http://dx.doi.org/10.12795/Ambitos.2000.i05.07
ÁMBITOS. Nº 5. 2º Semestre de 2000 (pp. 143-155)

La Red: el nuevo mercado de la vida privada

María Teresa Sandoval Martín
Profesora de la Unicarsidad Carlos III (Madrid)
mtsando@ull.es

RESUMEN

Mientras el mercado publicitario en Internet demanda cada vez más información de los ciberusuarios, diferentes organizaciones y determinados gobiernos defienden el respeto a la intimidad y a la privacidad en el nuevo entorno tecnológico. Algunos de estos países proponen leyes y otros prefieren la autorregulación, pero, a la vez, también se van incrementando las medidas y los sistemas de vigilancia con el supuesto fin de proteger a la sociedad. Además de la regulación, las normas o el desarrollo de códigos por las empresas, el mercado e incluso la propia tecnología pueden limitar la información que se toma de los navegantes de la red de redes. La mayoría de los especialistas consideran que en un futuro próximo los internautas deseos de discreción pagarán un precio por la seguridad de sus datos, mientras que los otros verán su intimidad ofrecida como mercancía.

ABSTRACT

While market in Internet demands more and more information about users, different organizations and certain governments defend the respect to the intimacy and the privacy in the new technological environment. Some of these countries propose laws and others lean for a self-regulation. At the same time, they also leave increasing the measures and systems of surveillance with the supposed end of protecting to society. Besides the regulation, the rules or the development of codes for the companies, the market and the own technology can even limit the information of users in the net. Most of the specialists consider that in a next future, some of the users will pay a price for the security of their data, while the other ones will see their intimacy offered as a merchandise.

Palabras claves: Internet/Regulación/Privacidad/Intimidad/Usuarios.

Key Words: Internet/Regulation/Pryvacy/Intimacy/Users.

Introducción

A mediados de agosto de 1998, la Comisión Federal de Comercio norteamericana acusó a una compañía instalada en Internet, Geocities, de haber divulgado informaciones sobre sus clientes, sin haber obtenido previamente su permiso. Estas informaciones vendidas sucesivamente a otras empresas, desarrollan un mercado en Internet alrededor de la vida privada

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

de los individuos. Esto hace que desaparezca la posibilidad de ser un navegante anónimo, uno de los atractivos que ha presentado la red desde sus comienzos. Ésta y otras muchas actuaciones similares, que atentan contra uno de los derechos fundamentales del hombre, el derecho a la privacidad, preocupan a numerosas comunidades y organizaciones que actúan entre el individuo, la sociedad y las nuevas tecnologías, en ese complejo y cambiante Tercer Entorno donde habitan los señores del aire de la Telépolis de Javier Echeverría[1]. Mientras, en el lado contrario, en los países del Primer Mundo, sobre todo en el continente africano, se considera a algunos sectores de Internet como una herramienta potencialmente liberadora. Esto se debe a que ambos factores están íntimamente relacionados: a mayor libertad de actuación mayor probabilidad de ser supervisados por los demás.

El respeto a la intimidad y a la privacidad, el derecho al anonimato y a la diversidad de identidades son principios y conceptos defendidos por las instituciones que velan por los derechos de los ciberusuarios ante las invasiones, sin previo aviso ni consentimiento, que se llevan a cabo a través de Internet y de las Nuevas Tecnologías de la Comunicación y la Información.

El derecho a ser dejado en paz

Antes de la existencia de las redes locales de comunicación (LANS) surgidas en los años 60 y 70 y de las redes globales de comunicación (WANS), con mayor presencia a partir de la década de los 80 y 90, la mayor parte de las informaciones concernientes a una persona estaban conservadas en su domicilio, cada uno era dueño de sus datos personales, y sólo una vigilancia física podía amenazar la vida privada, atentando al derecho a «ser dejado en paz, al abrigo de la mirada del otro», como afirma la Declaración Universal de los Derechos del Hombre. Sin embargo, el desarrollo de la informática ha permitido la integración y la centralización de las informaciones confidenciales privadas.

«El derecho del hombre a ser dejado físicamente en paz ocupa pues el lugar de la protección contra las intrusiones informacionales», una postura lógica que defiende el investigador Mathieu O'Neil (1998), quien añade que si el ser humano es propietario de todas las informaciones que le conciernen, esto hace que él sea el regulador de los flujos de difusión de esas informaciones. Al menos, así debería de ser en la práctica. Esto obliga a redefinir la noción misma de vida privada, que

---

1 Javier Echeverría es catedrático de Lógica y Filosofía de la Ciencia del Centro Superior de Investigaciones Científicas (CSIC) de España y autor del libro *Los señores del aire: Telépolis y el tercer entorno*, Destino, Barcelona, 1999, donde defiende la tesis de que algunas de las nuevas tecnologías permiten generar un nuevo entorno, bautizado por él como el tercer entorno (E3), con propiedades topológicas, métricas, físicas y sociales propias y diferentes a los otros entornos existentes en el mundo (E2 y E1) y donde Telépolis es la ciudad a distancia, la ciudad global, el conjunto de formas de interacción social que se han ido desarrollando y continúan expandiéndose en este tercer entorno.

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

se convierte en «la difusión más o menos restringida que se da a hechos públicos»[2]. Por otro lado, parece justo que una institución financiera o comercial que concede un crédito tenga derecho a informarse sobre los antecedentes financieros del solicitante. Del mismo modo que se comprende ¿por qué un propietario de una vivienda no puede informarse sobre el pasado judicial de un futuro inquilino?

Con el desarrollo de las redes, las cuestiones que conciernen a la exactitud de los datos y a la identidad de los que pueden acceder a ellos toman un nuevo sesgo. En la mayoría de los códigos deontológicos de trabajadores de la informática aparece la exactitud como principio ético fundamental, puesto que los dos aspectos que representa, la puntualidad y la fidelidad en la transmisión de los datos, son cada vez más necesarios en el tercer entorno (E3). En el ciberespacio se da una tendencia a «creérselo todo», debido a lo complejo de la tecnología y a las miles de áreas del conocimiento humano que por sus redes discurren y ello es peligroso. En este nuevo entorno regido por la tecnología, los ficheros han sido agrupados e integrados en bases de datos, suprimiendo el tiempo, las distancias y las gestiones administrativas que limitaban el acceso a una elite de controladores de informaciones. Con Internet, el acceso se generaliza bruscamente. Todo lo que no tiene restricción está instantáneamente disponible desde cualquier sitio. Por tanto, en la cuestión de la protección de la vida privada se pasa de la escala local y nacional a la escala internacional.

En cuanto a la identidad, como señalan Javier Echeverría y Francisco Álvarez (1999: 95), el E3 «debe ser considerado como un nuevo sistema identitario (...) una misma persona física o jurídica puede conectarse a la red a través de distintos servidores, lo cual le permite tener una identidad plural». Para estos autores un mismo sujeto físico o jurídico puede disponer de varias «telecasas» en Internet, donde en unas recibe a un tipo de gente en general, otra la destina a encuentros con amigos y, finalmente, deja un espacio para su estricto uso en la intimidad o incluso que puede llegar a ser secreto. Pero, sin embargo, ambos expertos reconocen que para lograr una mayor intimidad o privacidad de los contenidos que difundimos por la red es necesario renovar frecuentemente los sistemas de encriptación de los mensajes o «telecasas» para evitar visitas no deseadas. Sin embargo, la existencia de programas avanzados capaces de descifrar cualquier mensaje que circule por la red es una realidad y la mayoría de los navegantes de Internet lo desconoce.

---

2 LEJEUNE, JEAN.MARC. «Informatique et vie privée». *Problémes économiques.* París, 29 de mayo de 1996. (Cit. por Mathieu O'Neil en op. cit. p. 30).

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

De igual forma, los ciberusuarios no supieron de la existencia de la mayor red de espionaje a través de las nuevas tecnologías de la comunicación que ha habido nunca, el sistema de vigilancia Echelon, liderado por los Estados Unidos y el Reino Unido[3] hasta que se presentó en la Unión Europea un informe[4] sobre los peligros que conlleva que los gobiernos traten de controlar todo lo que circula por Internet. En el citado estudio se advertía que las actividades que desarrolla esta red, compuesta por 140 centros repartidos por todo el mundo, no tiene por único objetivo interceptar las comunicaciones con la finalidad de salvaguardar a la sociedad de terroristas, narcotraficantes, pederastas, etcétera, sino que, además, se estaba empleando para favorecer los intereses comerciales de los países participantes. Esto también lo confirma Margaret Newhan, quien contribuyó a crear el programa de aplicación de esta red de espionaje, y hoy en día forma parte del grupo de los arrepentidos que participaron en su creación. Según esta programadora, bajo el pretexto de que la red sirve al orden social, se observa a cualquier ciudadano y se espía a las empresas a favor de concretos y determinados intereses norteamericanos (Ramos Fernández: 2000)[5]. Con este «Gran Hermano» presente, cada vez que pronunciamos en una conversación telefónica o escribimos en nuestro correo electrónico o en un fax las palabras consideradas en ese momento como claves para las investigaciones que se están desarrollando, nuestro mensaje es interceptado y enviado a la Agencia Nacional de Seguridad (NSA) de Estados Unidos.

Otro tipo de ataque a la privacidad, aunque de índole distinto, fue desarrollado como consecuencia de la lucha que han mantenido las empresas de Microsoft y Netscape desde sus orígenes: Microsoft llegó a colocar un archivo rastreador para conocer el perfil de sus usuarios en el programa *Front Page* sin que de ello fuera informado con anterioridad el consumidor del producto.

En un informe de actividades presentado en julio de 1998, la Comisión Nacional de la Informática y las Libertades (CNIL) de Francia se alarmaba ante los «yacimientos de datos» que «pueden ser utilizados a espaldas de las personas para constituir perfiles individuales de consumo o vigilar la navegación de un internauta»[6]. Hoy en día, esta práctica es muy frecuente en la red y obedece a los

---

3 Además de los Estados Unidos y el Reino Unido, participan en Echelon los servicios secretos de Australia, Nueva Zelanda y Canadá.

4 El informe titulado *Una aproximación a las tecnologías de control político* presentado en enero de 1998 y elaborado por la oficina del Parlamento Europeo que se ocupa del estudio de las cuestiones científicas y técnicas (STOA) estudia extensamente los riesgos y peligros que implica la posibilidad de que gobiernos e instituciones supervisen todo lo que discurre por la red.

5 Esto quedó constatado en la operación que perdió el consorcio europeo Airbus con un país latinoamericano y que terminó en beneficio de los norteamericanos tras ser informados por los servicios de espionaje de Echelon.

6 CNIL (1998): *18º rapport d'activitè 1997*. París, La Documentation française. (Cit. por Mathieu O'Neil en op. cit. p. 30).

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

intereses del mercado publicitario principalmente, registrándose cada uno de los pasos que da un visitante en una *web* desde que entra en el sitio hasta que lo abandona. Si llega a realizar alguna compra, con la tarjeta de crédito estará facilitando su nombre y ayudará a completar así el registro personal que esta empresa tendrá a partir de entonces de este ciberusuario. Si no llega a comprar se le asignará un número de serie o un código de barras donde se recogen sus preferencias y se le relacionará con un perfil de usuario.

O'Neil va aún más allá y comenta que en los Estados Unidos las empresas pueden proceder a fructíferas agrupaciones entre los registros de estado civil, los ficheros de las agencias federales, las listas electorales y los ficheros en disposición de la policía o de los tribunales, las prisiones, las universidades, el ejército, los organismos que hacen inventario de las operaciones bursátiles, etcétera. Pero todavía hay más, porque las empresas más audaces trabajan para obtener «motores de búsqueda» superpotentes que desentierren datos para «clubes de genealogía, asociaciones de búsqueda de desaparecidos o de lugares» que permitan encontrar amigos perdidos de vista a partir de direcciones o de números de teléfono, entre otros[7]. Con ello se pretende proporcionar respuestas inmediatas a preguntas sobre personas concretas, como puede ser, por ejemplo, sobre la *baby-sitter* que se desea contratar, y saber así si se trata de una buena alumna universitaria o si ha sido condenada por exceso de velocidad o consumo de drogas.

Para algunos expertos el problema radica en la seriedad con que se tome el problema de la intimidad, que, como afirma el profesor Porfirio Barroso (1997), «si la intimidad se convierte en una broma en el ciberespacio, el medio será evitado tanto por los proveedores como por los consumidores por ser demasiado arriesgado para confiar los datos personales o de propietarios». Si los datos se manejan con seriedad y rigurosidad, para el beneficio del conjunto de la sociedad y de los individuos en particular, una parte de esta comunidad global, probablemente la formada por los navegantes más veteranos, no pondrá objeciones a perder parte de su vida privada en aras de una mayor comodidad, rapidez y seguridad de sus operaciones diarias a través de Internet.

Pero, ¿qué ocurrirá si los datos personales que se recogen no son exactos? ¿Y si se produce un error de identidad debido a nombres iguales o similares que circulan por las cientos de bases de datos que hay en la red relacionadas con pederastas, personas buscadas, etcétera? Entre los diversos sitios que hay en Internet donde se informa sobre la privacidad y la seguridad de los datos que se transmiten a través de la misma y que ofrece algunas soluciones ante estos casos se encuentra la *web* de Privacy, Inc. En ella se repasa a fondo los bancos de datos

---

7 EUDES YVES. «Vie privée à vendre sur le rèseau». *Le Monde diplomatique*, 15 de junio de 1997. (Cit. por Mathieu O'Neil en op. cit. p. 31).

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

públicos y se informa gratuitamente a los internautas norteamericanos «de la captura, del uso y de la redistribución de informaciones personales», además de «sensibilizarles ante los riesgos de error ligados a una identidad errónea» insertada en esos bancos de datos (URL: http://www.privacyinc.com). Esta entidad ofrece una solución ante los interrogantes planteados que, cuando menos, nos hace cuestionarnos quién estará realmente detrás de la Privacy, Inc. .Este organismo, para evitar problemas de identidad ofrece un servicio que denomina Goverment Dossier Service para que el usuario pueda introducir directamente los datos personales en los distintos bancos de datos (FBI, CIA, ATF y otras agencias) de los Estados Unidos. Una extraña forma de defender el derecho a la privacidad.

¿Leyes, normas o códigos de ética?

Ante la intromisión que se produce en el Tercer Entorno, favorecida por las nuevas tecnologías de la información y la comunicación (TIC), los estados están tomando diversas actitudes, mientras unos optan por proteger la privacidad mediante leyes, como ocurre en Europa y en partes de Asia, el país donde más presencia tiene Internet, Estados Unidos, no tiene previsto emprender acciones en ese sentido a corto plazo. Los motivos de esta ausencia de legislación se deben, según Lawrence Lessig (1999), profesor de derecho de la Universidad de Harvard, a varias razones complejas: «Algunas se relacionan con el escepticismo general existente sobre la protección legal en esta área; otras, con el extraordinario poder de presión de los intereses que se verían afectados por la regulación de la privacidad de la información; y otras más, relacionadas con las demandas de los propietarios de estos datos respecto de la privacidad de los individuos». Pero que la privacidad no esté amparada por la ley en todos los países no debe de alarmar, porque como apunta Lessig, ésta no es el único tipo de protección que podemos esperar, y constituye solamente una de las cuatro formas mediante las cuales se la salvaguarda en el espacio real.

Las normas también contribuyen a la protección de la privacidad. Son fuente de restricciones diferentes a las de la ley, pero tratan de proteger la vida privada de los individuos mediante sanciones ejecutadas por miembros de una comunidad determinada. Así, en las relaciones entre o con empresas o corporaciones, «las normas restringen el tipo de usos que estas compañías hacen de los datos que recogen» (Lessig, 1999). Además, en esa línea se encuentran diferentes asociaciones profesionales que proponen diversos «códigos de buena conducta». De hecho, ésta es la solución propuesta por el gobierno norteamericano, que quiere que las empresas desarrollen códigos que regulen el uso de los datos personales y el estado dependería de esa autorregulación para proteger la privacidad de sus ciudadanos.

Otra vía de limitar la vida privada la puede proporcionar el mercado. En este sentido, declaraba ya en 1997 el vicepresidente del sector informático de la

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

National Retail Federation (NRF, un *lobby* norteamericano que agrupa a las principales empresas comerciales) que, «en la ausencia de regulación, es el mercado el que determinará si las empresas satisfacen o no las necesidades de los consumidores en materia de vida privada. Las compañías que no den satisfacción a sus consumidores acabarán por perdernos»[8]. Lessig añade que la reputación existente en el mercado es afectada por el uso que las corporaciones hacen de los datos privados y propone que, en algunos casos, las empresas podrían ofrecer servicios más caros a cambio del compromiso de una mayor protección de la privacidad. Pero no todos están a favor de la autoregulación. Ya en junio de 1998, la Comisión Federal de Comercio de Estados Unidos (Federal Trade Commission, FTC), dedicada a la protección del consumidor y de la competencia criticaba en un informe que «el 85% de los editores de espacios *web* colecta informaciones personales de sus visitantes, pero sólo el 13% anuncia el uso que van a tener». La FTC renunciaba entonces a la autorregulación para preconizar una legislación «que obligue a los sitios *web* a mostrar claramente su política» en la materia[9]. Aquel mismo año esta comisión elaboraba las normas de protección de la privacidad infantil en línea (Children's Online Privacy Protection Act) y en abril de 2000 éstas se amplían a los operadores de *websites.* Entre las normas que se les exige cumplir a los sitios *web* está la de incluir su «Privacy Policy» (política de privacidad) en la página principal, donde se especifique el tipo de información personal que se recoge, qué uso va a darle el sitio a esa información, si se la va a facilitar a los anunciantes o a terceras partes y siempre debe de figurar una forma de contactar con el propietario de la página.

Pero para Lessig la restricción más importante se encuentra en lo que él llama la arquitectura, es decir en la propia tecnología, que debe de establecer fórmulas, programas, etcétera que protejan contra con la invasión de la intimidad y la vida privada (por ejemplo, la criptografía[10]) o que recreen la privacidad donde otras tecnologías la hayan erosionado. Pero este experto en la materia va más allá y recuerda que en realidad son «estas cuatro restricciones actuando conjuntamente lo que determina la privacidad en un contexto determinado». Como solución propone una acción conjunta entre arquitectura y mercado en la que se podría dar

---

8 «NRF to Adress Privacy Issues at Brussels Conference», comunicado de prensa de la NRF, 15 de septiembre de 1997. (Cit. por Mathieu O'Neil en op. cit. p. 31).

9 RULE, JAMES B. «Our Data, Our Rights». *The Washing Post, 17 de octubre de 1997.* (Cit. por Mathieu O'Neil en op. cit. p. 31).

10 La criptografía, en especial la de clave pública, facilita a los individuos ocultar más eficazmente datos y hechos de sí mismos ante terceras personas, pero no oculta los datos de las transacciones, o impide la supervisión de los movimientos o de los registros telefónicos. Pero la criptografía posibilita tanto la ocultación como la autentificación, permite ocultar lo que uno dice, y autentificar quién es uno. Piénsese en que la firma digital, por ejemplo, puede certificar que una persona ha enviado un documento y el certificado digital puede dar fe de que la persona es quien dice ser.

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

un régimen de propiedad en el que el poseedor -el individuo- tiene derecho a conservar su propiedad, al menos hasta que un comprador pague lo que el vendedor pide. Sin embargo, como plantea Lessig el problema radica en establecer los precios que deben ser pagados y para solucionar esto entran en juego las tecnologías, la arquitectura.

Existen varios programas que pueden hacer factible esa estructura de negociación como es la Plataforma para las Preferencias de Vida Privada (P3P), diseñada por el consorcio de la World Wide Web (Web Consortium, W3C) y sostenido por un centenar de empresas. El P3P es un estándar que negocia protocolos sobre privacidad entre los usuarios y los sitios web[11]. Esta «plataforma permite al internauta determinar por adelantado qué informaciones serán deducidas previamente durante sus visitas a un lugar *web* o en una transacción *on-line*, así como el grado de difusión ulterior de esos datos. Necesitará en el primer momento responder a un cuestionario que se almacenará en sus ordenadores y enumerará: su nombre, dirección, situación familiar, número de teléfono, dirección del correo electrónico, centros de interés y «categorías de mercancías preferidas». Se facilita la lista de sitios web a los que esas informaciones están destinadas. Para los que se sorprenden de esta curiosa manera de proteger la vida privada, se les responde que vale más un control limitado que un control absoluto. (O'Neil, 1998). Como podemos observar, nuevamente se da la posibilidad al usuario de que proporcione sus datos a cambio de una mayor seguridad o protección. Anteriormente vimos que la excusa era evitar que se produjeran errores de identidad al cruzarse las distintas bases de datos y ahora vemos que para impedir mayores intromisiones se nos ofrece que demos unos datos mínimos. Sin embargo, probablemente sean suficientes para que el mercado publicitario construya nuestro perfil de usuario en la red.

Para O'Neil (1998), la solución a «las exigencias contradictorias de los Estados, de las empresas y de los ciudadanos -reclamando los unos más informaciones íntimas, y los otros más barreras- serán verosímilmente resueltas en la armoniosa fusión del comercio electrónico: personalizado, seguro y eficaz al 100%». No cabe duda de que para que el comercio electrónico avance será necesario que aumente la seguridad en la red, y, con ello, esperemos que la protección del derecho a la privacidad sea mayor.

---

11 En palabras de sus autores, recogidas en el artículo de Lessig (1999), P3P es: «[una] forma interoperativa de expresar las prácticas y preferencias de privacidad por parte de los sitios web y los usuarios, respectivamente. Las prácticas de los sitios que encajen dentro de las preferencias de un usuario permitirán que este acceda al mismo sin problemas. En caso contrario, el sitio informará al usuario sobre sus prácticas de privacidad y este tendrá la opción de dar su conformidad y continuar su visita si lo desea».

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

La situación europea

En Europa, cuando se empezó a trabajar en estos asuntos se tomó como punto de referencia las autorregulaciones suecas, alemanas o francesas en esta materia, con las que en 1995 se adoptó una directiva comunitaria sobre la protección de datos, y su traslado a las legislaciones nacionales se dispuso para octubre de 1998. Esta directiva tiene por finalidad asegurar una armonización de las leyes que protejan las informaciones personales, con el fin de facilitar su flujo en el seno de la Unión Europea. El artículo 25 de la directiva dice que sólo países que garanticen un «nivel de protección suficiente» podrán beneficiarse de las transferencias de datos.

Otra de las herramientas que la Unión Europea ha articulado en relación con la protección de la vida privada ha sido la Decisión 276/1999 del Parlamento Europeo y del Consejo, de 15 de enero, por la que se aprobó una mayor seguridad en la utilización de Internet, mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Sin embargo, resulta obvio que los datos no se detienen en las fronteras de la UE y, por tanto, los juristas se encuentran con la dificultad de aplicar a las redes la concepción tradicional del derecho, que se funda en el lugar en donde se desarrolle un intercambio o una infracción y en la domiciliación de lo interesado. «Se comprende, pues, el interés que presenta, para empresarios poco escrupulosos la transferencia de información desde países proteccionistas hacia aquellos cuyas legislaciones son menos restrictivas» (O'Neil, 1998). La Decisión de la UE, además, se apoya en gran parte en la cooperación internacional, pero como se cuestiona Fernando Ramos (2000): «¿cómo fiarse de unos supuestos aliados que nos espían?» Pero quizás no deberíamos de ser tan desconfiados y agradecer que por medio de este sistema haya sido posible, entre otros logros, obtener pruebas de que Indonesia estaba violando los Derechos Humanos en Timor oriental.

En materia que afecta directamente a la privacidad, los países miembros de la UE aprobaron el 31 de mayo de 2000 el acuerdo llamado «Safe Harbor» (puerto seguro), aunque sus principios ya han sido criticados como insuficientes por algunas organizaciones como la Trans Atlantic Consumer Dialog (TACD)[12]. En torno a esa misma fecha la Unión Europea ha presentado un proyecto de plan de acción al que ha bautizado como *eEuropa 2002. Una sociedad de la información para todos,* con el que pretende no sólo estimular el uso del nuevo medio, invertir en competencias de Internet y en el acceso, que ésta sea más rápida y más económica, sino que también sea más segura[13].

---

12 *Washington Post*, 1 de junio de 2000.

13 El documento oficial del proyecto *eEuropa 2002* está fechado en Bruselas el 24 de mayo de 2000.

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

Así mismo, el grupo de los ocho países más industrializados del mundo, el G-8, reunidos en París en el mes de mayo de 2000 han estado trabajando en una resolución sobre el crimen cibernético, llegando a un acuerdo tanto la industria como los gobiernos para aumentar la cooperación en la lucha contra el cibercrimen. En materia de privacidad, se rechazaron las propuestas planteadas sobre el control de los ISPs o de tomar más informaciones sobre los usuarios.

No obstante, mientras determinados países hablan de buenas intenciones y de respeto a la intimidad de los individuos, otros, como el Reino Unido, afianzan su control sobre el ciberespacio estableciendo nuevos sistemas de vigilancia. A finales de abril de 2000 el Reino Unido anunciaba su nuevo sistema de supervisión de la red, situado en el llamado Goverment Technical Assistance Center -curiosamente no lleva por título ninguna palabra que lo relacione con control, supervisión o espionaje-. Este centro tiene el «superpoder» de ver todos los mensajes enviados y recibidos en el Reino Unido a través del correo electrónico. ¿Qué puede haber que atente más contra la intimidad del individuo que el hecho de que se lean su correo personal?

Vida privada *on-line*, en venta

Como puede desprenderse de los caminos que están siguiendo las líneas de protección de la vida privada *on-line*, y por las soluciones que apuntan expertos como Lessig, el deseo natural de ser dejado en paz puede convertirse en una fuente económica: si se puede vender todo ¿por qué no entonces también la vida privada? Andrew Saphiro, periodista del semanario norteamericano *The Nation*, pone en guardia contra la continuación lógica del pensamiento de Jame Rule, que coincide con la solución aportada por Lessig: el advenimiento de un mercado de la vida privada, donde los internautas deseos de discreción pagarán un precio por la seguridad de sus datos (su proveedor de servicio no revelará nada), mientras que los otros verán su intimidad ofrecida como mercancía[14]. Seguramente, ese sistema supondrá innumerables e importantes inconvenientes. El anonimato que hace las delicias de los ciberusuarios desaparecerá: será difícil protegerse, falsear informaciones. Los menos ricos, detentadores de informaciones confidenciales de «segunda clase», serán más pobres en intimidad al venderla a las empresas. Como dice O'Neil, a largo plazo, este sistema ratifica la concepción que convierte la vida privada en una propiedad alienable, y, usando la terminología de Román Gubern, esto provocará que los inforricos se protejan más contra el conocimiento de su intimidad y los infopobres serán la población de mayor riesgo.

---

14 SHAPIRO, ANDREW L., «Privacy for Sale: Pendig Data on the Internet», *The Nation*, junio de 1997. (Cit. por Mathieu O'Neil en op. cit. p. 31).

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

Nuestra época parece a veces estar habitada por numerosas paradojas: si hasta ahora había muchos famosos a los que la fortuna les había sonreído pero que a la vez podían ser los más desgraciados por estar privados de intimidad, sintiéndose hostigados por los paparazzis, en lo sucesivo, cada vez habrá más «conocidos públicamente», que transformarán su derecho elemental a la intimidad en un producto comercial (al estilo de la producción televisiva «El Gran Hermano» o de los sitiosweb en los que la gente muestra su vida en el hogar). A pesar de todo, uno puede tener la esperanza de que si hasta ahora siempre ha estado prohibido vender su voto o a sí mismo como esclavo, podemos preguntarnos como O'Neil «¿por qué la vida privada va a ser dispensada de esas reglas de autonomía cívica?» La respuesta a esta y a otras preguntas aquí planteadas todavía no la tenemos, pero lo cierto es que, por el momento, todo apunta a que cada vez más, lo queramos o no, vamos perdiendo en privacidad.

El movimiento contemporáneo de la ciudad a la aldea global, del que se felicitaba McLuhan, entraña, pues, el replanteamiento de un privilegio moderno y fundamental, el derecho al anonimato. Pero, ¿no es en estas aldeas, contrariamente a lo que ocurre en las ciudades, dónde se produce una mayor vigilancia y supervisión de las actividades que desarrolla el individuo?

La necesidad de un código

Ante la falta de regulación por parte de los Estados y el interés latente de conocer las audiencias a toda costa para mejorar los productos y servicios que se ofrecen en la red, y conseguir mayores beneficios a través de la publicidad, se hace necesario que desde distintas instituciones que trabajan en defensa de los consumidores y usuarios de Internet se elaboren propuestas de códigos deontológicos sobre este asunto.

Ya en 1986, Richard Manson publicaba un artículo que tuvo una gran repercusión, titulado «Four Ethical Isusues of the Information Age» donde identificaba cuatro temas éticos que son clave para las aplicaciones de la tecnología de la información. Estos son: intimidad, exactitud, propiedad intelectual y accesibilidad. Si se atiende al uso que hacen diferentes códigos existentes en el mundo vemos que el respeto a la intimidad está presente en todos ellos, pero el problema radica en que son las empresas en su conjunto las que utilizan esos datos para su beneficio y los códigos suelen aludir, en la mayoría de los casos, al compromiso ético y moral del trabajador y no a la empresa.

En una propuesta que hace el profesor Porfirio Barroso (1997), especialista en deontología informática, se argumenta, en esa línea, que se debe respetar la necesaria protección y seguridad en la información, así como la intimidad y la vida privada de las personas y la confidencialidad de la información cuando la hubiere.

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

Conclusiones

Después de este breve recorrido en el que se pone sobre aviso de los peligros que invaden a la privacidad de los ciberusuarios o habitantes del tercer entorno no podemos más que concluir con algunas observaciones que pensamos que deberían ser tenidas en cuenta por los usuarios de Internet, los Estados y las empresas con *websites*. La libertad de todo ser humano al anonimato tendría que ser respetada en todos los ámbitos, incluida la red de redes, por tanto, los usuarios no tendrían que verse jamás obligados a rellenar formularios con sus datos cuando quieran acceder a informaciones consideradas de interés público, si el fin es recabar información del cibernauta para aumentar los ingresos en publicidad, es decir con fines exclusivamente mercantiles. Pensamos que al usuario se le debe de preguntar e informar detalladamente de las prácticas que se van a realizar con sus datos en primer lugar, y se le debe de explicar el objeto del acto y el uso que se le va a dar a esas informaciones personales. Estas empresas jamás deberán vender a terceros dichos datos obtenidos sin el consentimiento tácito de los ciberusuarios.

Cada día son más numerosas las encuestas o pequeños formularios que aparecen en Internet, así como se está convirtiendo en habitual el tener que registrarse en numerosas páginas para poder entrar en sus contenidos, esto no siempre se hace con fines publicitarios sino también como medida de seguridad ante visitantes inoportunos, son las llamadas *firewalls* o pantallas que filtran qué usuarios pueden o no entrar en el *site*. Todo ello hace aún más necesario y urgente el establecer leyes o normas internas en empresas o asociaciones que regulen el uso que se hace de la información de los usuarios de la red, para garantizar este derecho a estar en paz y a poder usar el anonimato cuando se desee.

Otro problema que ataca a la intimidad es el derivado de la existencia de sistemas de control de las comunicaciones, es decir, sistemas de espionaje, como Echelon, por medio de los cuales nuestras comunicaciones son interceptadas en cualquier momento, si pronunciamos alguna de las palabras que estos centros tienen establecidas como claves y con las que se activa el proceso de grabación. De esta forma, el derecho a la intimidad de las personas no cabe duda que es vulnerado, pero, sin embargo, si además de operar por la defensa nacional se realiza para salvaguardar de peligros a su economía habrá que tratar de impedir que este otro Gran Hermano siga en funcionamiento. No hay que olvidar, como señalan Javier Echeverría y Francisco Álvarez (1999: 115), que este Tercer Entorno en el que nos estamos moviendo surge como prolongación y perfeccionamiento de actividades humanas muy concretas (militares, científicas, financieras, informativas, etc.), y, por tanto, estos ámbitos «marcan inicialmente los problemas y las reglas del juego en el Tercer Entorno».

Así mismo, para finalizar, compartimos con ambos expertos que la solución al problema de la intimidad en el nuevo entorno debe de centrarse en la búsqueda del equilibrio entre una reformulación de los «derechos tradicionales como el de

http://dx.doi.org/10.12795/Ambitos.2000.i05.07

la intimidad» y «las posibilidades de su realización en el nuevo marco tecnológico, las nuevas amenazas y las nuevas exigencias» (Echeverría y Álvarez,1999: 131). Argumento que está en la línea de pensamiento de Esther Dyson (*El País*, 4-6-2000), considerada como la pitonisa de Internet, y presidenta de la Internet Corporation for Assigned Names and Numbers (ICANN), quien recuerda que «la dificultad reside en mantener el equilibrio entre una buena seguridad y una buena libertad, éste va a ser nuestro próximo reto».

Bibliografía:

- O'NEIL, Mathieu: «Internet como riesgo para la vida privada», en *Le Monde Diplomatique*, septiembre, 1998.
- BARROSO, Porfirio: «Cuatro principios de ética en Internet», en *ZER. Revista de estudios de comunicación*, núm. 3, noviembre de 1997, Servicio Editorial Universidad del País Vasco.
- DEBORAH G., Johnson (Traductor Porfirio Barroso): *Ética informática*, Editorial Universidad Complutense de Madrid, 1996.
- ECHEVERRÍA, J. Y ÁLVAREZ, F.J. : *Valores y ética en la sociedad informacional*, Uned, Madrid, 1999.
- Federal Trade Commission (FTC) de los Estados Unidos. URL: http://www.ftc.gov/
- LESSIG, Lawrence: «La arquitectura de la privacidad», en *Cuadernos Ciberespacio y Sociedad*, núm. 2, febrero 1999. Texto traducido por Javier Villate. URL del documento original: http://cyber.harvard.edu/works/lessig/architecture_priv.pdf
- PIQUER, Isabel. «Esther Dyson, la pitonisa de Internet», en *El País*, domingo 4 de junio de 2000.
- Privacy Inc. URL: http://www.privacyinc.com
- Privacy Internacional. URL: http://epic.org
- RAMOS FERNÁNDEZ, Fernando: «Echelon, el Gran Hermano que realmente nos vigila y otros riesgos de Internet», en *Actas del Congreso de la Asociación Española de Periodística*, celebrado en Madrid en mayo de 2000. (En prensa).

(Recibido el 18-11-2000, aceptado el 1-12-2000)