 el Tribunal Federal de Apelación de Filadelfia declaró inconstitucional la *Communications Decency Acts* al violar, entre otras la Primera Enmienda de la Constitución americana que garantiza la libertad de expresión, por cuanto al no existir ningún método razonable que permitiese a los proveedores de contenidos asegurarse de que ningún menor accediera a contenidos indecentes, la ley obligaba a censurarlos todos, cuando los adultos, sin embargo, tienen un derecho constitucional de acceso a los mismos. Cfr. PIETTE-COUDOL, T. y BERTRAND, A., *Internet et la Loi*, Dalloz, Paris, 1997, pp. 114-132. No obstante, sucesos posteriores, y, más recientemente, la campaña mundial contra la erradicación de la pornografía infantil han hecho decantarse las orientaciones hacia medidas duramente restrictivas, limitadoras de la libertad de expresión. Sobre la reciente USA Patriot Act , vid. http://www.eff.org/Privacy/Surveillance/Terrorism

[29] Vid. el documentado y reciente trabajo de PRADOS PEREZ, E., "El turismo sexual infantil y la protección jurídico-penal del menor en la Unión Europea", en *Revista de Estudios Europeos*, num. 28, mayo-agosto 2001, pp.67-85, y cuyo texto debo a la deferencia de su autora.

b) Nuevas reglas de cooperación internacional.

Junto a las formas tradicionales de cooperación penal internacional previstas especialmente por los Convenios Europeos de Extradición[30] y Asistencia mutua en materia penal[31], la Convención exigirá formas de asistencia mutua que adaptadas a los poderes definidos previamente por la Convención, y por tanto, que los órganos jurisdiccionales y servicios policiales de un Estado puedan actuar por cuenta de otro país en la búsqueda de pruebas electrónicas, sin que en ningún caso puedan producirse investigaciones ni persecuciones transfronterizas.

Así lo establece el art. 25 (Principios generales relativos a la asistencia mutua) al señalar que "las partes acuerdan la asistencia mutua más amplia posible con fines de investigaciones o procedimientos relativos a infracciones penales ligadas a sistemas y datos informatizados o con el fin de recopilar las pruebas en formato electrónico de una infracción penal". No obstante, la dependencia de las legislaciones nacionales de cada uno de los Estados es evidente, por cuanto "...la asistencia está sometida a las condiciones fijadas por el derecho interno de la Parte requerida...".

A tal efecto, cada Estado determinará las medidas legislativas o de cualquier otro genero que sea necesarias para el cumplimiento de este acuerdo, permitiéndose, incluso, que en caso de urgencia, pueda realizarse una solicitud de asistencia por medios rápidos de comunicación, tales como la telecopia y el correo electrónico, en tanto éstos medios ofrezcan garantías suficientes de seguridad y autentificación.

Como elemento reforzador de la cooperación, e incluso como gesto de agilidad en la misma, se incluye la denominada "información espontánea", que conforme al art. 26, tendrá lugar cuando un Estado, y en ausencia de demanda previa, comunique a otro Estado informaciones obtenidas en el marco de sus propias investigaciones, cuando estime que puede ayudar al Estado destinatario a desarrollar o concluir investigaciones o procedimientos respecto de infracciones penales establecidas conforme al propio convenio, o cuando estas informaciones puedan conducir a una solicitud de asistencia[32].

[30] Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en Paris (STE n° 24).

[31] Convenio Europeo de Asistencia Mutua en materia penal abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE n° 30).

[32] Bélgica, a este respecto, solicitó por boca de su Ministro de Justicia, Marc Verwilghen, el "acceso transfronterizo a los datos informáticos" en caso de una infracción cometida en Internet. Cfr. http://www.delitosinformáticos.com/ noticias/23-11-01.

A fin de asegurar una asistencia inmediata en las investigaciones que tengan como objeto las infracciones penales referentes a sistemas y datos informatizados, o para recoger las pruebas en formato electrónico de una infracción penal, se constituye una Red 24/7 (art. 35)[33]. Cada Estado designará un punto de contacto disponible 24 horas sobre 24, siete días sobre siete.

Respecto a la jurisdicción aplicable, cada Estado adopta las medidas necesarias para establecer su competencia respecto de toda infracción penal contenida en el Convenio cuando se cometa en su territorio, a bordo de un barco o un avión matriculado en él, o por uno de sus nacionales, si la infracción es penalmente punible allí donde se ha cometido, o si no corresponde a la competencia territorial de ningún otro Estado (art. 22).

c) Nuevos procedimientos.

Una de las novedades relevantes establecidas en el Convenio consiste en el establecimiento de unas reglas que facilitarán el desarrollo de investigaciones en el mundo virtual y que representan nuevas formas de cooperación judicial.

El ámbito material viene determinado, según explicita el art. 14, por las infracciones penales incluidas en los arts. 2 a 11, cualesquiera otras infracciones penales cometidas por medio de un sistema informático, y por la recogida de pruebas electrónicas de cualquier infracción penal. Como se observará la amplitud e indeterminación de los supuestos camina hacia un sistema de control global, que no tiene en la relevancia de los datos, sino en su soporte técnico el único referente de actuación. Esta previsión ha sido objeto de una abierta impugnación, llegando incluso a afirmarse como "este artículo aparece como un mandato permanente para que cualquier fuerza policial, penetre, barra, copie, y supervise el contenido de los datos conservados en una computadora. De una forma concreta, este artículo autoriza el "allanamiento" constante y sin garantía ni control judicial de los datos personales"[34].

[33] Esta asistencia englobará el facilitar, o, si el derecho y la práctica internas lo permiten, la aplicación directa de las siguientes medidas: aportación de consejos técnicos, conservación de datos informatizados en los supuestos así previstos en el Convenio, y recogida de pruebas, suministro de información de carácter jurídico y localización de sospechosos. Para facilitar el funcionamiento de esta Red cada Parte procurará contar con personal formado y equipado.

[34] Cfr. http://www.pagina12.com.ar/2001/01-09/01-09-02/

La Convención pretende asumir el desafío que supone el cibercrimen velando por que la instauración, la puesta en marcha y la aplicación de los poderes y procedimientos que la misma establece se sometan a las condiciones legales de los Estados firmantes garantizando el respeto de los derechos humanos y con observancia del principio de proporcionalidad (art. 15).

En determinados casos, *incluso, se exigirá una supervisión judicial o de cualquier otra autoridad independiente.*

No obstante, tras estas "prometedoras" frases se esconden unas tentativas limitadoras de los derechos de los ciudadanos; sobre todo del derecho a la libertad informática[35].

c1. Conservación rápida de datos informáticos almacenados.

Conforme al art. 16, cada Estado adopta las medidas necesarias para permitir a sus autoridades competentes ordenar la conservación rápida de datos electrónicos específicos, comprendiendo los datos relativos al tráfico, almacenados por medio de un sistema informático.

Los destinatarios de tal orden, persona que tenga los datos en su poder o bajo su control, estará obligada conservar y proteger la integridad de los mismos, durante un periodo, que no podrá exceder de 90 días, con el fin de permitir a las autoridades competentes obtener su divulgación. Está persona está sometida, igualmente, al deber de guardar secreto.

[35] Sobre la delimitación del derecho a la libertad informática, vid., y de entre su numerosa producción científica, PEREZ LUÑO, A. E., *Nuevas Tecnologías, Sociedad y Derecho. El impacto socio-jurìdico de las N.T. de la información*, Fundesco, Madrid, 1987; "La libertad informática. Nueva frontera de los derechos fundamentales", en la obra colectiva *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 185-213; "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", en *Anuario de Derecho Público y Estudios Públicos*, num. 2, 1989/90, pp. 171-195; "*Del Habeas Corpus al Habeas Data*", en *Informática y Derecho*, num. 1, 1992, pp. 153-161; *Manual de Informática y Derecho*, Ariel, Barcelona, 1996; "Aspectos jurídicos y problemas en Internet", en la obra colectiva, coord. Por J. De Lorenzo, *Medios de Comunicación Social y Sociedad: De información a Control y Transformación*, Consejo Social de la Universidad de Valladolid, 2000, pp. 107-134; y *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, 7ª edic., Madrid, 2001; y LUCAS MURILLO DE LA CUEVA, P., "La protección de los datos personales ante el uso de la informática", en *Anuario de Derecho Público y Estudios Políticos*, núm. 2, 1989/90, pp. 153-170; *El derecho a la autodeterminación informativa. La protección de los datos personales ante el uso de la informática*, Tecnos, Madrid, 1990; *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993; y "La construcción del derecho a la autodeterminación informativa", en *Revista de Estudios Políticos*, num. 104, abril-junio 1999.

Vid. asimismo, SANCHEZ BRAVO, A., La protección del derecho a la libertad informática en la Unión Europea*, Publicaciones de la Universidad de Sevilla, 1998.*

Con el fin de asegurar específicamente los datos relativos al tráfico, el Convenio establece en su art. 17 la obligación de cada Estado de velar por la conservación rápida de los referidos datos cuando uno o varios suministradores de servicios[36] hayan participado en la transmisión de esa comunicación.

Igualmente se asume el compromiso de asegurar la comunicación rápida a la autoridad competente de una cantidad de datos relativos al tráfico suficientes para permitir la identificación de los suministradores de servicios y de la vía por la cual la comunicación ha tenido lugar.

Pero, ¿qué se entiende por datos relativos al tráfico?. La respuesta nos la facilita el propio Convenio cuando en su art. 1.d los define como "todos los datos generados en una comunicación que pase por un sistema informático, producidos por éste en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, la extensión y la duración de la comunicación o el tipo de servicio subyacente".

c2. Obligación de informar.

Cada Estado adopta las medidas necesarias para habilitar a sus autoridades competentes a ordenar: a) a una persona que se encuentre en su territorio a comunicar los datos informáticos especificados, que estén en su poder o bajo su control, y almacenados en un sistema informático o en un soporte de almacenamiento informático; b) a un suministrador de servicios que ofrezca sus prestaciones en el territorio de dicho Estado, a comunicar los datos que tenga en su poder o bajo su control relativos a los abonados y referentes a tales servicios.

Ahora, bien, al igual que inquiríamos con anterioridad, ¿qué datos deben entenderse subsumidos bajo la genérica apelación a datos relativos a los abonados? El propio art. 18, regulador de estas cuestiones, y más en concreto su apartado 3, califica como tales, "toda información, contenida bajo el formato de datos informatizados o bajo cualquier otra forma, teni-

[36] Conceptuados por el propio Convenio, a tenor de su art. 1.c, como "toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático", así como "toda otra entidad que trate o almacene datos informatizados para el servicio de comunicación o sus usuarios".

da por un suministrador de servicios y que se refiere a los abonados a esos servicios, que no sean datos relativos al tráfico o al contenido, y que permita establecer: el tipo de servicio de comunicación utilizado, los dispositivos técnicos utilizados a este respecto y el periodo de servicio; la identidad, la dirección postal o geográfica y el número de teléfono del abonado y, cualquier otro número de acceso, los datos relativos a la facturación y al pago, disponibles sobre la base de un contrato o de un acuerdo de servicio; y, cualquier otra información relativa al lugar donde se encuentran los equipos de comunicación, disponible sobre la base de un contrato o acuerdo de servicio.

c3. Registro y recogida de datos informáticos almacenados.

Cada Estado adopta, tal y como señala el art. 19, las medidas necesarias para habilitar a sus autoridades competentes a registrar o a acceder de una manera similar: a) a un sistema informático o a una parte del mismo, así como a los datos informáticos allí almacenados; b) a un soporte de almacenamiento informático que permita almacenar datos informáticos en su territorio.

Esta capacidad de registro (en el sentido de investigación policial) se extiende no sólo a los sistemas informáticos determinados, sino que se amplía a otros conexos, cuando haya motivos para pensar que los datos se encuentran en éstos últimos.

Igualmente se habilita para recoger los datos informáticos respecto de los cuales se ha verificado el acceso, en la forma anteriormente reseñada. Estas medidas incluyen las siguientes prerrogativas: intervenir un sistema informático o una de sus partes, o un soporte de almacenamiento informático; realizar y conservar una copia de datos informáticos; preservar la integridad de los datos informáticos pertinentes; y hacer inaccesibles o quitar datos informáticos del sistema consultado.

Se establece, inclusive, la obligación para, toda persona que conozca el funcionamiento del sistema o las medidas aplicables para proteger los datos informáticos, de facilitar todas las informaciones necesarias para realizar las intervenciones anteriormente reseñadas.

c4. Recogida en tiempo real de datos informáticos.

Dos modalidades diferentes, aunque vinculadas, establece el Convenio, a este respecto:

a) En lo tocante a datos relativos al tráfico asociados a comunicaciones especificas transmitidas en su territorio por medio de un sistema informático, el art. 20 habilita a las autoridades pertinentes a:

- recoger o registrar dichos datos, en tiempo real, mediante medios técnicos existentes en su territorio;

- obligar a un suministrador de servicios, en el marco de sus capacidades técnicas a recoger o registrar dichos datos, en tiempo real, mediante medios técnicos existentes en su territorio; o prestar a las autoridades competentes su concurso y asistencia para recoger o registrar los datos.

Los Estados podrán obligar a los suministradores de servicios a guardar secreto sobre cualquiera de las habilitaciones reseñadas con anterioridad, así como sobre cualquier información al respecto.

b) Respecto a la interceptación de datos relativos al contenido, el art. 21 establece que cada Estado adoptará las medidas necesarias para habilitar a sus autoridades competentes, respecto a un abanico de infracciones graves a definir en el derecho interno, a:

- recoger o registrar mediante medios técnicos existentes en su territorio, en tiempo real, datos relativos al contenido de las comunicaciones concretas, transmitidas por medio de un sistema informático.

- obligar a un suministrador de servicios, en el marco de sus capacidades técnicas, a recoger o registrar los datos *supra* citados; o a prestar a las autoridades competentes su ayuda y asistencia para tal fin.

5. LA CONCILIACIÓN DE LA LUCHA CONTRA EL CIBERCRIMEN Y EL RESPETO A LOS DERECHOS DE LOS CIUDADANOS. LA NECESARIA LIMITACIÓN DE LAS MEDIDAS RESTRICTIVAS

Conviene recordar ahora como el art. 15 del Convenio establecía que la instauración, la puesta en marcha y la aplicación de los poderes y procedimientos que la misma establecen se sometan a las condiciones legales de los Estados firmante, garantizando el respeto de los derechos humanos y con observancia del principio de proporcionalidad.

Tras la exposición del elenco de medidas "investigadoras" que se establecen, cabe cuestionarse: ¿se cumple dicha proporcionalidad?, ¿se garantizan los derechos de los ciudadanos?.

La respuesta ciertamente no puede ser positiva, por cuanto lo que se construye es un aparato represor, donde la idea de seguridad prima sobre cualquier otra consideración.

Sorprende, ante todo, que el Convenio no dedique ni una sección a la imprescindible consideración de los datos personales ante tales poderes de investigación, salvo una mera referencia en el Preámbulo al Convenio 108 del Consejo de Europa[37].

De igual modo, se habilita a las autoridades nacionales a registrar y recoger datos, incluso en tiempo real, haciendo participes "obligatorios" de tal control a los suministradores de servicios, que de esta manera pasan a convertirse en "Policías de la Red".[38] Por si fuera poco, la determinación de las autoridades competentes corresponde a cada uno de los Estados signatarios, lo cual puede hacer diferir el rango –judicial o administrativo- de quienes se hallen legitimados para ordenar y supervisar tales controles. Creemos imprescindible que entre esas autoridades deben hallarse los encargados de la protección de datos en cada Estado, a

[37] Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

[38] Expresión esta utilizada por Javier Valiente, cuando con respecto al polémico e incoherente Proyecto de Ley de Servicios de la Sociedad de la Información en España, manifiesta que "El proyecto de Ley convierte a los Prestadores de Servicios de Internet en "Policías de la Red", teniendo que discernir qué contenidos o servicios son ilícitos y cuales no, o si quien comunica una presunta infracción es o no "la autoridad competente por razón de la materia". Cfr. http://www.elpais.es/misc/lssi/articulo15.html

quienes deberá consultarse inexcusablemente para evitar violaciones o intromisiones innecesarias en los derechos de los ciudadanos.

La lucha contra el delito, incluido el informático, debe ser, y de hecho es, una labor prioritaria en nuestras sociedades democráticas. Sucesos recientes han puesto de manifiesto la vulnerabilidad de nuestros sistemas de seguridad y la aparente facilidad con la que pueden perpetrarse atentados lesivos contra las personas y los bienes. Pero, sin menoscabo del recuerdo a las víctimas particulares, la violencia adquiere nuevos visos, pues busca como objetivo último la destrucción de nuestro modelo democrático, de nuestro sistema de libertades; sembrando el terror, e intentando convertirnos a todos en rehenes de la sinrazón, la violencia y el miedo.

Ahora bien, frente a esto no puede acogerse la teoría del "todo vale", pues existen límites éticos, y por supuesto jurídicos, al poder de control absoluto, amparándose en la indeterminación de conceptos como la seguridad nacional, el orden público o la "lucha sin cuartel" contra la violencia. No puede tolerarse la imagen, que parece consolidarse, de que todos debemos soportar la intromisión en nuestros derechos en aras de la seguridad. Como se ha señalado recientemente, "la reivindicación de límites éticos y morales al poder de la voluntad y, por tanto, de la supremacía del Derecho no puede ser parcial, escindida, de forma que sólo afecte a unos, pero no a otros"[39].

Las facultades investigadores que instituye el Convenio parecen avalar esa corriente.[40]

Todas las leyes de protección de datos contienen algún tipo de excepciones a la aplicación de sus normas[41], tipificando las situaciones en las que por razones de seguridad, para la defensa de la democracia y el orden

[39] GARZÓN REAL, B. Y GÓMEZ BENÍTEZ, J. M., "Terroristas, halcones y criminales de guerra". Vid. http://www.elpais.es articulo.html?xref=20020305elpepiopi_8&print=1&anchor=elpepiopi&type=Tes&d_date=05/03/02

[40] Uno de los países signatarios, concretamente Estados Unidos, pretende en su futura Ley sobre ciberseguridad endurecer duramente los castigos. Así las intrusiones en ordenadores que pongan "temerariamente" a personas en peligro significarán cadena perpetua , después que un Comité del Gobierno decidiera reescribir la futura *Cyber Security Enhancement Act.* El propio presidente de del comité manifestó que "hasta que nuestra infraestructura no sea segura, unos golpes de tecla y una conexión a Internet es todo lo que se necesita para desestabilizar la economía y poner vidas en peligro. Un ratón puede ser tan peligroso como una bomba". Cfr. http://www.elpais.es/articulo.html?xref=20020307 elpepiopi_8&print=1&anchor=elpepiopi&type=Tes&d_date=08/03/02

[41] Cfr. PEREZ LUÑO, A.E., «Informática jurídica y derecho de la informática en España», en *Informatica e Diritto*, nº 2, p. 97.

constitucional o para la defensa de los derechos de los demás se podrá limitar o suspender el derecho a la autodeterminación informativa[42].

En el ámbito convencional internacional el Convenio 108 del Consejo de Europa establece a este respecto, que podrán, dejarse sin efecto sus preceptos relativos a calidad de los datos, datos sensibles y derechos de los afectados cuando así estuviere previsto en la legislación de las Partes contratantes, y constituyera una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado, la seguridad pública, los intereses monetarios o la represión de los delitos, así como para la protección del interesado y de los derechos y libertades de otros (art. 8.2).

Se consagra de este modo la posición a tenor de la cual no existe un derecho absoluto ni una soberanía irrestringible sobre los propios datos, ya que la personalidad del individuo se desenvuelve dentro de la sociedad y de la comunidad, y ha de aceptar ciertas limitaciones. Ahora bien, esta naturaleza «limitada» no debe suponer en ningún caso una quiebra de la autodeterminación informativa.

La apelación a la defensa de determinados valores o intereses colectivos, no debe ser óbice para un uso torticero de las habilitaciones legales. La propia indefinición de los supuestos en los que es tolerable esa «limitación», coadyuva a la necesidad de una aplicación estricta de los mismos.

Así, como ha señalado Rigaux, del interés general debe distinguirse claramente el interés del Estado. Mientras que el primero señala los valores comunes a la colectividad política y a la sociedad civil, valores inscritos en los textos constitucionales e internacionales, el interés del Estado señala la permanencia de las instituciones políticas y su protección frente al enemigo exterior. No obstante, cuando los detentadores del poder invocan el interés del Estado, la seguridad pública o la seguridad nacional para legitimar la limitación de determinados derechos fundamentales, están particularmente expuestos a confundir este interés con la perpetuación del poder del que están democráticamente investidos[43].

[42] Para un estudio histórico de las limitaciones de los derechos fundamentales en función de la defensa de los intereses del Estado, vid. CRUZ VILLALON, P., El estado de sitio y la Constitución (La constitucionalización de la protección extraordinaria del Estado (1789-1878), Centro de Estudios Constitucionales, Madrid, 1980.

[43] Cfr. RIGAUX, F., «Introduction Generale», en Revue Trimestrielle des droits de l´homme, núm. 13 (monográfico «La liberté d´expréssion, son étendue et ses limites), janvier 1993, p. 17.

En este sentido si bien dichas limitaciones han de ser aceptadas, las mismas están sujetas a determinados requisitos que, ya desde lo señalado por el Convenio de 1981 del Consejo de Europa y el *Bundesversfassungeritchs* en su Sentencia sobre la Ley del Censo de Población de 1983[44], pueden sistematizarse en dos ineludibles y concretas exigencias:

a. Un fundamento legal, del que pueda deducirse con claridad y de forma inteligible para el ciudadano los supuestos y el ámbito de las limitaciones, y que responda, por tanto, al imperativo de claridad normativa inherente al Estado de Derecho[45].

A este respecto, el TEDH ha realizado unas importantes precisiones señalando como la expresión «prevista por la ley» indicada en el párrafo 2 del art. 8 del CEDH, implica que no basta con que la injerencia en los derechos esté prevista por una norma nacional, si no que ésta debe ser accesible al interesado, quien debe, además, poder prever las consecuencias que pueda tener para él. Además, cuando su práctica se realiza por medio de medidas secretas, que escapan al control de las personas afectadas, la misma ley debe definir el ámbito del poder atribuido a la autoridad competente con bastante claridad para proporcionar al individuo una protección adecuada contra la arbitrariedad[46].

b. Ha de utilizarse el principio de proporcionalidad en la restricción de estos derechos fundamentales; es decir, que la medida sea adecuada - necesaria en una sociedad democrática - y, además, indispensable para la consecución de los respectivos y predeterminados fines. La interferencia que lleve aparejada no puede ser desproporcionada a la importancia del objeto y a las cargas que imponga al ciudadano.

El concepto de necesidad implica, según reiterada jurisprudencia del TEDH, una exigencia social imperiosa; y sobre todo, la medida tomada debe ser proporcionada a la finalidad legítima perseguida. Además, el alcance del margen discrecional que tienen las autoridades no depende

[44] La sentencia se encuentra publicada, en trad. cast. de M. Daranas, en BJC, 1984, núm. 33, pp. 126-ss.

[45] Cfr. TORNE-DOMBIDAU JIMENEZ, J., y CASTILLO BLANCO, F. A., «Informática y protección de la privacidad del individuo (II)», en Actualidad Administrativa, núm. 22, 7-13 de julio 1993, p. 281; PEREZ LUÑO, A. E., La Seguridad Jurídica, 2ª edic. revisada y puesta al día, Ariel, Barcelona, 1994.

[46] Sentencias, Silver y otros, de 25 de marzo de 1983; Malone, de 2 de agosto de 1984; y Leander, de 26 de marzo de 1987.

solamente de la finalidad de la restricción, si no también de la naturaleza del derecho de que se trate[47].

Por su parte, la regla de la proporcionalidad es de observancia obligada para proceder a la limitación de un derecho fundamental. Ello conduce a la negación de la legitimidad de aquellas limitaciones que incidan en el ejercicio de los derechos fundamentales de forma poco comprensible, de acuerdo con una ponderación razonada de bienes y proporcionada de los mismos en relación con el contenido y finalidad de la medida restrictiva[48].

Por otra parte, las limitaciones del derecho no deben ser de tal calado que supongan un menoscabo de su contenido esencial. De nada sirve el reconocimiento de los derechos a favor de los ciudadanos si se limita su ejercicio de forma que, más que una limitación, debamos hablar de una derogación encubierta, de su propia naturaleza, atributos y funciones.

Tal y como ha señalado Pérez Luño, y siguiendo la doctrina de nuestro Tribunal Constitucional, «dos acepciones pueden distinguirse de la noción de «contenido esencial»: la primera equivalente a «naturaleza jurídica de cada derecho», que se considera preexistente al momento legislativo; la segunda a «intereses jurídicamente protegidos», en el sentido de que se lesionaría el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección»[49].

Ante la proliferación y constante apelación por parte de las autoridades públicas a estas limitaciones conviene insistir, siguiendo nuevamente a Pérez Luño, en el carácter excepcional de estos supuestos; en que su razón de ser no puede ser otra que la conservación del orden democrático; y en que la existencia de tal motivación no puede quedar en manos de la Administración, sino que debe quede ser reconocida por los Parlamentos como depositarios de la soberanía popular[50].

[47] Sentencias, Lingens, de 8 de julio de 1986; Gillow, de 24 de noviembre de 1986; y Leander, de 26 de marzo de 1987.

[48] Cfr. GOMEZ TORRES, C., «El abuso de los derechos fundamentales», en la obra colectiva, edic. a cargo de A. E. Pérez Luño, Los derechos humanos: significación, estatuto jurídico y sistema, Publicaciones de la Universidad de Sevilla, Sevilla, 1979, pp. 301-332. Asimismo, TORNE-DOMBIDAU JIMENEZ y CASTILLO BLANCO, F. A., «Informática y protección de la privacidad...», cit., p. 283.

[49] Cfr. PEREZ LUÑO, A. E., Los derechos fundamentales, 3ª edic., Tecnos, Madrid, 1988, p. 77.

[50] Cfr. PEREZ LUÑO, A. E., «Informática jurídica y derecho de la informática en España», cit., p. 97.

Como conclusión, debe tenerse presente que estas limitaciones *suponen de facto* otorgar a los poderes públicos la posibilidad de actuar, generalmente de forma secreta, al margen de los mecanismos de control establecidos en las sociedades democráticas. Ello ha llevado al TEDH ha afirmar la necesidad de establecer unas garantías adecuadas y suficientes contra los abusos, ya que un sistema de control destinado a proteger la seguridad nacional crea el riesgo de socavar, e incluso destruir, la democracia con el argumento de defenderla[51].

[51] Vid. entre otras las Sentencias, Klass y otros, de 6 de septiembre de 1978; y Leander, de 26 de marzo