LAS LIBERTADES EN LA ERA DE INTERNET

ANTONIO-ENRIQUE PÉREZ LUÑO[1]

1. PLANTEAMIENTO: INTERNET Y LAS LIBERTADES

En una sugerente Ponencia presentada en el Coloquio Internacional Humboldt celebrado en Montevideo en Abril de 2003, Mario G. Losano reivindicaba el fortalecimiento de la relación entre las culturas jurídicas europea y latinoamericana. La garantía del pluralismo cultural, también en la esfera jurídica, puede ser una respuesta para muchos de los problemas del mundo globalizado. La potenciación del acercamiento entre Europa e Iberoamérica como contrapeso a la avasalladora hegemonía norteamericana, puede permitir abordar soluciones más equilibradas para los grandes retos de las sociedades tecnológicas del presente (Losano, 2004, 28). La obra cien-

[1] Catedrático de Filosofía del Derecho de la Facultad de Derecho de la Universidad de Sevilla

tífica del profesor Mario G. Losano constituye un modelo estimulante de inquietud intelectual tendente a enfocar, desde una tradición cultural europea que no desdeña el diálogo con la cultura jurídica norteamericana contemporánea, algunos de los retos más acuciantes que el desarrollo informático plantea al derecho (Losano, 1985, 1986 a y b, 1987, 1991, 1992, 1993). En las reflexiones en que este trabajo consiste, se tratará de proseguir el ejemplo científico y el magisterio del profesor Losano en lo que concierne a los problemas centrales del desarrollo tecnológico en el plano jurídico. En particular, se abordará una cuestión de insoslayable actualidad e importancia: los impactos de Internet en la esfera de las libertades.

Uno de los desafíos más importantes de la época en que vivimos consiste en establecer una ecuación exacta, correspondiente a los apremios del tiempo, en las relaciones entre los avances tecnológicos y la tutela de las libertades. El ámbito del mundo, cada vez más planetario, ha apretado decisivamente sus exigencias y reclama un adecuado planteamiento de las garantías de los derechos cívicos ante el desarrollo de las Nuevas Tecnologías (NT). El horizonte actual de la ciudadanía, que orienta y circunscribe las pautas de su ejercicio, se halla determinado por los impactos tecnológicos de la información y la comunicación. Esas redes telemáticas suscitan la impresión de que el tamaño del mundo se ha contraído, de que los ciudadanos y los pueblos se hallan dinámicamente más próximos que en cualquier etapa histórica anterior.

La era de la informática y de la telemática ha contribuido a que se adquiera la convicción de que el *hábitat* cívico del presente posee dimensiones planetarias, en la medida en que hoy con el acceso a Internet cada ciudadano puede establecer, sin salir de su domicilio, una conversación en tiempo real, sin límites en el espacio ni en las personas.

Los últimos veinticinco años han acelerado con ritmo creciente los procesos de renovación tecnológica que tan profundamente inciden en las relaciones cívicas. La presencia de las redes de información y comunicación en los ámbitos jurídicos y políticos ha determinado que se adquiera consciencia de que nunca como hoy se había sentido tan intensamente la necesidad de concebir los valores y derechos de la persona como garantías universales. De esa exigencia de universalidad se infiere la reivindicación de que los derechos de la persona se tutelen sin discriminación alguna por razones de raza, de lengua, de sexo, de las religiones profesadas o de las convicciones

ideológicas. Se siente hoy con mayor intensidad que en cualquier etapa histórica precedente, la exigencia de que los derechos y las libertades no se vean comprometidos por el tránsito de las fronteras estatales; lo que implica tomar en serio el compromiso en pro de la ciudadanía cosmopolita.

Estos requerimientos imponen a la teoría jurídico-política una reflexión sobre las libertades que ya no puede transitar por los cómodos carriles preestablecidos por una larga historia doctrinal e institucional. En un mundo interdependiente, en el seno de sociedades interconectadas, la garantía de los derechos cívicos, se halla en directa conexión, para bien o para mal, con los procesos que definen su instalación tecnológica. El estudio actual de los derechos humanos no puede omitir esa referencia contextual, ni puede abdicar del juicio crítico de sus implicaciones. Se trata de lograr que los desarrollos tecnológicos no menoscaben ni se alcancen a costa de las libertades cívicas. Por ello, las reflexiones interdisciplinarias tendentes a establecer un diálogo fluido entre el universo tecnológico y la esfera de los derechos de los ciudadanos se han hecho cada vez más perentorias.

Entraña una significativa paradoja que en la obra del más importante pensador español contemporáneo, José Ortega y Gasset, se enuncie una premonitoria alarma sobre los riesgos de la técnica y, al propio tiempo, un reconocimiento de sus virtualidades y su necesidad. En su estimulante *Meditación de la técnica*, de 1939, indicaba que: "De puro llena de posibilidades, la técnica es mera forma hueca, como la lógica más formalista; es incapaz de determinar el contenido de la vida. Por eso estos años en que vivimos, los más intensamente técnicos que ha habido en la historia humana, son de los más vacíos" (Ortega y Gasset 1983, 5. 366). Pero como contrapunto y captando la profunda ambivalencia del fenómeno tecnológico, en su Prólogo a un *Diccionario enciclopédico abreviado*, que data de la misma fecha, Ortega mostraba no ser inmune a las inmensas posibilidades que abren los avances tecnológicos y a la necesidad de no ser indiferentes, o ingenuamente hostiles a ellos. Decía Ortega que, en las sociedades desarrolladas, la propia vida humana se ha hecho tan compleja que requiere el recurso a la técnica. Por eso, denunciaba la postura simplista de "todo el que quiere dárselas de muy espiritual habla contra el maquinismo contemporáneo... El antimaquinismo es pura fraseología y beatería". Estima Ortega que el hombre es el animal maquinista y, por eso mismo, lo que hace falta es que invente las nuevas

máquinas que demandan los nuevos problemas y conflictos de la época presente. "Ahora nos encontramos –en palabras de Ortega– ante una nueva necesidad: las máquinas son tantas y tan complicadas, que hace falta una máquina para manejar las demás, o, dicho en otros términos: es preciso suscitar una nueva sabiduría que nos enseñe a asimilar y practicar toda nuestra oceánica sabiduría. Esto –y no retroceder de la máquina al cocotero– es lo que reclama la altitud de los tiempos" (Ortega y Gasset, 1983, 6, 364-365).

El ejemplo de Ortega constituye una oportuna invitación a abordar los problemas presentes de los derechos humanos desde las amenazas y las posibilidades que dimanan de su condicionamiento tecnológico. Al asumir el desafío que ello entraña, Ernesto Garzón Valdés, en fecha muy reciente, avanza un lúcido balance sobre las actitudes de *Optimismo y pesimismo en la democracia*, indicaba algo que es del todo pertinente para el asunto aquí estudiado. En relación con quienes se aferran a un mantenimiento, cerrado a cualquier transformación renovadora, de las libertades, opaco a las proyecciones tecnológicas, serían pertinentes sus observaciones relativas a que "no se debe: caer en la tentación de suponer que se ha logrado ya la realización plena de todas las potencialidades que encierra la concepción de la democracia constitucional". Es necesario admitir que: "la siempre cambiante realidad exige la actualización coherente de sus principios y la adecuación cabal a los desafíos que el progreso científico-técnico trae aparejados". El reforzamiento de las libertades en las sociedades democráticas requiere, para Garzón Valdés: "la vigilancia estricta de los posibles vaciamientos de las instituciones democráticas y un deber de pensar los ajustes que las democracias nacionales, consolidadas o no, requieren para enfrentar los peligros que dimanan de los desafíos sociales, culturales y tecnológicos del presente". Al propio tiempo, respecto a la actitud de los que abogan por una inmediata aceptación de un nuevo diseño tecnológico de los derechos humanos, a través de la "panacea" de experiencias teledemocráticas, tiene pleno sentido la advertencia de Garzón Valdés dirigida a: "no admitir las falsas ilusiones que suelen tender un velo que distorsiona la realidad al idealizar futuros inalcanzables y vedar el camino hacia soluciones sensatamente realizables" (Garzón Valdés, 2003a, 32). Una de las cuestiones de mayor actualidad y relevancia en la que se hace patente la exigencia de la "conciencia tecnológica" de los juristas y politólogos auspiciada por Frosini, es la evaluación del impacto de Internet en los sistemas jurídicos actuales. Dicha

"conciencia tecnológica supone una actitud reflexiva crítica y responsable ante los nuevos problemas que, en las diversas esferas del acontecer social suscita la tecnología, y ante los que ni el derecho ni los derechos humanos pueden permanecer insensibles" (Frosini, 1986).

2. INTERNET: NUEVA FRONTERA DE LA INFORMACIÓN Y LA COMUNICACIÓN

No parece lícito dudar que Internet (*International Network of Computers*) está siendo el fenómeno estelar de las Nuevas Tecnologías de la información y la comunicación a partir de la década de los noventa. En el umbral de un nuevo milenio, Internet se presenta como un paso decisivo en el avance de los sistemas de información y comunicación a escala planetaria. Gracias a Internet cada ciudadano, sin moverse de su casa, puede acceder a los centros de documentación más importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia. Si hace algunos años parecía que la "aldea global" era el gran reto del futuro, hoy Internet ha convertido en realidad presente el "hogar global", en la medida en que cada domicilio de los usuarios de la red constituye la terminal de un sistema integrado universal.

Conviene no resbalar, por su importancia, en la extensión presente y perspectivas futuras –se dice que cada minuto se incorpora un nuevo usuario a la red– de este amplísimo vehículo de información e intercomunicación. Internet es una red de redes que conecta millones de ordenadores pertenecientes a instituciones académicas, entes públicos, empresas privadas y un número creciente de internautas particulares. Se calcula que en la actualidad la emplean más de cien millones de usuarios, cifra que aumenta con una dinámica expansiva y limitada. La explosión de su crecimiento se ha debido principalmente a la difusión del parque de ordenadores personales equipados con módem y con posibilidades de conectarse a la red telefónica. Con la aparición de herramientas de uso de la red accesibles a todos se ha multiplicado el número de usuarios no especialistas en informática, frente al carácter privativo para los expertos que Internet tuvo en sus inicios (cfr. Colom y Van Bolhuis, 1995; Moreno, 1995; Rico, 1995).

El ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada. Su conquista se ha convertido en meta obligada para quién desee sentirse miembro de la sociedad informática y es en la actualidad uno de los puntos de encuentro para el ocio y el negocio, que cuenta con mayores perspectivas de futuro (Castillo, 2003; Lagares, 2000; Rico, 1995; Sánchez Bravo, 2001).

3. PROBLEMAS Y RIESGOS JURÍDICOS DE INTERNET

No obstante, junto con esas incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permite la navegación por el ciberespacio, Internet ha hecho surgir en los últimos tiempos graves motivos de inquietud. El escándalo que, en fecha no muy lejana, agitó a la opinión pública europea en relación con el tráfico de imágenes de prostitución infantil a través de Internet, así como la utilización de la red para difundir propaganda de grupos neonazis y bandas terroristas, ha supuesto la confirmación de un peligro desde hace algún tiempo anticipado. Los miles de ciudadanos europeos, inmediata o potencialmente agredidos por esas imágenes o mensajes criminales, abren una brecha en la inconsciencia cívica y política sobre los peligros que entrañan determinadas manipulaciones de las nuevas tecnologías. Ha sido preciso llegar a esta situación para que el conformismo cotidiano de quienes tienen como misión velar por la tutela de las libertades, y quienes tienen como principal tarea cívica el ejercerlas, se viese agitado por la gravedad del riesgo y la urgencia que reviste su respuesta.

No es admisible, al menos para juristas, políticos y tecnólogos, aducir sorpresa o desconocimiento de los eventuales peligros implícitos en el uso de las nuevas tecnologías. Desde hace tres décadas, quienes han evaluado el impacto de la informática en las libertades, han alertado sobre esos peligros, y cualquier especialista mínimamente avisado incurriría en negligencia inexcusable de haberlos desatendido. En las sociedades avanzadas con tecnología punta ya no se puede juzgar como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que con el descubrimiento de los abusos perpetrados a través de Internet se han convertido en una siniestra realidad (Branscomb, 1995; Cavazos y Morin, 1994; Lagares, 2000).

Internet ha supuesto un factor de incremento de formas de criminalidad, al potenciar la difusión de sabotajes, virus y abordajes a los

sistemas por parte de un número imprevisible e incontrolable de *piratas informáticos* (*Hackers*). Las "autopistas de la información" entrañan también un grave riesgo para la protección de los programas. Asimismo, la facilidad de intercambiar informaciones a distancia puede generar importantes peligros para la protección de los datos personales.

Internet implica, por tanto, el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos (Bensoussan, 1996; Iteanu, 1996; Ribas, 1996). Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos: la intimidad, la imagen, la dignidad y el honor de las personas, la libertad sexual, la propiedad intelectual e industrial, el mercado y los consumidores, la seguridad nacional y el orden público (Pérez Luño, 1998; 2000; Sánchez Bravo, 2001).

El carácter internacional e ilimitado de esas conductas hace más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas pueden plantearse conflictos sobre la jurisdicción sancionadora competente. Existe una evidente dificultad para determinar la responsabilidad jurídica en un medio, como el de Internet, en el que existen diferentes operadores que concurren en la cadena de comunicaciones: el proveedor de la red, el proveedor de acceso, el proveedor de servicio y el proveedor de contenidos. Este problematismo se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos con legislaciones, a su vez, diferentes. En la doctrina francesa se ha aludido al fenómeno de "*délocalisation*" de Internet (Piette-Coudol y Bertrand, 1997; Lagares 2000), para hacer hincapié en los problemas jurídicos que plantea establecer el Derecho aplicable a actuaciones realizadas en una red planetaria sin "localización" geográfica precisa y determinada.

Debe también tenerse en cuenta la dificultad que entraña establecer la responsabilidad derivada de determinados contenidos ilícitos transmitidos a través de Internet. A tenor de las diferentes regulaciones legislativas nacionales se tenderá a hacer recaer dicha responsabilidad en los *creadores* de la información, en los que han facilitado su *transmisión* y *acceso* a la misma, o en los *consumidores* que la aprovechan o utilizan (Piette-Coudol y Bertrand, 1997; Stuckey, 1995).

Internet plantea una preocupante paradoja, que deriva de su eficacia global e ilimitada para atentar contra bienes y derechos, mien-

tras que la capacidad de respuesta jurídica se halla fraccionada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean a los ordenamientos jurídicos nacionales y al orden jurídico internacional.

No huelga tampoco reconocer que la impunidad de determinadas formas de criminalidad informática no siempre constituye una negligencia imputable al legislador. Porque en un sector como el de las relaciones entre la Informática y el Derecho, constantemente, cada Feria tecnológica abre nuevas proyecciones informáticas al Derecho, o innova bienes informáticos que requieren nuevos procedimientos de tutela jurídica, o da a conocer dispositivos que condenan al anacronismo los medios de protección jurídica anteriormente existentes. La criminalidad informática se caracteriza, en suma, por las dificultades que entraña *descubrirla, probarla y perseguirla*. Se ha hecho célebre la imagen de que los sistemas informáticos son como "queso de Gruyer" (Pérez Luño, 1998; 2000), por las enormes oquedades y lagunas que quedan siempre abiertas a posibles atentados criminales.

4. SISTEMAS DE SEGURIDAD EN INTERNET

Aunque Internet puede haber contribuido a crear nuevos riesgos, las técnicas informáticas ofrecen también nuevas medidas de seguridad para oponerse a los atentados contra bienes e intereses jurídicos. Entre las medidas de seguridad más difundidas y eficaces se pueden citar las siguientes:

a) *Programas de encriptación*, que permiten la conversión de mensajes en lenguaje natural en textos que utilizan un lenguaje clave y que aseguran que nadie excepto quien posea la transcripción de esas claves podrá descifrar. Ha adquirido especial celebridad el programa de encriptación debido a Philip Zimmermann denominado PGP (*Pretty Good Privacy*), que está siendo utilizado por numerosos usuarios de Internet.

Si bien estos programas de seguridad, junto a sus logros para garantizar la confidencialidad de la transmisión de informaciones lícitas, tiene su reverso en haber contribuido a dificultar el descubrimiento de redes informativas ilícitas. La DEA, servicio norteamericano antidrogas, así como otros servicios policiales, han denunciado sus dificultades para perseguir a los narcotraficantes entre los laberintos y las encriptaciones de sus mensajes electrónicos.

b) *Los filtros*, consistentes en programas informáticos selectivos que bloquean el acceso a determinados documentos pero no a otros. La Unión Europea apoya la denominada PICS (*Platform for Internet Content Selection*). Se trata de un servicio para seleccionar contenidos en Internet que lanzó oficialmente el *World Wide Web Consortium*. Estos filtros pueden programarse en un triple sentido: 1) *"Lista blanca"*, dejando pasar solamente aquellos servicios o informaciones que previamente han sido registrados; 2) *"Lista negra"* bloqueando aquellos servicios o programas a los que no se desea tener acceso. Se ha hecho famosa la lista *CyberNot*; que abarca unos siete mil programas clasificados como nocivos por sus contenidos de violencia, obscenidad, racismo, cultos satánicos, drogas... Gracias a este sistema los padres pueden bloquear de forma selectiva el acceso a aquellos servicios que consideran nocivos o peligrosos para sus hijos; 3) *"Etiquetado neutro"*, permitiendo construir un menú de servicios personalizados para cada usuario. Este sistema ofrece un alto grado de flexibilidad y seguridad, al facilitar que cada usuario realice personalmente la criba de aquellos contenidos de Internet que juzgue apropiados a su sensibilidad, cultura y sistema de valores.

c) *Los cortafuegos*, que operan facilitando o impidiendo la transferencia de imágenes o datos desde Internet a un ordenador o viceversa. Estos sistemas de seguridad permiten el acceso a aquellos servicios previamente establecidos, cortando la entrada o salida a los demás.

d) *Los certificados digitales*, que permiten identificar o relacionar a todas las partes que intervienen en transacciones comerciales realizadas a través de Internet, dotándolas de la máxima rapidez y seguridad. Así, por ejemplo, el sistema *SET* (*Secure Electronic Transaction*).

e) *Los Ciberpolicías*, se trata de entidades, como por ejemplo *FIRST* (*Forum of Incident Response and Security Teams*) y *CERT* (*Computer Emergency Response Team*), las cuales ofrecen equipos de expertos en la localización de piratas informáticos, y suministran programas de defensa frente a sabotajes y proporcionan ayuda en caso de siniestros informáticos. Algunas policías de países técnicamente desarrollados han organizado unidades especiales en la investigación de actividades criminales realizadas a través de Internet. En España existe un Grupo de Delitos Informáticos perteneciente a la Unidad Central de Policía Judicial.

Estos sistemas de seguridad representan un principio de esperanza frente a los riesgos y peligros que, sin resquicio a dudas, com-

portan las actividades abusivas o ilícitas realizadas a través de Internet. Su eficacia es diversa y, todavía, difícilmente evaluable, pero esos sistemas demuestran frente a pesimistas y escépticos que Internet no es un paraíso para el ejercicio de la delincuencia, ni un espacio inexorablemente condenado a la zozobra y la inseguridad (Bensoussan, 1996; Bustos, 1996; Lagares, 2000; Ribas, 1996).

5. SEGURIDAD VERSUS LIBERTAD: ECHELON Y CARNIVORE

Para combatir las nuevas formas de criminalidad potenciadas a través de la Red, se han creado potentes sistemas estatales de seguridad. Los Estados han diseñado mecanismos de investigación y espionaje, con los que hacer frente a los nuevos desafíos.

Estos sistemas entrañan, sin embargo, un preocupante riesgo para las libertades cívicas, al suponer implacables mecanismos de control social y de perforación de la intimidad. El funcionamiento de estos sistemas, no siempre responden a los cauces y exigencias de las sociedades democráticas, ya que, en la práctica, imponen a los ciudadanos la aceptación resignada de la intromisión en algunos de sus derechos.

Echelon es un sistema de interceptación de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda. Sus dos principales características, frente a otros sistemas de espionaje, son: su capacidad para ejercer un control simultáneo de todas las comunicaciones. Todo mensaje enviado por fax, teléfono, Internet o e-mail, con independencia de su remitente, puede captarse mediante estaciones de interceptación de comunicaciones, lo que permite conocer su contenido. Se trata de un sistema que funciona a escala mundial gracias a la colaboración e interacción de los Estados *supra* citados, lo cual posibilita una vigilancia a nivel mundial de las comunicaciones por satélite. Poniendo en común iniciativas, recursos técnicos y lógicos, costes y objetivos, representando una implacable y completa red de control a escala planetaria.

Carnivore es un sistema de sofware y hardware con capacidad para localizar y perseguir las comunicaciones de un usuario de Internet. El sistema interviene la comunicación en un punto estratégico, como es el ISP (Proveedor de Servicio de Internet). Toda información pasa por los ISP, servidores que todos los internautas utilizamos para conectarnos a Internet. Cada palabra que escribimos o ejecuta-

mos siempre es recogida por el ISP que nos da acceso a la Red. La *Caja Negra* del FBI se instala en el servidor del ISP. Pero además de *software*, el FBI incluye el *hardware* compuesto por una PC ensamblado en una caja modelo Rack para que pueda incorporarse fácilmente en las redes del ISP, como si fuera un concentrador o un "router" más, sin necesidad de dispositivos externos.

Echelon y Carnivore son la muestra palpable de los riesgos que para la libertad de los ciudadanos implica la creación de sistemas de seguridad y vigilancia, no sometidos a controles por parte de instancias internacionales garantes de que la persecución de criminalidad en la Red, no pueda degenerar en una vigilancia incontrolada de millones de ciudadanos pertenecientes a todos los países del mundo. Los terribles e inexcusables atentados del 11 de Septiembre, no pueden servir de coartada para una limitación injustificable de los derechos y libertades cívicos. El secretismo, la falta de transparencia de su forma de proceder, la extensión de sus poderes, son buena muestra de ese asedio a los derechos, que se pretende legitimar bajo la coartada de la seguridad. Urge reivindicar el status de una ciudadanía universal frente al riesgo de que las potencias hegemónicas degraden a millones de ciudadanos del planeta a la mera condición de súbditos.

En fecha reciente, Ernesto Garzón Valdés, en una interesante reflexión sobre: *Lo íntimo, lo privado y lo público* (2003b,14 ss.), ha planteado, con ejemplar lucidez el dilema en el que se debaten las sociedades democráticas del presente. De una parte, estas sociedades se hallan asediadas por la amenaza de organizaciones criminales (terrorismo, mafias, narcotraficantes…), que ponen en peligro la seguridad de los ciudadanos y la propia subsistencia de un modelo de convivencia basado en la paz y la libertad. Para combatir esa amenaza se recurre a medios de vigilancia y control, cada vez más poderosos, que suponen un grave menoscabo del derecho a la intimidad. "¿Cómo lograr un equilibrio moralmente aceptable –se pregunta Garzón Valdés– entre la ventaja de prever y castigar delitos, por una parte, y, por otra, evitar el peligro de la destrucción de la personalidad del *inspeccionado*?"(2003b, 24 ss.).

Según el propio Garzón Valdés, tras los ataques terroristas en Nueva York y Washington, esta cuestión ha adquirido enorme actualidad y relevancia. Los medios tecnológicos permiten hoy una omnisapiencia de la Thought-police (policía del pensamiento), parangonable a la omnisapiencia divina de las sociedades teocráticas del

pasado. En dichas sociedades se aseguraba la sumisión y el consentimiento de los súbditos, al difundir en ellos la creencia en un "ojo de Dios" capaz de escrutar hasta lo más íntimo y recóndito de cada persona (vid. Pérez Luño, 2003, 345 ss.). Garzón sugiere al respecto, las siguientes propuestas de decreciente radicalidad:

> *"1. Permitir la acción de una Thought-police a todo lo largo y lo ancho de la sociedad, sin distinción de inocentes, sospechosos y culpables.*
> *2. Limitar la acción de la Tbought-police a sospechosos y culpables.*
> *3. Limitar la acción de la Thought-police a culpables.*
> *4. Prohibir en todos los casos la acción de la Tbought-police" (Ibíd.).*

Los partidarios de la alternativa 1 podrían aducir que toda sociedad que desee lograr el mayor grado de seguridad y orden público, es decir, el menor riesgo de criminalidad, tiene interés legítimo en distinguir los buenos de los malos ciudadanos y, en caso de sospecha, conviene eliminar la duda colocando al sospechoso en alguna de las dos categorías básicas. Desde este enfoque, habría que rechazar de plano la alternativa 4. La alternativa 3 sería también insuficiente, porque siempre actuaría una vez cometido el delito. La alternativa 2 parecería una versión empobrecida de 1 y no pocas veces difícil de practicar debido a la vaguedad del concepto de "sospechoso" desprendido del concepto de "inocente".

Desde la perspectiva antitética de los defensores de la alternativa 4 se sostendrá que una cosa es procurar, a través de medios de prueba externos: indicios, análisis de contexto y declaraciones de testigos…, conocer la intención que animó la realización del acto en cuestión y otra forzar la intimidad de la persona con la consiguiente destrucción de su autonomía personal. Admitir cualquier versión de la Thought.-police sería propiciar una de las formas más refinadas de la tortura: la aniquilación espiritual del observado.

En función de estas premisas, concluye Garzón Valdés que, quien proponga alguna de las alternativas 1-3 se ha saltado el cerco del Estado social de derecho democrático liberal. En una sociedad de ciudadanos vigilados y transparentes la posibilidad de cometer delitos podría llegar a ser inexistente. Pero esa sería la aspiración del Estado totalitario llevado a sus últimas consecuencias: la negación total de la libertad individual. En un Estado de derecho siempre será posible, aunque no deseable, una actuación delictiva y es esta capacidad para

delinquir la que está en la base de la responsabilidad jurídica y confiere sentido a la imposición de deberes y sanciones jurídicos. "Pero no sólo de la capacidad jurídica sino también de la capacidad de ser agente moral" (Garzón Valdés, Ibíd.).

Estas consideraciones conducen a inferir que los macrosistemas de seguridad en el ciberespacio, es decir, *Echelon* y *Carnivore* constituyen versiones extremas de la alternativa 1, en la tipología propuesta por Garzón Valdés. Se trata de mecanismos de vigilancia y control que vulneran todas las garantías penales propias de una sociedad democrática. Involucran en su Thought.-police a todos los ciudadanos, sin distinguir, ni respetar la presunción de inocencia, ni siquiera diferentes grados de peligrosidad social. Suponen la instauración universal de la sospecha y de la presunción de culpabilidad.

Los macrosistemas de seguridad son, paradójicamente, un atentado frontal contra la seguridad jurídica, al desconocer las garantías básicas de la promulgación (lex promulgata) con carácter previo (lex previa) y con la necesaria claridad (lex manifesta) de los supuestos fácticos de ilicitud. No respetan, por tanto, el principio de legalidad penal, al no tipificar previamente las conductas que van a ser objeto de control e injerencia en el ámbito íntimo (Pérez Luño, 1994, 30 ss.)

Los macrosistemas de control ciberespacial representan formas implacables de colonización y aniquilación de la intimidad y suscitan la alarma de incubar una versión todavía más siniestra del "Gran Hermano" imaginado por Orwell, en la medida en que sus poderes de vigilancia y control exceden los límites de un Estado para extenderse por todo el orbe. La seguridad nunca debe conseguirse a costa de la libertad de los ciudadanos, pues sin libertad nunca podremos estar seguros (Pérez Luño, 2004; Sánchez Bravo, 2002).

6. EL CIBERESPACIO: ¿ANARQUÍA LIBERTARIA O LIBERTAD GARANTIZADA?

Como la mayoría de las grandes conquistas científicas y tecnológicas que registra la historia, Internet es una realidad ambivalente. Renunciar a sus logros sería hoy una pretensión imposible, porque se trata de un avance imprescindible y un signo del progreso de nuestro tiempo. Pero ello no debe conducir a aceptar pasivamente o a claudicar ante los riesgos de "*abordaje*" criminal que amenazan la navegación por el ciberespacio, ni ante la "colonización" de la Red por parte de los controles estatales que limitan injustificadamente la libertad.

He indicado *supra* que, en sus inicios, uno de los mayores alicientes de Internet residía en su carácter *ácrata*; se trataba de un espacio absolutamente libre, sin ningún tipo de autoridad o poder que lo regulara o acotara. Como elocuente ejemplo de esa concepción anárquica y libertaria de Internet puede citarse la *Declaración de Independencia del Ciberespacio* "promulgada" por John Perry Barlow en Davos, Suiza, el 8 de Febrero de 1996. Dicha Declaración ha adquirido notable celebridad en estos meses entre los usuarios de Internet. Consiste en un texto que, en mi opinión, se articula en torno a tres ideas-guía:

1ª) La afirmación de la total *autonomía* de los cibernautas respecto a cualquier tipo de autoridad estatal: "Gobiernos del Mundo Industrial...No son bienvenidos entre nosotros. No tienen ninguna supremacía donde nos juntamos...El Ciberespacio está fuera de sus fronteras".

2ª) Negación de los *conceptos y categorías jurídicas tradicionales*: "Vuestros conceptos legales de propiedad, expresión, identidad, movimiento y contenido no se aplican a nosotros. Aquellos se basan en la materia, pero en nuestro mundo la materia no existe".

3ª) Confianza *utópica* en un ciberespacio ideal: "Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y justa que el mundo creado anteriormente por sus gobiernos" (Barlow, 1996). En España [se] ha mantenido una tesis análoga, tendente a reivindicar la libertad del ciberespacio y su consiguiente independencia respecto a cualquier intento de reglamentación jurídica estatal, Fernández Hermana (1998).

Como contrapunto a esa visión idílica de Internet señala el profesor de Teoría de la Comunicación en la Universidad París-VII y Director de *Le Monde Diplomatique*, Ignacio Ramonet, que el ciberespacio está siendo colonizado despiadadamente por todos los gigantes de las telecomunicaciones. Internet está creando nuevas formas de desigualdad entre "inforicos" e "infopobres", al establecer discriminaciones graves en el acceso y utilización de informaciones entre el Norte y el Sur, donde la falta de equipos va a condenar a la marginación a millones de personas. Recuerda, por ejemplo, que hay más líneas telefónicas sólo en la isla de Manhattan (Nueva York), que en toda África negra, y sin esas líneas no se puede acceder a Internet. Según Ramonet resulta ingenuo pensar que necesariamente el au-

mento de comunicación debe traducirse en mayor equilibrio y armonía social. La comunicación, en sí, no es progreso social "y mucho menos cuando la controla, como es el caso de Internet, las grandes firmas comerciales y cuando, por otra parte, contribuye a acrecentar las diferencias y desigualdades entre ciudadanos de un mismo país, y habitantes de un mismo planeta. Internet –concluye Ramonet– era una esperanza; nos la han robado" (Ramonet, 1997; vid., también, Fenández Calvo, 1996).

Internet ha abierto nuevas y preocupantes posibilidades operativas a los sistemas de control social y político. Se ha hecho célebre una imagen expuesta por Philip Zimmermann en su informe ante el Subcomité de Política Económica, Comercio y Medio Ambiente del Congreso Norteamericano. Indicaba allí Zimmermann que en el pasado cuando el Estado pretendía violar la intimidad de los ciudadanos debía esforzarse en interceptar, abrir al vapor y leer el correo, o escuchar, grabar y transcribir conversaciones telefónicas. Eso era como pescar con caña, de pieza en pieza. Por el contrario, los mensajes del correo electrónico son más fáciles de interceptar y se pueden escanear a gran escala, y ordenar en función de palabras claves. Esto es como pescar con red; y supone una diferencia orwelliana cuantitativa y cualitativa para la garantía de la democracia.

El utopismo ácrata se opone a cualquier regulación del Ciberespacio por entender que con ello se reprime la libertad de los cibernautas, a la vez, que se refuerza el poder estatal. Pero la realidad no es tan simple. Paradójicamente los grandes beneficiarios de la anarquía de Internet no son los cibernautas particulares, sino las grandes multinacionales e, incluso los aparatos de control social de los gobiernos. No huelga advertir que, en los últimos años, se están transmitiendo por Internet, sin ningún tipo de garantías y con evidente menoscabo del derecho a la intimidad, datos personales (incluso voz e imagen) en investigaciones policiales; a través de un medio que por su naturaleza y características es accesible a millones de usuarios de todo el mundo. Tampoco está de más, recordar que algunos Colegios de Abogados norteamericanos han denunciado las prácticas de determinadas oficinas fiscales tendentes a interceptar las comunicaciones por Internet entre distintos bufetes de sus colegiados, especialmente en casos referentes a narcotráfico (Cavazos y Morin, 1994).

Los peligros de una utilización abusiva, incontrolada o criminal de ese espacio plantean ahora, de forma apremiante, la necesidad de su ordenación. Han sostenido historiadores muy autorizados que la

historia es cíclica y retorna siempre; quizás por ello los actuales debates sobre Internet recuerdan a aquellos mantenidos hace siglos por los filósofos contractualistas en relación con el estado naturaleza. En la tradición contractualista se explica el origen de las instituciones políticas y jurídicas a partir de la exigencia –empírica o racional, utilitaria o ética, a tenor de las diversas interpretaciones del estado de naturaleza y el pacto social– de abandonar una situación (el estado de naturaleza) en la que el hombre posee una ilimitada (aunque insegura) libertad, a otra de libertad limitada pero protegida y garantizada por la autoridad y las leyes (Pérez Luño, 1998; 2000).

7. ALGUNAS RESPUESTAS JURÍDICAS

Una vez perdida la inocencia del idílico "estado de naturaleza" de libertad sin restricciones de Internet, las circunstancias aconsejan remediar los peligros del desorden mediante soluciones jurídicas. Esa necesidad de apelar al Derecho para poner coto a los abusos perpetrados desde Internet ha llevado a algunos juristas a invocar el art.301 del nuevo Código Penal español de 1995, que pena a quién "convierta o transmita bienes, sabiendo que éstos tienen su origen en un delito grave...". Cabría asimismo aducir que, en la medida en que Internet es hoy, entre otras muchas cosas, un espacio lúdico utilizado para su esparcimiento de forma habitual por un creciente número de niños, sería posible incriminar, al amparo del art. 186 del Código Penal español a quién "por cualquier medio directo, difundiere, vendiere o exhibiere material pornográfico entre menores de edad o incapaces...".

Pero el recurso a esas normas suscita la inquietud de si se está escanciando el vino nuevo de las más recientes formas de criminalidad informática en los odres viejos de tipos penales pensados para castigar conductas delictivas ajenas al universo tecnológico. Porque a diferencia de los más graves atentados informáticos contra la intimidad, la utilización ilícita de tarjetas electromagnéticas y la estafa o fraude informáticos, que se hallan expresamente previstos en el nuevo Código Penal español (en los arts. 197, 239 y 248.2, respectivamente), parece evidente que nuestro legislador penal no pensaba en Internet al tipificar el delito de receptación o de exhibicionismo y provocación sexual. Por ello, la aplicación de estos tipos puede suscitar serias dudas en orden al respeto del principio de legalidad penal, pero no hacerlo puede provocar situaciones de profunda alarma en la sociedad.

En los últimos años se han producido algunas iniciativas dirigidas a establecer un marco jurídico regulador de los contenidos criminales de Internet. La más importante ha sido la Ley para la Decencia en las Comunicaciones (*Communications Decency Act*) (CDA), aprobada por el Congreso de los Estados Unidos en febrero de 1996. Dicha ley prevé sanciones para quienes almacenen o distribuyan por la red informaciones, imágenes o sonidos que puedan considerase obscenos o indecentes por agredir a la media de los valores morales de la comunidad.

Esta norma ha suscitado una viva polémica entre los juristas y ha sido objeto de diversos recursos. Como resultado de uno de ellos, un Tribunal de Pennsylvania ha declarado la inconstitucionalidad de dicha ley, el 11 de Junio de 1996, por decisión unánime de sus tres jueces. Se considera que la CDA limita injustificadamente el derecho a la libertad de expresión garantizado en la Primera Enmienda de la Constitución norteamericana, ya que al no considerar las informaciones transmitidas por Internet como prensa escrita se las somete a la censura previa por parte de la influyente Comisión Federal de Comunicaciones. Se denuncia también que esta ley lesiona las debidas garantías procesales (*due process of law*) reconocidas por la Quinta Enmienda y, en definitiva, la seguridad jurídica de los ciudadanos por la forma excesivamente vaga e imprecisa con la que se tipifican los supuestos que pueden entrañar atentados contra la decencia. Asimismo se considera que, la legítima protección de los menores, no debiera limitar la libre difusión de informaciones o imágenes normales para adultos, ya que los suministradores de servicios no pueden determinar la edad de los usuarios.

Uno de los jueces del Tribunal que declaró la inconstitucionalidad de la CDA, Stewart R. Dalzell, entendió que Internet implica una garantía para el desarrollo libre y autónomo de las comunicaciones entre los ciudadanos normales frente a la prepotencia de los grandes magnates poseedores de los medios de información. Internet puede considerarse, según este juez, como una "conversación mundial sin fin". Por ello, el Gobierno no puede arbitrariamente interrumpir esta conversación cívica por medio de normas como la CDA. Internet, según el juez Dalzell, por ser la forma más utilizada para un diálogo participativo de masas desarrollada hasta el presente, merece la más eficaz protección jurídica frente a intervenciones restrictivas gubernamentales que no se hallen debidamente justificadas.

Esta sentencia del Tribunal de Distrito de Pennsylvania fue recurrida ante la Supreme Court norteamericana, en el proceso de Janet

Reno, Attorney General of the United States, et al., *versus* American Civil Liberties Union et al., que ha sido resuelto por la sentencia de 26 de Junio de 1997 (nº 96-511), que ha confirmado con el voto unánime del Tribunal la inconstitucionalidad de la CDA. El juez John Paul Stevens, al expresar la opinión mayoritaria del Tribunal, indica que la CDA es abiertamente contraria a la Primera Enmienda y, de forma expresa, considera: "como un aspecto de la tradición constitucional que, en ausencia de evidencia en contrario, se presume que la regulación gubernamental del contenido de las comunicaciones tiende más a interferir el libre intercambio de ideas que a promoverlo. El interés por fomentar la libertad de expresión en una sociedad democrática sobrepasa cualquier teórico e improbable beneficio de la censura". Los jueces Sandra Day O´Connor y William Rhenquist, en un voto particular, mantienen también el carácter inconstitucional de la CDA, excepto en su estricta aplicación a cuanto hace referencia a la comunicación a los menores de informaciones o imágenes indecentes u obscenas (sobre todo ello vid., The Electronic Frontier Foundation, 1997)

8. INICIATIVAS DE LA UNIÓN EUROPEA

En el seno de la Unión Europea se ha elaborado, en octubre de 1996, una Comunicación de la Comisión sobre *Contenidos ilícitos y nocivos en Internet*. Constituye el fin principal de dicho documento el logro de "un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público" entre los Estados miembros de la Unión Europea. Se parte para ello del principio básico de que lo que es ilegal fuera de la red también lo es en ella, por lo que los Estados miembros deben aplicar la legislación existente que pueda sancionar esas conductas ilícitas. No obstante, dada la descentralización y el carácter planetario de Internet, parece necesario establecer medidas en el ámbito de Justicia e Interior para intensificar la cooperación y la respuesta jurídica unitaria frente al reto que representa la criminalidad en Internet. Para ello, la Comisión, en el documento de referencia, insta a incrementar el intercambio de información entre los Estados miembros sobre los suministradores de contenidos delictivos; al tiempo que exhorta a los Estados miembros para que establezcan "criterios europeos mínimos" sobre contenidos criminales en Internet. La comisión reitera su propósito de fomentar los proyectos de autorregulación elaborados por las aso-

ciaciones de suministradores de acceso a Internet, por considerar que el papel de las mismas es de primordial eficacia para limitar la distribución de contenidos ilícitos en la red.

Complementaria, en cuanto a su cronología y alcance, de esa iniciativa se puede considerar el *Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información*, debida también a la Comisión respondiendo a una petición previa del Parlamento Europeo y del Consejo. Si se coteja el *Libro Verde* con la Comunicación se advierte que se trata de un documento, paradójicamente, más genérico y más específico. Más genérico en cuanto a su *ámbito*, ya que no se limita a la regulación de Internet, sino que se ocupa de todos los servicios audiovisuales y de información. Pero, al propio tiempo, se trata de un texto más específico en cuanto a su *objeto*, ya que se circunscribe a la protección de los menores y de la dignidad humana.

El *Libro Verde* recuerda que la protección jurídica de los menores y la dignidad en las normas constitucionales y legislativas de los Estados miembros de la Unión Europea tienen como soporte básico el Convenio Europeo de Derechos Humanos. Dicho Convenio ha sido integrado en el ordenamiento jurídico comunitario por el art. F2 del Tratado de la Unión Europea.

En el Convenio Europeo se reconoce el derecho al respeto de la vida privada y familiar (art.8) y, asimismo, el derecho a la libertad de expresión (art.10). No obstante, ambos derechos no son considerados como absolutos e ilimitados, al estar previsto que pueda condicionarse su ejercicio por medidas necesarias, en una sociedad democrática, para garantizar la seguridad, la salud, la moral o los derechos y libertades de los demás (arts.8.2 y 10.2). Este planteamiento normativo ha sido asumido por la Carta de los Derechos Fundamentales de la Unión Europea proclamada en Niza en diciembre de 2000. En ella se reconocen también el derecho a la vida privada (art.7) y a la libertad de expresión y de información (art.11) de los ciudadanos europeos. Se declara, asimismo, en este texto la prohibición de un ejercicio abusivo de los derechos y libertades allí reconocidos (art.54). Pero, tiene especial interés la alusión expresa en la carta a la protección de los datos de carácter personal. En efecto, se establece en su artículo 8 que: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro

fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedarán sujeto al control de una autoridad independiente". Esta disposición supone una importante garantía para la tutela de la intimidad de los ciudadanos europeos frente a cualquier tipo de ingerencia indebida en esa esfera perpetrada a través de la Red.

La libertad de expresión a través de los servicios audiovisuales y, en consecuencia, de Internet no es ilimitada en el seno de la Unión Europea, si bien, sus limitaciones deben ser admitidas restrictivamente. No en vano la libertad de prestar servicios, también en la esfera de la información y la comunicación, es una de las libertades básicas reconocidas en el Tratado de la Unión. El *Libro Verde* se remite a la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) de Estrasburgo para advertir que la libertad de expresión defiende no sólo las ideas e informaciones que no suponen intromisión u ofensa en los valores o derechos ajenos, sino también las susceptibles de ofender, contradecir o perturbar (STEDH, Handyside/Reino Unido, 1976).

El Libro Verde, acogiendo la jurisprudencia del TEDH (SS, Handyside/Reino Unido, 1976; The Sunday Times/Reino Unido, 1979; Autronic, 1990; Groppera Radio, 1990; Informationsverein Lentia, 1993), propugna que las restricciones a la libertad de expresión fundadas en la defensa de derechos ajenos, en concreto de los de los menores y la dignidad, se halle condicionada a tres exigencias acumulativas:

1) *Prohibición de arbitrariedad*, lo que implica que cada restricción deba estar prevista por la ley;
2) *Necesidad social* imperiosa de garantizar valores y derechos de las sociedades democráticas;
3) *Legitimidad de objetivos*, enumerados de forma limitada y entre los que la defensa de la moralidad y la salud públicas se estiman particularmente adecuados para proteger a los menores y la dignidad humana.

Es fácil inferir los problemas que pueden derivarse de la precisión de lo que, en cada caso, deba considerarse como "necesario" para legitimar una medida legal restrictiva y que persiga un "objetivo legítimo". No basta para ello que tal medida resulte "útil" o "razonable". El carácter legítimo de la medida sólo puede probarse tras un profundo examen de su eficacia en relación con el grado de injeren-

cia que implica. Este análisis constituye una *prueba de proporcionalidad* de las medidas restrictivas. De ello se desprende que no deben imponerse restricciones a la libertad de expresión audiovisual que no estén justificadas en virtud de dicha prueba de proporcionalidad.

El Libro Verde, en definitiva, auspicia una regulación de las redes audiovisuales que tienda a armonizar la libertad de expresión con la defensa de los menores y de la dignidad. Para ello, aboga por el establecimiento de sistemas (por ejemplo, filtros de clasificación de contenidos) que garanticen que los menores no accedan a programas perjudiciales, permitiendo no obstante el acceso de los adultos. Se trata de soluciones procedentes de la base (*bottom up*) más que procedentes desde arriba (*top down*), que permiten obviar la necesidad de censura previa y aumentan la potencial eficacia de la autorregulación.

La Unión Europea ha prestado especial atención a la utilización presente y futura de la Red para facilitar la relación de los ciudadanos con los servicios públicos, así como para el logro de la mayor eficacia en el disfrute de sus derechos. En 1996 la Comisión de la UE encargó a un grupo de expertos la elaboración de un Informe titulado: *Construir la sociedad europea de la información para todos* (cfr. Sánchez Bravo, 2001). El documento más reciente de los impulsados por la Comisión es el titulado *Europa 2005: una sociedad de la información para todos*, que fue presentado en el Consejo Europeo celebrado en Sevilla en junio de 2002.

9. INTERNET Y LAS LIBERTADES EN LA JURISPRUDENCIA EUROPEA: EL "CASO LINDQVIST"

En el ámbito de las decisiones jurisprudenciales europeas sobre la incidencia de Internet en la esfera de las libertades, resulta necesario aludir, por su actualidad e importancia, a la Sentencia del Tribunal de Justicia de la UE de 6 de noviembre de 2003 (asunto C-101/01). Dicha sentencia tiene por objeto una petición dirigida al Tribunal de Justicia, con arreglo al artículo 234 CE, por el Góta hovrátt de Suecia, destinada a obtener, en el proceso penal seguido ante dicho órgano jurisdiccional contra Bodil Lindqvist, una decisión prejudicial sobre la interpretación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos .

Bodil Lindqvist, además de su trabajo retribuido como empleada de mantenimiento, desempeñaba funciones de catequista en la parroquia de Alseda (Suecia). Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página web en Internet. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran. A petición suya, el administrador del servidor Internet de la Iglesia de Suecia creó un enlace entre las citadas páginas y dicho centro servidor.

Las páginas web de que se trata contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, sólo su nombre de pila. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Asimismo, señaló que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad La Sra. Lndqvist no había informado a sus compañeros de la existencia de estas páginas web, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion (organismo público sueco para la protección datos personales). En cuanto supo que algunos de sus compañeros no apreciaban las páginas web controvertidas, las suprimió. El ministerio fiscal inició un proceso penal contra la Sra. Lindqvist por infracción de la legislación sueca de protección de datos personales (Personuppgiftslag, de 1998, en adelante PUL), y solicitó que fuese condenada por:

1) haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la Datainspektion (artículo 36 de la PUL);
2) haber tratado sin autorización datos personales sensibles, como los relativos a la lesión en un pie y a la baja parcial por enfermedad (artículo 13 de la PUL);
3) haber transferido datos de carácter personal a países terceros sin autorización (artículo 33 de la PUL).

La Sra. Lindqvist reconoció los hechos, pero negó que hubiera cometido una infracción. El Eksjó tingsrátt (Suecia) la condenó al pago de una multa; la Sra. Lindqvist recurrió en apelación esta resolución ante el órgano jurisdiccional remitente.

El Tribunal de Justicia de la UE, pronunciándose sobre las cuestiones planteadas por el Góta hovrátt mediante resolución de 23 de febrero de 2001, he declarado:

1) Que la conducta referente a elaborar informaciones sobre personas, en una página web, que permiten su identificación por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE.
2) Que un tratamiento de datos personales de esta naturaleza no está comprendido en ninguna de las excepciones que figuran en el artículo 3 apartado 2, de dicha Directiva.
3) Que la indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud en el sentido del artículo 8, apartado 1, de la Directiva 95/46.
4) Que no existe una «transferencia a un país tercero de datos» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el servidor de **Internet** en el que se puede consultar la página web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros.
5) Que las disposiciones de la Directiva 95/46 no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950. Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario.
6) Que las medidas adoptadas por los Estados miembros para garantizar la protección de los datos personales deben ate-

nerse tanto a las disposiciones de la Directiva 95/46 como a su objetivo, que consiste en mantener el equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad. En cambio, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a lo dispuesto en la Directiva 95/46 a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello.

Esta decisión del Tribunal de Justicia de la UE, muestra la incidencia creciente de Internet en la esfera de las libertades. De dicha sentencia, estimo, que pueden inferirse tres consecuencias básicas:

1ª) En el "caso Lindqvist" se advierte, con meridiana claridad, la ambivalencia del fenómeno Internet desde el punto de vista del desarrollo y la tutela de los derechos fundamentales. En su polaridad positiva, Internet supone un vehículo potenciador de las libertades de expresión y comunicación de datos e ideas, que se consideran derechos irrenunciables de las sociedades políticas democráticas contemporáneas y, en concreto, de la UE. Pero, en su polo negativo, se vislumbran riesgos inquietantes en relación con usos abusivos de Internet que directamente menoscaban el ámbito íntimo de los ciudadanos. En el caso de referencia el Tribunal de la UE, consciente de esa ambivalencia, ha optado por una actitud de equilibrio es decir, por una ponderación de bienes (*Güterabwägung*, cfr.,Pérez Luño, 2003, 302 ss.). A través de esa actitud mediadora, pretende compatibilizar el disfrute del derecho a la intimidad con el ejercicio de la libertad de expresión en el uso de la red en el espacio europeo.

2ª) Respecto a los riesgos de Internet, la sentencia del 6 de noviembre de 2003, supone una garantía contra cualquier elaboración de páginas web en Internet, en las que se incluyan datos personales, especialmente informaciones sensibles, sin que se cumplan los requisitos establecidos en la Directiva 95/46, así como en las legislaciones de los Estados miembros de la UE que la han adaptado a su orden jurídico interno. Que tales garantías no suponen

3ª) Se desprende, asimismo, de esta sentencia, que la tutela de la intimidad en Internet no debe extenderse más de lo estrictamente necesario, de modo que interfiera en el ejercicio, a tra-

vés de la red, de las libertades de información, expresión y comunicación. Por ello, el mero hecho de incluir en una página web datos personales, aunque se hayan elaborado sin cobertura legal, no supone incurrir en el supuesto de transmisión ilícita de datos y en la consiguiente vulneración de cuanto dispone el artículo 25 de la Directiva 95/46. Para que se produzca dicho supuesto ilícito será necesario que concurra una acción directa y deliberada de envío de datos. De este modo, el Tribunal de Justicia de la UE corrige la interpretación del órgano jurisdiccional sueco, a tenor de la cual se llegaba a la conclusión desorbitada de que cualquier introducción de datos en la red implica la transmisión o transferencia de los mismos.

10. INTERNET Y LOS DERECHOS CÍVICOS: LA "CIBERCIUDADANÍA"

Uno de los aspectos más actuales del debate sobre la incidencia de Internet en el ejercicio de las libertades es el referente a su impacto en el ámbito de la ciudadanía. En esta esfera se contraponen abiertamente los enfoques de quienes recelan de la Red, al ver en ella un riesgo de despolitización y consiguiente debilitamiento del status de ciudadanía activa en las sociedades democráticas; y la postura opuesta que confía en el reforzamiento de la vida cívica a través de su ejercicio por los nuevos cauces que dimanan de Internet.

Entre las posturas críticas, resulta especialmente representativa la actitud del constitucionalista norteamericano Cass Sunstein. En su estimulante libro *Republic.com*, no vacila en reconocer las posibilidades para una renovación política de la vida democrática, cimentadas por la inmensa capacidad informativa y comunicativa que entraña Internet. Pero su sugerente análisis plantea algunos reparos de fondo de incuestionable calado. Entiende Sunstein que la Red propicia un tipo de información y comunicación política individualizada y personalizada. Cada usuario se construye su propio "menú" de datos y documentación política. Ello puede conducir a una fragmentación, que dificulte la existencia de opciones y programas políticos colectivos y puede menoscabar la vertebración y la cohesión estructural de la experiencia democrática republicana (Sunstein, 2001, 2 ss. y 13 ss.).

Sunstein entiende que la Red ha generado un tipo de usuario-consumidor, ha creado, por tanto, unos hábitos de uso que pueden

extrapolarse a todos los ámbitos de su empleo. La búsqueda del provecho individual, que es inherente a todas las transacciones comerciales en la Red, puede proyectarse a las actividades políticas. De este modo, el usuario que, en su condición de ciudadano, debe asumir puntos de vista solidarios, que trascienden a su mero interés individual, puede verse fagocitado por el usuario-consumidor, que proyecta en todas sus actividades en la Red la obtención de beneficios inspirados en el egoísmo: los valores de la democracia republicana se ven suplantados por la "lógica económica del mercado" (Sunstein, 2001, 105 ss.).

Cass Sunstein, insiste en denunciar el riesgo de transmutación del ciudadano en consumidor, como consecuencia negativa del ejercicio de la ciudadanía en la Red. Cabría, por tanto, inferir del planteamiento de Sunstein, que a esa *República.com* le correspondería una *ciudadanía.com*; cuyos titulares habrían abdicado de su condición de sujetos políticos activos y quedarían degradados a la condición de meros consumidores pasivos de los programas producidos por los grandes poderes económicos.

La visión optimista respecto al reforzamiento de los derechos cívicos a través de Internet, se ha tematizado bajo la rúbrica de la "ciberciudadanía". Entre las experiencias más estimulantes para la afirmación de la polaridad positiva de la Red, se inscribe el *Manifiesto por el ejercicio de una ciberciudadanía activa, responsable y comprometida*. Dicha declaración fue elaborada por el 1er Congreso ONLINE del Observatorio para la Ciber-Sociedad, celebrado en septiembre de 2002, donde fue aprobada mayoritariamente y en todos sus puntos. El Congreso reunió a 700 cibernautas de todo el mundo. El Manifiesto cuenta con algunas iniciativas precedentes. Entre ellas, puede citarse la *Declaración de Independencia del Ciberespacio* "promulgada" por John Perry Barlow, a la que se ha tenido ocasión de aludir *supra*.

Los autores del Manifiesto elaborado por el Observatorio para la Ciber-Sociedad, entienden que: "el acceso a la cultura, el conocimiento y la información nunca estuvo tan al alcance de la humanidad como ahora. La invención y popularización de las Tecnologías de la Información y la Comunicación (TIC) tiene gran parte de responsabilidad sobre este hecho que supone un cambio cualitativo radical en lo que a esta posibilidad de acceso se refiere". El propósito principal de dicha Declaración se cifra en reivindicar el ejercicio de una ciudadanía electrónica o *ciberciudadanía*, "responsable y éticamente com-

prometida con una utilización de las TIC que trabaje para la consecución de una sociedad más solidaria, justa, libre y democrática". Esa ciudadanía debe estar cimentada en el "derecho universal de acceso al ciberespacio y a su defensa y conservación como un ámbito social libre e igualitario un derecho que debe estar por encima de monopolios estatales, oligárquicos o empresariales".

Para la consecución de ese objetivo se establecen ocho puntos que, en una referencia compendiada, pueden englobarse en torno a tres postulados guía:

1º) Proclamación de la *libertad e igualdad del ciberespacio*. Se propugna una apuesta decidida de los gobiernos y los organismos internacionales para el progresivo establecimiento de las infraestructuras y medidas necesarias que brinden a todo ser humano la posibilidad de ejercer su ciberciudadanía, con lo que se vaya reduciendo primero y erradicando después, la fractura digital" (punto 1). Asimismo, se auspicia la creación de un marco legal que permita la libertad de servicios en el ciberespacio sin barreras ni proteccionismos, que perjudiquen a persona o sociedad alguna (punto 2). Se defienden las ventajas derivadas de "utilizar soluciones tecnológicas de código libre en las administraciones públicas y su implantación, siempre que sea viable, en detrimento de herramientas de tipo comercial, privado o cerrado" (punto 4). Se propugna, además, una política tendente a velar por la libre y fluida difusión de la información y el conocimiento en formatos tecnológicos públicos, que permitan que estos recursos sean fácilmente localizables y utilizables (punto 6).

2º) Fortalecimiento de la *cultura cívica*. Los propulsores de la ciberciudadanía vinculan su plena eficacia a la elaboración, y realización de programas educativos a todos los niveles, también de cultura cívica, que propicien la utilización de las TIC y que "permitan que su utilización y provecho no quede limitado a los grupos social y económicamente privilegiados" (punto 5).

3º) Estrategias de *tutela* de la ciberciudadanía. Los autores del Manifiesto abogan por la implantación de organizaciones que protejan jurídicamente la ciberciudadanía contra las prácticas abusivas de gobiernos o empresas que afecten aspectos de fondo, forma, cualitativos o cuantitativos de sus derechos (punto 3). Se proponen también: "la denuncia de

incumplimiento de los puntos contenidos en este manifiesto con especial referencia de las consecuencias sociales a las que dicho incumplimiento nos lleva. Convirtiéndonos, de facto, en una voz firme que remueva las conciencias de las personas y de las administraciones públicas" (punto 7). Por último, los signatarios de la declaración, concientes de la facilidad de hacer público todo tipo de información a través de la Red, se comprometen a promover la elaboración y defensa de los contenidos que puedan servir de guía, referencia o información para reforzar la ciberciudadanía; desde un ejercicio de responsabilidad ética, que tome en consideración las posibles consecuencias de la información publicada. Entienden quienes han formulado el manifiesto que: "ya no es posible seguir poniéndole vallas al mundo, ni fronteras, ni aduanas, ni peajes monopolísticos u oligárquicos. Porque estas vallas, fronteras, aduanas y peajes son testigos de un mundo caduco e injusto al que debemos renunciar para que la Humanidad sobreviva y porque creemos que el ciberespacio es el primer lugar donde esos obstáculos pueden ser, efectivamente, salvados" (punto 8).

La contribución de Internet a forjar una ciberciudadanía, como forma de ciudadanía internacional y cosmopolita, se ha visto confirmada por determinados fenómenos recientes. La actitud solidaria puesta de manifiesto en la concienciación y protesta de miles de cibernautas contra la pena de lapidación impuesta a mujeres nigerianas, acusadas de supuestos adulterios; la difusión de una conciencia crítica planetaria sobre los riesgos de la globalización; la protesta respecto a la intervención bélica, al margen de la ONU en Irak... representan experiencias elocuentes de la conformación de ese universo ciberciudadano. Por ello, se ha indicado que preguntarse sobre si Internet es buena o mala para la democracia, "parece casi ridículo" (Vallespín, 2003, 12).

11. EL IMPACTO DE INTERNET EN LAS LIBERTADES: NI APOCALÍPTICOS, NI INTEGRADOS.

La alternativa entre la dimensión "buena", que representa la ciberciudadanía y la "mala" evocada por la ciudadanía.com, suscita un debate que puede ser ilustrado tomando en préstamo una certera caracterización general sobre las actitudes en relación con el progreso

tecnológico. *Apocalittici e integrati* es el título de una conocida obra de Umberto Eco en la que se definen estas dos actitudes básicas frente a la cultura de masas y a la sociedad tecnológica. Así, mientras que "el Apocalipsis es una obsesión del *dissenter*, la integración es la realidad concreta de aquellos que no disienten" (Eco, 1982, 4). Los *apocalípticos* tienen el mérito de captar y denunciar los impactos perversos de determinados usos de las NT. Es esta una actitud que peca de unilateralidad, porque entraña una postura obcecadamente ciega ante los avances y virtualidades del progreso. Su divisa se compendia en el tópico alarmista del: "¿a dónde vamos a llegar?" No es menos insatisfactoria y unilateral la actitud de los *integrados*, de esos espíritus ingenuos que adoran lo nuevo por el sólo hecho de ser nuevo. Esta posición acrítica representa una claudicación servil ante los riesgos implícitos en determinados abusos de las NT y puede tener peligrosas consecuencias.

Como manifestaciones contemporáneas del pensamiento apocalíptico habría que situar, sin duda, las reflexiones de George Orwell, contenidas en su célebre *1984*. El Gran Hermano representa la imagen anti-utópica de todos los peligros contra la democracia y las libertades, que subyacen a una utilización perversa de la tecnología en el ámbito político; aunque con la salvedad, de que su disentimiento no pretende tanto atacar el desarrollo tecnológico como advertir de las amenazas de su utilización por gobiernos totalitarios (Orwell, 1980; cfr. sobre la anti-utopía de Orwell, Pérez Luño, 1987, 132 ss.). Mucho más apocalíptica que la actitud de Orwell resulta una reflexión de Robert Musil incluida en una de sus más conocidas obras, que implica una visión plenamente pesimista del progreso tecnológico. "La matemática –escribe–, madre de las ciencias exactas, abuela de la técnica, es también el antecedente de aquel espíritu del que finalmente surgieron el gas venenoso y los aviones de combate" (Musil, 1953, 40). Se han hecho también célebres, en una etapa más reciente, las implacables críticas de Herbert Marcuse a la sociedad tecnológicamente avanzada, en la que el progreso técnico se ha convertido en un dogma. En dicha sociedad, la cultura, la política y la economía se hallan integradas en un sistema de dominación omnipotente que no tolera ninguna alternativa y que absorbe cualquier actitud de oposición (Marcuse, 1964, 3).

En el polo opuesto de *esta* actitud se hallan los integrados, es decir, aquellos que se sienten satisfechos y consideran normal que en la actualidad ya no exista ningún ámbito de la vida pública y privada,

individual o social que no esté condicionado directa o indirectamente por la técnica. Para designar a estos sujetos Henri Lefèbvre ha propuesto el término de *cybernanthrope*. El "hombre-cibernético" vive en simbiosis con la máquina. En ella encuentra su doble real. El *cybernanthrope* se define a sí mismo como un organismo complejo que obedece a leyes simples (menor actividad, economía...) y dispone de un sistema integrado de sistemas parciales autorreguladores que conforman un hermoso conjunto (el sistema nervioso, el sistema óseo, el sistema glandular...). El "hombre cibernético" acepta gustoso una vida cotidiana llena de aparatos técnicos, cuyo funcionamiento muchas veces ni siquiera entiende y no se plantea sus repercusiones. Para Lefèbvre, el *cibernenthrope* rechaza toda posibilidad que no sea su propia confirmación y consolidación: su equilibrio. Es un hombre establecido, funcionalizado, institucionalizado, estructurado: ya ha dejado de ser un hombre (Lefèbvre, 1971, 36 ss.).

Es evidente que desde los enfoques apocalípticos o integrados es imposible captar la radical ambivalencia del fenómeno tecnológico y, por tanto, aprovechar a través de una reglamentación jurídica adecuada sus aspectos positivos y evitar, a través de las oportunas garantías jurídicas, sus amenazas (cfr. Rapp, 1981, 175 ss.). Por ello, si no se quiere incidir en planteamientos simplistas o lamentaciones pesimistas sobre el poder de la Red, es preciso reconocer que a lo largo del proceso evolutivo de la humanidad el desarrollo científico y técnico no ha sido sino la respuesta histórica a los sucesivos problemas propios de cada época y contexto. Por tanto, la tecnología actual no es más que el esfuerzo de la ciencia y de la técnica por responder, no siempre adecuadamente eso es cierto, a las cuestiones surgidas de las nuevas formas de convivencia y de la ampliación incesante de las aspiraciones y necesidades sociales. Quizás exista un olvido cuando se impugna, con razón, la abusiva omnipresencia de los sistemas informativos y de control social, que hoy se hallan lo mismo en manos del Estado, que en las de las grandes empresas, que ha sido el propio progreso técnico quien los ha hecho imprescindibles. Nadie puede negar que una gestión eficaz del aparato administrativo estatal hace necesario el empleo de la tecnología. La complejidad de la vida moderna, las inmensas posibilidades que en las grandes sociedades de nuestro tiempo se ofrecen para dejar en el anonimato o en la impunidad conductas antisociales o delictivas exigen la puesta en funcionamiento de medios de información y control. Pero estas observaciones no pretenden conducir a la falsa disyuntiva de que o se deja inerme al

Estado y la sociedad, o los ciudadanos deben aceptar la existencia de un colosal aparato informativo y de control que haga que nadie sepa con certeza lo que los demás saben de él, quién puede utilizar esas informaciones y con qué finalidad va a hacerlo. Frente a esa opción equívoca, la alternativa razonable no puede ser otra que la de una organización política y una disciplina jurídica eficaz y democrática de los medios tecnológicos de información y control; de forma que las NT lejos de actuar como medio opresivo, se conviertan en vehículo para una convivencia política en la que el progreso no se consiga al precio de la libertad y de la justicia: se trata, en suma, de dar respuesta al viejo problema del *quis custodiet ipsos custodes?*

Esta exigencia ha hallado certera expresión en Ernesto Garzón Valdés, cuando advierte que: "El control de los expertos es uno de los problemas de la democracia actual: eliminarlos sería científica y técnicamente suicida; dejarlos librados a su arbitrio personal significaría renunciar a uno de los pilares de la decisión democrática" (Garzón Valdés, 2003a, 32). Urge, por ello, evitar que la consideración jurídica y política de Internet degenere en pura meditación utópica o en una apología de la claudicación conformista ante el hecho consumado de la tecnología. Frente a cualquier tipo de planteamiento maniqueo o unilateral debe propiciarse el juicio crítico y la reflexión totalizadora e interdisciplinar entre el mundo de las NT y el mundo de los ciudadanos. La Red, en definitiva, puede ser el principal cauce para promover una participación política más auténtica, plena y efectiva en las democracias del siglo XXI, en términos de ciberciudadanía; o para degenerar en un fenómeno de colonización y control de la vida cívica, quedando degradada en versiones indeseables de ciudadanía.com.

12. HACIA UNA ÉTICA JURÍDICA CIBERESPACIAL

No es este el lugar para una consideración detenida en pormenores sobre las múltiples implicaciones económicas, culturales, sociales y políticas que se derivan de ese ciberespacio cuya navegación y conquista ha hecho posible Internet. Las consecuencias que pueden derivarse de esa forma de comunicación humana en soporte informático son imprevisibles y, a veces, paradójicas. Puede darse la circunstancia de que el máximo desarrollo de la comunicación tecnológica implique simultáneamente un empobrecimiento de las formas de comunicación tradicionales. Suele aducirse, para corroborar esos

riesgos, la anécdota de un foro de "cibernautas" que concertaron un encuentro personal para reforzar sus contactos iniciados a través de Internet. La reunión fue un completo fracaso por las dificultades para establecer un diálogo interpersonal; la comunicación sólo se hizo de nuevo fluida cuando cada uno de los cibernautas la reemprendió desde su pantalla de ordenador.

No obstante, esta reflexión pecaría de un exceso de pesimismo si no reconociese las posibilidades de una renovación de los valores cívicos que puede promover Internet. En el área francófona se ha utilizado la expresión "*Netiquette*", es decir, "ética de la *Net* (red)", para aludir a las reglas deontológicas que deben presidir la utilización de Internet. Se trata de normas o programas éticos dirigidos a evitar las conductas perturbadoras realizadas por los cibernautas y para prevenir cualquier actividad que perjudique el normal funcionamiento de la red (Piette-Coudol y Bertrand, 1997).

Las redes de telecomunicaciones pueden conducir a una nueva ética "ciberespacial", que genere y estimule actitudes de conciencia colectiva sobre el respeto de las libertades y de los bienes amenazados por una utilización indebida del ciberespacio, y contribuir a la formación de vínculos solidarios para la prevención de los crímenes informáticos y la ayuda a su descubrimiento. La difusión capilar de las redes comunicativas puede conducir a la producción de reglas jurídicas consuetudinarias sobre su uso, en las que la dimensión coactiva de las normas basada en la autoridad de un poder centralizado, deje paso a códigos de conducta cuya eficacia se base en la convicción de los usuarios y en su responsabilidad solidaria (Colom y Van Bolhuis,1995; Forester, y Morrison, 1990).

Ha recordado oportunamente Cass Sunstein que los redactores de la Constitución norteamericana se reunieron a puerta cerrada en Filadelfia, en el verano de 1787. Cuando concluyeron su trabajo, el pueblo congregado ante la sede de la Sala de Convenciones, se hallaba expectante e impaciente. Cuando Benjamin Franklin salió del edificio, alguien le preguntó: "¿Qué vais a darnos?" La respuesta de Franklin fue, a un tiempo, esperanzadora y desafiante: "Una república, si sabéis conservarla" (Sunstein, 2001, 105).

Este episodio es del todo pertinente para ilustrar el debate sobre la incidencia de la Red en las libertades. El comentario de Franklin nos invita a considerar que las NT constituyen un inmenso cauce de desarrollo de la condición humana, en todas sus esferas. Pero, supone también la aparición de riesgos y amenazas para la libertad más

implacables que los sufridos e imaginados en cualquier periodo anterior de la historia. Que Internet contribuya a lo primero o a lo segundo, es algo que no depende del azar, la fatalidad o de fuerzas y poderes esotéricos. La decisión sobre los impactos presentes y futuros de Internet en la esfera de las libertades, corresponde a los ciudadanos de las sociedades democráticas: se trata de una responsabilidad de la que no deben abdicar.

REFERENCIAS BIBLIOGRÁFICAS

BARLOW, J. P. "Declaración de Independencia del Ciberespacio", en [Internet: *Cibernautas por la Tolerancia*, 1996; http://www.ctv.es/ USERS/mrb/tolerancia/].

BENSOUSSAN, A. (ed.) *Internet: aspects juridiques* , Hermes, Paris, 1996.

BRANSCOMB, A.W. "Anonimity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace", en *Yale Law Journal*, n.104, 1995, pp. 1639 ss.

BUSTOS, M. "Detectives en el Ciberespacio", en, *El País* ("Especial Simo"), 5, noviembre, 1996.

BYASSEE, W.S. "Jurisdiction of Cyberspace", en *Wake Forest Law Review*, n. 30, 1995, pp. 197 ss.

CASTILLO JIMÉNEZ, C. *Las Nuevas Tecnologías de la Información y el Derecho. De Vittorio Frosini a Internet*, Instituto de Estadística de Andalucía, Sevilla, 2003. [Con prologo de A.E.Pérez Luño].

CAVAZOS, E.A.; MORIN, G. *Cyberspace and the Law*, MIT Press, Cambridge (Mass.), 1994.

CIAMPI, C. "Una guida per giuristi nel ciberspazio di Internet: strumenti per la navigazionee prospettive di sviluppo", en *Atti del Congresso Annuale AIC A*, Chia-Cagliari, vol.I, 1995, pp. 543-550.

CIAMPI, C. [Internet: *Guida all´informazione giuridica nel ciberspazio*; http://www.idg.fi.cnr.it/ita/informazione/guida/cs_guide.htm; 1996].

COLOM, V.; VAN BOLHUIS, H. E. *Cyberspace Reflections*, Brussels, European Commission, 1995.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión de las Comunidades Europeas *Contenidos ilícitos y nocivos en Internet*, Documento COM (96)" 487 final, 1996.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión de las Comunidades Europeas *Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información*, Documento COM (96)" 483 final, 1996.

CUTRERA, T. "The Constitution in Cyberspace: the Fundamental Rights of Computers Users", en *University of Missouri Law Review*, n. 60, 1991, pp. 139 ss.

ECO, U. *Apocalittici e integrati*, 3a ed, Milano, Bompiani, 1982.

FERNÁNDEZ CALVO, R. "El Ciberespacio y sus dilemas" en *El País* ("Especial Simo"), 5, noviembre, 1996.
FERNÁNDEZ HERMANA, L.A. *En red ando*, Barcelona, Ediciones B, 1998.
FERNÁNDEZ RODRÍGUEZ, J. *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red*, México, UNAM, 2004.
FERNÁNDEZ SALMERÓN, M. *La protección de los datos personales en las Administraciones Públicas*, Madrid, Thomson & Civitas, 2003.
FORESTER, T.; MORRISON, P. *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*, Cambridge (Mass.), MIT Press, 1990.
FROSINI, V. *Law and Liberty in the Computer Age*, Oslo, Tano, 1995.
FROSINI, V. *La democrazia nel XXI secolo*, Roma, Ideazione, 1997.
FROSINI, V. *L´uomo artificiale. Etica e diritto nell´era planetaria* , Milano, Spirali, 1986.
GARCÍA-BERRIO, T. *Informática y libertades. La protección de datos personales y su regulación en Francia y España*, Murcia, Servicio de Publicaciones de la Universidad de Murcia, 2003.
GARRIGA DOMÍNGUEZ, A. *La protección de los datos personales en el Derecho español*, Madrid, Universidad Carlos III & Dykinson, 1999. [Con Prólogo de A. E. Pérez Luño].
GARRIGA DOMÍNGUEZ, A. *Tratamiento de datos personales y derechos fundamentales*, Madrid, Dykinson, 2004.
GARZÓN VALDÉS, E. "Optimismo y pesimismo en la democracia" en *Claves de Razón práctica*, n. 131, 2003a.
GARZÓN VALDÉS, E. "Lo íntimo, lo privado y lo público" en *Claves de Razón práctica*, n. 137, 2003b.
GONZÁLEZ DE LA GARZA, L. *Comunicación pública en Interntet*. Madrid, Creaciones Copyright, 2004.
HANCE, O. *Leyes y negocios en Internet*, México, MacGraw-Hill, 1996.[Trad., de Y. Juárez].
Internet desde la perspectiva jurídica, en *Manual práctico de Internet*, nº 13, 19, Febrero, 1997. [Col. "Cuadernos de Cinco Días"].
ITEANU, O. *Internet et le Droit*, Paris, Eyrolles, 1996.
La explosión Internet, en *Dossier de Muy Especial*, nº 28, 1997.
LAGARES, D. *Internet y el Derecho*, 2ª ed, Barcelona, Carena, 2000.
LEFEBVRE, E. *Vers le cybernanthrope*, París, Denoël & Gonthier, 1971.
LOSANO, M. G. *Corso di informatica giuridica*, vol. I, *Informatica per le scienze sociali*, Torino, Einaudi, 1985.
LOSANO, M. G. *Corso di informatica giuridica*, vol. II.1, *Il diritto privatto dell´informatica*, Torino, Einaudi, 1986a.
LOSANO, M. G. *Corso di informatica giuridica*, vol. II.2, *Il diritto pubblico dell´informatica*, Torino, Einaudi, 1986b.
LOSANO, M.G, (1987): "Los Proyectos de Ley italianos sobre la protección de los datos personales", PÉREZ LUÑO, A (ed). E. Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986,

Problemas actuales de la documentación y la informática jurídica, Madrid, Tecnos & Fundación Cultural, 1987.

LOSANO, M. G, "Il Trattato di Schengen e le frontiere europee" en *Data Manager*, n. 114, 1991.

LOSANO, M.G, "Para una teoría general de las leyes sobre la protección de los datos personales", en *Implicaciones socio-jurídicas de las tecnologías de la información. Encuentro 1991*, Madrid, Fundación Citema, 1992.

LOSANO, M. G, "La legge espanogla sulla protezione dei dati personali", en *Il Diritto dell´Informazione e dell´Informatica*, n. 4/5, 1993, pp 867-892.

LOSANO, M. G. "Europa y América Latina. El "viejo Occidente" y el "otro Occidente", en Actas del Coloquio Internacional Humboldt celebrado en Montevideo en Abril de 2003,*El Derecho ante la globalización y el terrorismo*, Valencia, Tirant lo Blanch, 2004.

MARCUSE, H. *One-Dimensional Man. Studies in the Ideology of Avanced Industrial Society*, London, Routledge & Kegan, 1964.

MORENO, M. A. "¿Es segura la Internet?" en *Base Informática*, n. 27, 1995, pp.60-65.

MUSIL, R. *Der Mann ohne Eigenschaften*, Hamburg, Rowohlt, 1952.

OROZCO PARDO, G. "La protección de datos en Derecho español a la luz de la reciente jurisprudencia constitucional", en *Actualidad Civil*, n. 6, 2002, pp. 173-237.

Observatorio para la CiberSociedad *Manifiesto por el ejercicio de una ciberciudadanía activa, responsable y comprometida*, en [Internet: http://cibersociedad.rediris; 2002].

ORTEGA Y GASSET, J. *Meditación de la técnica*, V. 5, Madrid, Alianza Editorial & Revista de Occidente, 1983. [Col. Obras Completas, 1939].

ORTEGA Y GASSET, J. *Prólogo a un Diccionario enciclopédico abreviado*, V. 6, Madrid, Alianza Editorial & Revista de Occidente, 1983. [Col. Obras Completas, 1939]..

ORWELL, G. *1984*, 5ª ed, Destino, Barcelona, Destino, 1980.

PASCUZZI, G. *Cyberdiritto*, Bologna, Zanichelli, 1995.

PÉREZ LUÑO, A.E. *Nuevas tecnologías, sociedad y Derecho. El impacto socio-jurídico de las N.T. de la información*, Madrid, Fundesco, 1987.

PÉREZ LUÑO, A.E. *La seguridad jurídica*, 2ª ed, Barcelona, Ariel, 1994.

PÉREZ LUÑO, A.E. *Manual de Informática y Derecho*, Barcelona, Ariel, 1996.

PÉREZ LUÑO, A.E. "Internet navegaciones y abordajes", en *La Ley* (*Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía*), nº 4258, 1997, pp. 1 y 14-15.

PÉREZ LUÑO, A.E. "Internet e il diritto", en PÉREZ LUÑO, A.E. *Saggi di informtica giuridica*, Milano, Giuffrè, 1998. [con prólogo de V. Frosini]

PÉREZ LUÑO, A.E. *¿Ciberciudadanía o ciudadanía .com?*, Barcelona, Gedisa, 2004.

PIETTE-COUDOL, T.; BERTRAND, A. *Internet et la loi*, Paris, Dalloz, 1997.

RAMONET, I. "¡Nos han robado una esperanza!". "Internet, ¿un bien o una maldición?" en *El País Digital-Debates*, 25 de Febrero de 1997.

RAPP, F. *Filosofía analítica de la ciencia*, Barcelona, Alfa & Laia, 1981. [Trad., de E. Garzón Valdés].
RHEINHOLD, H. *La comunidad virtual*, Barcelona, Gedisa, 1996. [Trad., de J.A. Alvarez].
RIBAS, J. "Aspectos legislativos de las autopistas de la información: Delitos en Internet", en *Jornadas Profesionales Informat- 96*, Barcelona, Octubre, 1996.
RICO, I. "Navegar por Internet" en, *Ideas-IBM* n. 15, 1995.
ROCHA, M.L.; MACEDO, M. *Direito no ciberespaço*, Lisboa, Cosmos, 1996.
SÁNCHEZ BRAVO. A. *La protección del derecho a la libertad informática en la Unión Europea*, Sevilla, Publicaciones de la Universidad de Sevilla, 1998. [Con Prólogo de A.E. Pérez Luño].
SÁNCHEZ BRAVO, A. (2001): *Internet y la sociedad europea de la información: implicaciones para los ciudadanos*, Sevilla, Publicaciones de la Universidad de Sevilla, 2001. [Con Prólogo de A.E. Pérez Luño].
SÁNCHEZ BRAVO, A. "El control de la Red: Echelon y Carnivore", en *La Ley*, nº 5686, de 30 de diciembre de 2002.
SARTORI, G. *Homo videns. La sociedad teledirigida*, Madrid, Taurus, 1998.
SCIUTO, P. "Internet e diritto romano", en *Informatica e diritto*, n.1, 1997.
STUCKEY, K. "Business and Legal Aspects of the Internet and online Services: Rights and Responsabilities of Information Service Provider", en *The Data Law Report*, vol, 2, n. 4 y 5, 1995.
SUNSTEIN, C. *Republic.com*, Cambridge, Princeton University Press, 2001. [Existe trad. cast., de P. García Segura, Barcelona, Paidós, 2003]).
TERCEIRO, J.B. *Socied@d digit@l. Del homo sapiens al homo digitalis*, Madrid, Alianza Editorial, 1996.
The Electronic Frontier Foundation, *Free Speech On-Line Blue Ribbon Campaign*, en [Internet: http://www. eff. org/; 1997].
VALLESPÍN, F. "Democracia e Internet", en *El País*, 12 de abril de 2003.