INTERNET y la sociedad de la información

Una mirada desde la periferia

TOMO II

Editor: Octavio Islas

CIESPAL
2005

INTERNET y la sociedad de la información
Una mirada desde la periferia

1000 ejemplares - agosto 2005

SBN 9978-55-049-6
Código de Barras 9789978550496
Registro derecho autoral Nº 022136

Portada:
Juan Pablo Muñoz

Diagramación texto:
Fernando Rivadeneira León

Impresión:
Editorial "Quipus", CIESPAL
Quito – Ecuador

Contenido

La protección de datos en la sociedad de la información

*Carlos Colina**

Introducción

Para algunos autores, la privacidad es uno de los temas centrales de nuestra época. De hecho, desde hace unos lustros, la rápida dinámica de la globalización y la amplia implantación concomitante de las tecnologías digitales han conllevado a la necesidad de crear o reconstruir las políticas sobre privacidad informática en distintas naciones. El comercio electrónico y el flujo de datos transfronteras han encontrado marcos legales dispares en las distintas regiones del orbe. Latinoamérica se ha separado de la política legislativa estadounidense que se fundamenta en la autorregulación, porque quizá ha comprendido que la ley, si bien no puede llegar al extremo de obturar el libre funcionamiento de las redes de información y comunicación, tampoco puede dejar de proteger los derechos fundamentales de sus ciudadanos. Sin embargo, en general, la legislación de la región se ha desarrollado lentamente, presenta grandes vacíos y deficiencias institucionales (Castro, 2003).

* Venezolano. Doctor. Profesor de pregrado y postgrado. Investigador del Instituto de Investigaciones de la Comunicación (ININCO), de la Facultad de Humanidades y Educación de la Universidad Central de Venezuela.

Desde el punto de vista sociológico, no existe una definición unívoca de privacidad, ya que varía de acuerdo con el contexto, la cultura y el tiempo. Según David Banisar (1998), el concepto de privacidad abarca varios aspectos: la información, las comunicaciones, la privacidad territorial, y la privacidad corporal. Rankin delineó tres componentes de la privacidad: la concebida como resguardo del territorio y del espacio; la vinculada a la persona como tal; y la correlacionada con la integridad y dignidad humana ante la recolección y venta masiva de la información (Citado en Lyon y Zureyk, 1996: 14).

Esta noción tiene significados diferentes para los distintos pueblos, en función de los cuales se sostienen distinciones disímiles entre lo público y lo privado y diferentes criterios sobre lo que puede ser difundido públicamente. Así mismo, el valor discriminatorio de una información privada depende del contexto. No obstante, no se abundará aquí sobre la dimensión sociológica del fenómeno, sino más bien sobre su enfoque jurídico. Lo que puede señalarse, aunque sea de paso, es que parecemos asistir a una redefinición de las fronteras entre lo público y lo privado. Además, puede agregarse que la privacidad es un valor esencial en una sociedad democrática, tolerante y pluralista. Los gobiernos totalitarios prefieren un estado de vigilancia (Reidenberg, 1999).

En la sociedad contemporánea no es un secreto que empresas públicas y privadas almacenan datos y cifras sobre las personas en archivos de bases de datos. Administrar archivos de este tipo no es una novedad para los gobiernos modernos, pero el Estado actual se documenta sobre los ciudadanos como nunca antes. A través de las redes informáticas se interconectan los distintos programas y archivos, con lo cual aumenta exponencialmente la utilidad y aplicabilidad de la información.

En realidad, lo que permiten las nuevas tecnologías son mayores facilidades de elaboración y transmisión de la información dentro de una red, y el acceso a distancia. Para algunos se trata de unos medios de verificación, control y manipulación mucho más eficaces:

"La información almacenada en un expediente automatizado puede ser correlacionada con la información de otras bases de datos y transmitida a lo largo y a lo ancho del país en cuestión de segundos a un costo relativamente bajo. La amenaza a la privacidad no podría ser más obvia". (Forester, 1992: 316).

En los Estados Unidos los sectores público y privado cooperan y se intercambian información, y, más aún, ciertas oficinas de crédito la registran en fichas bajo el epígrafe de *estilo de vida*. El denominado *modelado en bloque* integra información fragmentaria proveniente de numerosas fuentes y la somete a programas que la comparan con esquemas de personalidad generalizados:

"La información que contienen los bancos de datos es la vida reducida a las necesidades mínimas para tomar rápidamente una decisión comercial o jurídica...Conceded o no concedáis un préstamo...Detenedle o no le detengáis"... (Roszak, 1988: 226).

La elaboración de perfiles de las personas se realiza mediante el emparejamiento de datos:

"Que supone el cruce de dos o más elementos contenidos en diferentes bases de datos". (Campuzano, 2000: 61).

El mercado de la recolección y posterior venta de datos personales es un gran negocio en los Estados Unidos, que en 1998 arribaba a ganancias anuales superiores a 1.5 billones de dólares. Compañías poco conocidas como Acxiom o Firts Data poseen *data houses* con la información detallada e íntima de millones de estadounidenses. La primera empresa vende datos tales como la pertenencia étnica y religiosa, el modelo de auto y el tipo de vestimenta que una persona suele adquirir.

Cualquier usuario de Internet es consciente de las amenazas y violaciones a la confidencialidad que se sufren con la utilización del correo electrónico:

"Cada vez que alguien utiliza el correo electrónico, navega por la red, interviene en foros de discusión (chats), participa en grupos de noticias o hace uso de un servicio, está revelando datos acerca de su personalidad, economía, gustos, hábitos sociales, residencia, etc., los cuales pueden ser utilizados por terceros en perjuicio del usuario". (Campuzano, 2000: 67).

En cada oportunidad en la cual el internauta enciende el ordenador e inicia una sesión de navegación, deja datos personales en archivos ocultos denominados cookies. Cuando visita una página Web suministra información clave de manera rutinaria al proveedor o administrador del sitio:

"A éste no le resulta difícil averiguar la dirección de Internet de la máquina desde la que está operando, la dirección de correo electrónico del usuario, que páginas lee y cuántas no le interesan, cuántas páginas ha visitado, así como el sistema operativo y el navegador utilizado". (Campuzano, 2000: 68).

Algunos navegadores envían al fabricante un archivo oculto de las direcciones de Internet visitadas por el internauta.

En 1999, Intel tuvo la iniciativa de incluir un número de serie único en sus procesadores Pentium III. El *Procesor Serial Number* (PSN) es un número exclusivo que identifica al procesador, mediante el cual los proveedores de servicios on-line pueden elaborar un perfil del usuario, útil para asuntos de marketing y para el Spam, pero no para la privacidad del 75 por ciento de los usuarios, ya que la multinacional de los microprocesadores poseía ese porcentaje del mercado.

"Gracias a la actividad de grupos como bigbrotherinside, Intel ha decidido alentar a los fabricantes de PC a que pongan en modo de apagado al PSN así como de proveer el processor serial number control utility, que es un programa con el cual se puede desactivar o activar el PSN". (S/A, 1999).

La jurisprudencia ha tratado de responder al desafío que plantea toda esta problemática y ha creado una legislación específica. Como *derecho de la protección de datos* se entiende el conjunto de normas, principios y garantías empleados para la tutela de los diversos derechos de las personas que pudieran verse afectados por el tratamiento de sus datos nominativos. En realidad, han existido distintas fórmulas para nombrarlo y etiquetarlo, a saber; libertad informática, derecho a la autodeterminación informativa o informática, *information control*, habeas data, que bien ahora pueden referirse a diversos aspectos del objeto de estudio. Existe consenso en cuanto a la ubicación del *derecho de la protección de datos* dentro del conjunto de la tercera generación de derechos. La *autodeterminación informativa* sería un aspecto del derecho a la protección de datos, y el habeas data, su garantía e instrumento procesal. (Puccineli, 1999: 69).

La mayoría de los autores coincide en que el derecho a la protección de datos personales es una suerte de mutación evolutiva del derecho a la privacidad, empero, nunca se agota en ella, y solo parcialmente pueden ser descrito o fundamentado a través de la noción tradicional de intimidad.

El derecho a la protección de datos personales se erige en contra de ciertas actividades como el acceso, el registro, tratamiento y transferencia ilegítimos de datos personales por parte de individuos no autorizados. En la legislación no existe uniformidad en cuanto al ámbito de aplicación: bases de datos públicos o privados, archivos informatizados o manuales. Para la Directiva Europea de 1995, la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual.

El derecho a la protección de datos suele ser tutelado de diversas formas, entre las cuales encontramos las normas generales o específicas, convencionales, constitucionales o legales; derechos de los registrados; vías judiciales de amparo específicamente amoldadas a este campo (v.gr. el habeas data del constitucionalismo

iberoamericano); la remisión a mecanismos procesales genéricos (el amparo, tutela o recurso de protección) y los convenios internacionales.

Con la informatización de la vida cotidiana del hombre de hoy, ha surgido la necesidad de establecer nuevos derechos que preserven al individuo de las amenazas que conllevan determinadas actividades de ciertas instituciones. Para algunos, estas salvaguardas jurídicas están llenas de excepciones y lagunas, y carecen de medios efectivos para hacerlas cumplir. En ese sentido, estas leyes impondrían tantas concesiones que prácticamente dejarían sin contenido derechos y garantías (Abad. 1996: 121). No obstante, conocidas las limitaciones jurídicas y sociológicas de la legislación, pienso que estas leyes son un interesante fenómeno de contravigilancia que cabe apuntalar, no solo para la defensa jurídica de los afectados sino también para la promoción de la discusión pública de un problema relevante en nuestra contemporaneidad.

Están en juego derechos y libertades fundamentales, verbigracia, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, reconoce a los ciudadanos el derecho a no verse sometidos a una decisión con efectos jurídicos significativos, si ésta se basa exclusivamente en un tratamiento automatizado de datos, destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros. (Sección VI, artículo 15). Para Herminia Campuzano Tomé, la protección de los datos personales está enraizada en la protección de los derechos y libertades fundamentales y, en concreto, en la protección del derecho a la vida privada. (Campuzano, 2000: 73).

En cierto sentido, el derecho a la privacidad e intimidad (informática) puede verse como derecho del destinatario dentro del gran marco del Derecho de la Información. La protección de los datos personales, privados e íntimos, constituye un tema íntimamente ligado a otros derechos y valores fundamentales de innegable

relevancia, tales como la libertad de expresión e información. No obstante, no son valores y derechos que coexisten siempre de manera armónica.

La libertad de expresión y la intimidad personal suelen entrar en conflicto en la sociedad actual. En algunos casos se concilian, en otros, prevalece uno sobre otro. En la práctica, el juego de uno de estos derechos se encuentra limitado por el otro. Este tema ha sido debatido reiteradamente por la doctrina a partir de los años setenta (Campuzano, 2000: 94). Para Judith Wagner (1997: 27), el concepto de privacidad ha estado desarticulado; no está claro qué se protege y qué no, y cuando se logra un poco de claridad no se sabe cómo puede ser sopesada la privacidad frente a otros derechos individuales o públicos.

Para algunos, estarían en juego varios de los principios filosóficos y axiológicos que han pretendido fundamentar las democracias occidentales. ¿Qué habría de primar?: ¿el valor individual de la intimidad o el interés social de la información? ¿la protección de datos personales o la libre circulación de la información? ¿renuncia a la privacidad en aras de la eficiencia?

En los Estados Unidos, los legisladores a favor de la protección de la privacidad han encontrado el escollo de la Primera Enmienda, la cual consagra la libertad de expresión. Si bien mi postura no tiene una base exclusivamente legal, creo que debe abogarse resueltamente por la consolidación de los nuevos derechos ciudadanos, en donde la jurisprudencia europea debe ser el norte. En los Estados Unidos de Norteamérica se han promulgado normas específicas de privacidad y leyes aisladas de alcance limitado, en forma reactiva ante situaciones escandalosas de uso abusivo de la información. Se ha rechazado la idea de crear un set completo de estándares de privacidad, porque se parte del supuesto de que funcionará la autorregulación propulsada por el sector empresarial. Como ejemplos podemos mencionar la *Fair Credit Reporting Act* y la *Video Privacy Protection Act*, que protegen comportamientos muy

específicos realizados por determinados individuos en las agencias que proveen informes crediticios o en las tiendas de alquiler de videos.

La política es reactiva, porque se considera que el mercado en sí mismo protege la privacidad ya que con un tratamiento adecuado de la data personal, se favorecería el consumidor y, por ende, se conquistaría su confianza, lo que se traduce en una maximización de los ingresos. El trabajo cooperativo entre la industria y las asociaciones de consumidores serían preferibles a la regulación por parte del gobierno. Según Reidenberg (1999), en la práctica esta política de privacidad, cimentada en la tesis de la autorregulación, se ha revelado sofística.

Las iniciativas de autorregulación como TRUSTe y BBBOnLine, presentadas como signos de progreso en el área, demuestran las deficiencias estructurales del esquema de autorregulación. Todo nos conduce a pensar que una combinación de desarrollos tecnológicos ad hoc y una legislación adecuada serán los elementos que brindarán la efectiva protección de la privacidad de los ciudadanos.

El hombre moderno conquistó el derecho a disponer libremente de sí mismo en su vida privada. Para Lipovetsky (1995:116), el ideal de autonomía individual es el gran triunfador de la condición postmoderna, en donde el homo psicologicus realizaría una hiperinversión en el espacio privado. No obstante, a la supuesta privatización exacerbada de los individuos habría que oponer la *invasión* de lo público sobre lo privado; o la simple mercantilización de lo privado por los mass media y su consentimiento por parte de los sujetos. Quizá estemos a las puertas de una reconceptualización social de ambas nociones.

Más allá de la tradición liberal que entroniza al individuo y sus derechos, más acá de la tradición totalitarista marxiana, que los niega. Pienso que la defensa de la privacidad puede ligarse a la autonomía de individuos, pero también a la de sujetos sociales, a veces excluidos. No se trata de mitificar el espacio privado, allí

también pululan los poderes, pero colocar cotos al Estado y a las megaorganizaciones podría coadyuvar a la ampliación de los espacios de autonomía y a la reducción de los espacios de heteronomía. Esta demás decir que una ley ad hoc sería solo *un paso* para que se cumplan estos nuevos derechos. No necesariamente sería el primero. Por el contrario, la participación de la ciudadanía constituye ahora y después el elemento indispensable en el logro de los mismos.

La aplicación de la normativa general de protección de datos a los medios de comunicación no esta exenta de problemas. El conflicto es inminente a medida que los mass media se informatizan y tienen acceso a las redes telemáticas. En general, independientemente de las excepciones expresas que pueda haber o no en cada nación, la normativa aludida no se aplica plenamente a los medios, como consecuencia de la situación constitucional especial de las normas relativas a la libertad de expresión y de prensa. En la *Directiva 95/46/CE* del Parlamento y del Consejo de Europa, el tratamiento de datos para fines periodísticos está eximido del régimen general de protección de datos personales, tal como reza en su artículo 9. Ahora bien, volviendo al marco general, esta normativa tiene un origen y una evolución específica que cabe revisar.

Génesis y desarrollo histórico específico de la protección de datos nominativos

Es en Alemania donde se producen los primeros antecedentes del desarrollo normativo del derecho a la protección de datos nominativos. El proceso de reconocimiento de este derecho se inicia tempranamente con la Constitución de Weimar de 1919, que en su artículo 129 establecía el debido proceso en los procedimientos disciplinarios seguidos a los funcionarios públicos, con el reconocimiento del derecho de acceso a sus expedientes personales y la prohibición de anotar datos negativos en sus legajos, hasta que hubiesen tenido la oportunidad de formular sus respectivos descargos.

Puede decirse que esta es la semilla del derecho a la protección de datos nominativos. No obstante, no será sino hasta el año 1970, mutatis mutandi, cuando en el Land de Hesse germánico, se promulgue una ley específica y especializada en la materia que nos ocupa. Al dictado de esta norma le siguieron otros Lander alemanes y otros países europeos: Austria, Dinamarca, Francia, Luxemburgo, Noruega, el Reino Unido y Suecia. A estas iniciativas legislativas pueden sumarse las acometidas por países pertenecientes a la Commonwealth británica: Nueva Zelanda (1976) y Canadá (1977). En los años setenta, la difusión de los ordenadores muestra de manera palmaria sus ventajas y riesgos. Como una respuesta a estos últimos, comenzó el proceso de desarrollo normativo del derecho a la protección de datos.

En el ámbito constitucional, los primeros países que incorporan normas específicas fueron Portugal (1976) y España (1978). En el ámbito regional europeo se destacan el Convenio 108 del Consejo de Europa de 28 de Enero de 1981 (Estrasburgo) y la Directiva relativa a la protección de datos personales, adoptada en 1995 por el Parlamento Europeo y el Consejo de la Unión Europea. La Directiva 95/46/CE tenía como objetivo expreso, precisar y ampliar los principios del Convenio 108 del Consejo de Europa. El convenio constituyó el primer texto internacional que permitió la armonización de las leyes de diversos Estados, en este caso de la UE. Sin embargo, esta legislación ha tenido que actualizarse en sucesivas directivas.

En la Unión Europea, la Comisión y el Consejo de Europa se han centrado fundamentalmente en la promoción de la industria europea de procesamiento de datos, con el objeto último de adjudicarle competitividad internacional. En cambio, el Parlamento Europeo ha focalizado su atención en la salvaguarda de los derechos individuales. A aproximadamente un cuarto de siglo desde que estas normas entraron en vigor, puede decirse que muchos de sus principios conservan vigencia, pero que el desarrollo indetenible de las TIC obliga a replantearse algunos de sus conceptos. En esta sentido, se han promulgado sucesivas Directivas. Un análisis

profundo del problema hace pensar que trasciende el ámbito legislativo.

Este régimen jurídico toma en consideración la realidad de la globalización, por ejemplo, para autorizar la transferencia de datos personales a países terceros, la Directiva 95/46/ del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, exige la garantía de un nivel de protección adecuado y el cumplimiento de todas las disposiciones del Derecho Nacional, adoptadas de acuerdo con la misma Directiva (capítulo IV, artículo 25). Como *norma general*, para el movimiento internacional de datos, la LOPD española exige un nivel de protección equiparable a la que ella misma asegura (Título V, artículo 33).

En el plano global rigen los principios adoptados por la ONU, y con ciertas limitaciones, las reglas establecidas por la Organización para la Cooperación Económica y el Desarrollo (OCDE). La problemática comienza a esbozarse en la Proclama de Teherán, aprobada por la Conferencia Internacional de Derechos Humanos el 13 de mayo de 1968. En 1980 encontramos la *Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronteras de datos personales* (OCDE, 1980). En 1990, la Asamblea General de la ONU adopta una serie de principios rectores para la reglamentación de los archivos computarizados de datos personales.

Entre las leyes pioneras, además de las germánicas, podemos mencionar la *Data Lag* sueca de 1973, la *Loi relative à l'infomatique, aux fichiers et aux libertés* francesa de 1978, la leyes de Austria, Dinamarca y Noruega del mismo año, y la *Data and Computer Proccesing Act* dictada por Luxemburgo en 1979.

Luego del hito que significó el Convenio Europeo de 1981, fueran adoptadas otras normas nacionales, por ejemplo, la *Data Protection Act* inglesa de 1984, la ley 10/91 portuguesa, la *LORTAD* hispánica de 1992 y la *Legge di tutela delle persone e di altri soggetti*

rispetto al trattamento dei dati personali de 1996. Además, se establecieron algunos acuerdos internacionales, dentro de los cuales despunta el *Acuerdo de Schengen*, del 14 de junio de 1985, relativo a la supresión gradual de los controles en las fronteras comunes. Este acuerdo fue desarrollado por un Convenio de Aplicación de 142 artículos firmado en dicha localidad luxemburguesa en junio de 1990. Como contrapartida de la supresión aludida se creó una gran base de datos policiales, el Sistema de Información Schengen o SIS. Su finalidad original era el control de las personas *indeseables* o *inadmisibles*.

En el plano judicial, cabe citar también como un hito el reconocimiento del *derecho a la autodeterminación informativa,* por parte del Tribunal Constitucional Alemán de Karlsruhe en la sentencia del 15 de diciembre 1983 sobre la ley de censo de la población, que discutió su constitucionalidad y sirvió de precedente a nurnerosos fallos y normas posteriores. El decreto confirió un poder jurídico a los individuos para disponer de la información personal y su utilización en todas las fases de elaboración y uso.

En los Estados Unidos no existe una ley de carácter general que regule la protección de datos personales. Por el contrario, existen normas específicas para determinados sectores y asuntos concretos. La ley sobre libertad de información *(Freedom Information Act),* sancionada en 1966, establece que la información contenida en los documentos públicos es de libre acceso al pueblo estadounidense. Esta ley se aplica exclusivamente a las informaciones en poder de la administración pública. El *Fair Reporting Act* de 1970 protege al cliente de las compañías de crédito contra la violación de su privacidad por parte de las agencias de información, independientemente del método empleado para su registro. La ley de protección de la vida privada, *Privacy Act*, de 1974, otorga a todo ciudadano su derecho a la privacidad y se aplica a las informaciones referidas a personas físicas, contenidas en registros manuales y automáticos del gobierno federal. Desde ese entonces, diez Estados Federados han adoptado disposiciones normativas

sobre protección de datos, sin que ninguno contemple disposiciones legales que cubran al sector público y al privado. Por otra parte, los Estados Unidos carece de una institución especializada en la vigilancia y aplicación de estas normas, a diferencia de lo que ocurre en Europa.

En relación a las democracias europeas, los Estados Unidos de Norteamérica se distingue por su falta de protección en este campo:

"Data protection is an important part of European human rights law. But with slight exceptions, it is not an important part of our tradition..." (Lessig, 1999).

Esta disparidad jurídica ha traído varios problemas para el intercambio comercial intercontinental y el flujo de datos transfronteras.

Las disposiciones del *Convenio 108* del Consejo de Europa de 1981, si bien en principio solo cubren los datos de carácter personal de personas físicas, en el artículo 3º 2-b, permite a las partes contratantes extender la aplicación de la Convención a datos relativos a las personas jurídicas. Algunos países europeos como España, Alemania, Francia, Irlanda, entre otros, han excluido expresamente dicha titularidad. En cambio, otros como Austria, Dinamarca, Islandia, Luxemburgo, Noruega y Suiza, han aprobado leyes de protección de datos que extienden su campo de aplicación a las personas jurídicas. El problema de la atribución o no del derecho a la intimidad a las personas jurídicas, es *resuelto* por Puccineli de manera salomónica:

"Sea como fuere, si bien la adjudicación de la intimidad a las personas jurídicas es un tema muy discutible, el problema planteado simplemente desaparece si cambiamos de punto de vista, dejando de considerar al nuevo derecho como un mero desprendimiento o apéndice de la privacidad". (Op Cit: 95).

No obstante, no cabría aplicar aquí la estrategia del avestruz; la doctrina le adjudica al derecho a la intimidad el carácter de fuente inmediata a la protección de datos. De hecho, tal como lo reconoce el mismo autor, la intimidad ha sido el punto de arranque para la configuración del derecho de protección datos de las personas físicas (Puccineli, 1999: 89). En este sentido, cabe discutir mínimamente su evolución a través del tiempo.

Intimidad y privacidad informática

Puede establecerse un paralelismo entre el concepto liberal clásico de libertad (Locke, Mill, Constant) y la noción de intimidad, y entre el concepto liberal contemporáneo de libertad y la categoría de privacidad informática. El primer concepto es *negativo* y alude a la no interferencia de otros, en particular, la no injerencia estatal. En esta línea de ideas, cuanto más amplia es el área de no interferencia, más amplia es la libertad. Esta noción de libertad está en el origen de los derechos civiles. En 1873, el juez estadounidense Thomas Cooley, en su obra, *The Elements of Torts*, acuñó una frase para aludir a la intimidad, que se corresponde con esa noción de libertad: *the right to be let alone*, es decir, tener derecho a ser dejado en paz, a ser dejado solo. No obstante, los abogados Brandeis y Warren fueron quienes le dieron mayor proyección al concepto.

En las postrimerías del siglo XIX, la familia de un joven abogado y empresario de Boston, Samuel D. Warren, recibió determinados comentarios de la prensa local que incluían referencias desagradables de índole personal, relacionadas con las fiestas y eventos sociales que celebraba su esposa. Mr. Warren, afectado, acudió a su compañero de estudios en Harvard, Louis D. Brandeis, con el objeto de publicar conjuntamente un artículo titulado *The right of privacy*, en la Harvard Law Review (1890) que poco después comenzó a emplearse por los tribunales norteamericanos para proclamar este derecho. Dichos autores pretendían establecer un límite jurídico que vedase las intromisiones de la prensa en la vida

privada. En 1952, la famosa frase aludida quedó plasmada en una sentencia firmada por el juez William Douglas. Más tarde, en 1965, la decisión del Tribunal Supremo, en Connecticut, invalidó una ley que prohibía el uso de anticonceptivos, incluso a las parejas casadas. La instancia dictaminó que la relación matrimonial es *íntima hasta el extremo de ser sagrada*.

En contraposición a la noción tradicional, el concepto liberal moderno de libertad es positivo y quiere significar autonomía y autodominio. Esta vez se trata de libertad de intervención o libertad de participación, conceptos que están en la base de los derechos políticos. El hombre sería su propio dueño y sus decisiones deberían depender de sí mismo y no de fuerzas externas. Como diría Kant:

"Libertad es obediencia, pero obediencia a una ley que prescribimos nosotros mismos". (Citado por Macedo, 01:2).

A la discusión sobre los límites de esta concepción de la libertad y del hombre (atomizado, individualista y racional) no nos detendremos aquí. Únicamente nos interesa destacar que el concepto de privacidad informática se adecua a estas premisas. Dicha categoría alude a la capacidad de gestión y decisión que tienen los individuos sobre los datos que le conciernen. Aquí no se considera solo al Estado, sino también a las corporaciones privadas, como virtuales *invasores*. No solo se configura un NO a las interferencias extrañas; se trata de preservar la identidad y libertad frente al intenso e invisible poder informático.

En la actualidad, el derecho a la intimidad (o privacidad, más propiamente) conserva el núcleo original de libertad negativa o status libertatis, pero absorbe la dimensión de autodeterminación de la persona. No se trata únicamente de negar información sobre sí mismo, sino también del derecho a pretenderla. Al controlar la información que nos concierne, preservamos nuestra propia identidad, nuestra dignidad y libertad (Murillo, citado por Puccineli, 1999: 96).

La libertad informática tutela el acceso, conocimiento, control y disposición de datos personales, concepto que es homologable a la categoría germana de derecho a la autodeterminación informática.

La noción tradicional de intimidad está ligada al espacio, especialmente al oikos griego. De hecho, sus primeras manifestaciones se remontan a la Edad Media, como el derecho a la inviolabilidad del domicilio. Si bien nació jurídicamente a finales del siglo XIX, se trata de un concepto eminentemente antropológico. Existen distancias espaciales mínimas que protegen al individuo y que difieren de una cultura a otra (Hall, citado por GSI. 01:2). Esa burbuja personal ha sido agujereada por la irrupción de las tecnologías de la información y la comunicación. Por ello, la privacidad no se define tomando en cuenta el concepto físico de espacio:

"La intimidad (intimus) responde a la idea de lo más interno o recóndito de la interioridad de la persona. Es lo que pertenece exclusivamente, como secreto o reservado y que se manifiesta, incluso como un derecho a la soledad (ius solitudinis) o a ser dejador tranquilo (to be left alone)". (Puccineli, 1999: 205).

De manera independiente, el derecho a la intimidad aparece enunciado de forma expresa en los textos constitucionales solo en fechas muy recientes. La Constitución portuguesa de 1976 (artículo 26.1) es pionera en este sentido. Posteriormente, la Constitución española lo incorpora en su artículo 18.

Como derecho humano fundamental y universal, ha sido reconocido en:

- El artículo 12 de la *Declaración Universal de Derechos Humanos* de las Naciones Unidas de 1948.
- El artículo 8 del *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales* de 1950.
- El artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos*. (¿?)

- El artículo 16 de la *Convención Internacional sobre los Derechos del Niño* de la ONU en 1989.
- Los artículos 9 y 10 de la *Declaración Americana de Derechos Humanos.*
- Los artículos 11.2 y 11.3 del *Pacto de San José de Costa Rica.*
- Los artículos 6.2 y 11.2 de la *Declaración de los Derechos y Libertades Fundamentales,* aprobada por el Parlamento Europeo en 1989.

El Habeas Data y la redefinición del concepto de privacidad

Existen dos versiones principales de habeas data: aquella que pretende garantizar el acceso a la información pública o habeas data impropio, y aquella que otorga garantía procesal al derecho a la autodeterminación informativa o habeas data propio. Nuestro interés se centra en este último. De hecho, la posición predominante -y la que diera origen al instituto- se relaciona solo con los datos nominativos, y tiende a la protección de los derechos de las personas que pudieran ser vulnerados por el tratamiento de tales informaciones.

El respeto de los nuevos derechos ciudadanos constituye el nuevo *habeas data (o habeas scriptum)*, correspondiente al antiguo *habeas corpus;* del respeto debido a la integridad y libertad de la persona:

"El habeas data constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de la primera generación correspondió el habeas corpus respecto a la libertad física o de movimientos de la persona". (Pérez Luño, citado por Puccinelli, 1999: 210).

El habeas data propio tutela, al menos, el derecho a la autodeterminación informativa y todo el conjunto de principios

(igualdad, dignidad, libertad) y derechos (por ejemplo, honor, reputación, intimidad, imagen), que podrían ser vulnerados por el tratamiento de la información nominativa.

Según el autor citado, al cotejar ambas habeas, se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica:

"En ambos casos no se trata de derechos fundamentales, strictto sensu, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del habeas corpus, y de la libertad informática en lo concerniente al habeas data". (Puccineli, 1999: 214).

Así, mientras el habeas corpus se circunscribe a la dimensión física y externa de la libertad, el habeas data protege prioritariamente aspectos internos de la libertad: la identidad de la persona, su autodeterminación y su intimidad. Ambas habeas protegen distintas esferas.

Con la denominada libertad informática, ha habido una redefinición de la *privacy*, en donde ya no se trata simplemente de negar información sobre los datos personales y privados, con el objeto de salvaguardar la intimidad, sino también y sobre todo, garantizar la libertad de controlar el uso de los propios datos insertos en un archivo informático:

"La acepción positiva de la libertad informática lleva implícito el reconocimiento del derecho a conocer, corregir, cancelar o añadir datos en una ficha personal contenida en un registro informático. En consecuencia, supone el derecho de acceso a los bancos de datos, derecho de control de su exactitud, derecho de puesta al día y de rectificación, derecho de secreto para los datos sensibles, o derecho de autorización para su difusión". (Abad, 1993: 129-130).

En suma, el acceso es el presupuesto para el ejercicio de los demás derechos, que suponen operaciones, borrado, inclusión,

actualización, rectificación, disociación, impugnación de decisiones automatizadas y de diseño de perfiles virtuales, entre otras.

La defensa de la privacidad se presenta ahora como protección ante una posible arbitrariedad, y la existencia de informaciones cuyo potencial valor discriminatorio es relativo, histórico y no absoluto. Por ejemplo, en nuestra sociedad, algunas informaciones sobre el estado de salud que revelan disminución de la capacidad laboral o informaciones que indiquen posibles *desviaciones* de la norma: enfermedades mentales, enfermedades venéreas, hábitos sexuales, uso de la droga, abortos, entre otras.

Si bien a nosotros nos interesa resaltar aquí la expropiación de informaciones a que son sometidos los sujetos en su vida cotidiana, algunos autores apuntan también a aquella que se da en las llamadas instituciones totales (hospitales, ejército, cárceles, manicomios, etc.). Como casos extremo, algunos señalan la expropiación a que son sometidos los individuos sujetados a dichas instituciones:

"Muchas veces se ha subrayado cómo la imposibilidad para un paciente de poder ver, y sobre todo, comprender, su cartilla clínica es fuente de alienación y de sujeción al poder de la institución". (Manacorda, 1982:166).

Ante esta situación, plantean como primera garantía la libre circulación de la información entre las instituciones y los sujetos institucionalizados.

En indoiberoamérica, la defensa de los derechos de los registrados reviste un carácter marcadamente judicial. No deja de sorprender la exuberancia de tipos y subtipos de habeas data, establecidos por Puccineli (1999:220-225): informativo, aditivo (actualizador), rectificador o correctivo, reservador, exclusorio o cancelatorio, impugnativo, bloqueador, disociador, asegurador y reparador. En los años finales de la década de los ochenta se prepararon los primeros proyectos de ley que incluían la categoría

de habeas data en sus diversos tipos y subtipos. El habeas data aparece regulado en la región, a veces como derecho y a veces, dado su carácter instrumental, como acción o garantía constitucional. En realidad, no existe consenso normativo, respecto a la naturaleza jurídica del habeas data.

Es certera la afirmación de Vanossi en el sentido de que:

"si al habeas data se lo convierte en un mecanismo complejo, demasiado sofisticado y demasiado articulado, no va a ser captado y entendido por los propios interesados, es decir, por los ciudadanos.... (entre los cuales me incluyo) que van a encontrar dificultades en el acceso mismo para aducirlo y utilizarlo como herramienta protectora..." (Citado por Puccineli, 1999:225).

Para una mejor comprensión de la problemática tratada, cabe describir ahora el marco legal en el cual se inscriben los nuevos derechos aludidos. Para Manuel Heredero Higueras (1993), el régimen jurídico de la protección de datos está constituido por dos grandes órdenes de temas:

1. los principios
2. las garantías del interesado (derechos de los registrados).

Los principios del régimen jurídico de la protección de datos personales

El principio de calidad de los datos; limita el tipo de datos que pueden ser recogidos y registrados en los archivos y los condiciona a unos objetivos determinados. Este principio a veces se denomina principio de licitud de los datos y establece que debe existir un propósito socialmente aceptado que legitime su extracción.

El principio de finalidad; limita el uso de los datos recogidos y registrados a unos determinados y exclusivos fines. Por ejemplo, la ley francesa de Informática y libertades incorpora la noción de *desviación de finalidad*.

El principio de seguridad de los datos; se refiere a la seguridad de la información recabada, que genéricamente debe ser física y lógica y, concretamente, establece restricciones al acceso a los datos y previene la alteración de los mismos. Los datos deben protegerse contra la destrucción accidental o no autorizada o la pérdida incidental, así como contra el acceso, modificación o difusión no autorizados. (v.g. artículo 7 del Convenio 108 del Consejo de Europa).

El principio de conservación limitada de los datos; y la consiguiente supresión de los que hubieran dejado de ser necesarios. El derecho al olvido es propio de la libertad informática.

El principio del consentimiento del afectado; el registrado dará o no su aprobación (*libremente*) para que se proceda al tratamiento automatizado de datos nominativos (artículo 6, Título II de la LOPD). Este principio ha sido en gran medida socavado por el desarrollo de la red de redes, en donde se sustraen datos de las operaciones de los internautas, sin que ellos se percaten de ello. En Internet existen herramientas que permiten el tratamiento invisible de la información mediante la creación de archivos ocultos (cookies). De hecho:

"El derecho a decidir si una determinada información debe o no debe ser transmitida, va desapareciendo progresivamente a medida que avanzan las tecnologías de la información". (Campuzano, 2000: 57).

Por otra parte, los ciudadanos, en tanto consumidores, pueden dar el consentimiento presionados o seducidos por recibir una determinada contraprestación, cuestión que deberían considerar las leyes de protección de datos.

El principio de la fidelidad de la información; los datos deben ser completos, exactos y actuales.

El juego de todos los principios enunciados anteriormente conforma un *megaprincipio*:

El principio de la autodeterminación informativa; es la facultad que tiene toda persona para ejercer control sobre la información que le concierne. Atribuye al titular del dato una serie de derechos, en aras de permitirle autotutelar su propia identidad.

Los derechos de los registrados en el régimen jurídico de la protección de datos personales.

La legislación establece derechos básicos de las personas para la protección efectiva de los datos nominativos. Nosotros enumeraremos, más o menos exhaustivamente, estos derechos de los registrados:

Derecho de acceso; el afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados.

A partir de haber accedido al conocimiento de los datos personales, y de quién y para qué los tiene registrados, el titular puede ser autorizado, en ciertas circunstancias, a realizar determinadas operaciones sobre ellos.

Derecho de rectificación; los datos de carácter personal que resulten inexactos o incompletos podrán ser rectificados. El derecho a rectificar puede incluir una serie de operaciones, a saber: corregir, actualizar, aclarar y agregar o completar.

Derecho de cancelación; se puede estipular que un registro no deba contener ciertos datos, y por ende, corresponda cancelarlos.

Derecho a la oposición al tratamiento; la pretensión exclutoria se ejerce antes de que se hayan registrado los datos.

Derecho de impugnación a la valoración de datos; el ciudadano podrá impugnar los actos administrativos o decisiones privadas que impliquen valoración de su conducta, cuya única base sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Derecho de inclusión; en ocasiones se torna necesario incluir a una persona en un registro para acceder a ciertos beneficios (por ejemplo, prestaciones sociales).

Derecho de bloqueo; establece que el dato debe mantenerse en el registro sin la posibilidad de tratamiento alguno.

Derecho de disociación; consiste en la eliminación de toda referencia que pueda permitir la individualización de la persona a la que pertenecen los datos (v.gr. datos que se usan en estadística o investigación).

Derecho al olvido o a la caducidad del dato negativo; ciertas legislaciones establecen plazos para la conservación de ciertos datos negativos.

Derecho a la seguridad de los datos; se deben establecer mecanismos de seguridad que impidan el acceso a personas no autorizadas; tratamientos contra legem o transferencias indiscriminadas de datos.

Derecho a la tutela efectiva (judicial y administrativa); el Estado debe establecer normas protectoras y recursos y vías judiciales que neutralicen los actos que pretendan negar injustificadamente el ejercicio de los derechos concedidos.

Derecho a la gratuidad de los procedimientos; el registrado debe tener el derecho a obtener la información recabada sin demoras ni gastos excesivos. Las gestiones ante la autoridad de registro y

control, o ante las instancias judiciales (que podrán ser o no ser específicas) no deben ser onerosas, para que el ejercicio de los derechos de los registrados no se torne ilusorio.

Derecho a indemnización; los interesados que, como consecuencia del incumplimiento de lo dispuesto en la Ley, sufran daño o lesión en sus bienes o garantías tendrán derecho a ser indemnizados por el responsable o el encargado del tratamiento (artículo 19, Título III de la *LOPD).*

Para finalizar las referencias jurídicas internacionales, cabría comentar brevemente la legislación española ad hoc, que sigue los lineamientos fundamentales de los organismos competentes de la Unión Europea y sobre la cual poseemos mayor documentación directa e indirecta.

El caso español: *LOPD 99*

Como desarrollo legislativo del artículo 18 de la Constitución Española de 1978, casi tres lustros después, concretamente en 1992, sanciona una ley específica, conocida como *LORTAD.* España había ratificado el convenio 108 del Consejo de Europa el 27 de enero de 1984 y lo hizo entrar en vigor el 1 de octubre de 1985. Desde fines de los años setenta y en los años ochenta, podemos contabilizar aproximadamente seis leyes que tocan tópicos correlacionados y que pueden considerarse antecedentes indirectos. (Ambrosio. 2000). La *Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD*, BOE, núm. 262, de 31 de octubre de 1992), ordenará inicialmente esta materia en el país ibérico. El Consejo de Europa había reiterado el año anterior su diagnóstico sobre la escasa protección de los datos personales en ese país.

La *LORTAD* dio origen a un desarrollo normativo, entre lo que cabe resaltar:

- *Real Decreto* 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre.

- *Resolución de 22 de junio de 1994,* de la Agencia de Protección de Datos, por la que se aprueban los modelo normalizados en soporte papel y magnético a través de los que deben efectuarse las correspondientes inscripciones en el Registro General de Protección de Datos.

- *Instrucción 1/1995,* del primero de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

- *Instrucción 1/1996,* del primero de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

- *Instrucciones 1/1998,* de 19 de enero, de la Agencia de Protección de Datos relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

- *Ley 5/1998,* de 6 de marzo, de incorporación al Derecho Español de la *Directiva 96/9/CE,* del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

- *Orden del 31 de julio de 1998*, por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. (Ambrosio, 2000).

El 13 de diciembre de 1999, es decir, siete años después, se promulga la *Ley Orgánica de Protección de Datos de Carácter Personal (LOPD),* que modifica artículos de leyes preexistentes y deroga a la *LORTAD 92.* Como disposición final primera habilita al

gobierno para aprobar o modificar las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la ley. En cuanto a su ámbito de aplicación, se puede decir que tiene mayores pretensiones que la anterior, porque protege la información concerniente a personas físicas en *cualquier* clase de archivo y tipo de tratamiento de datos, automatizado o no.

En la legislación española en esta materia podemos mencionar también el *Real Decreto 994/1999,* del 11 de junio, por el cual se aprueba el *Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.* El citado reglamento establece una trilogía de niveles de protección (básico, medio y alto), en función de los cuales se estipulan medidas de seguridad correlativas.

En la *LOPD* se definen las nociones básicas de este campo específico de la jurisprudencia, y se exponen los principios de la protección de datos, los derechos de las personas y las disposiciones sectoriales para los archivos de titularidad pública y privada. De acuerdo con las Directivas regionales, esta ley establece una autoridad pública de control, que en principio actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones (Título VI, artículo 35). Es la denominada *Agencia de Protección de Datos*, que vigila en España la aplicación de las disposiciones adoptadas. Así mismo, se define el régimen jurídico de la Agencia, el papel de su director, sus funciones y el Registro General de Protección de Datos, en tanto órgano integrado en este ente de Derecho Público.

La *LOPD* establece una tipología de infracciones (leves, graves y muy graves) y una serie de sanciones administrativas correlativas (multas de 100 mil a 100 millones de pesetas). "La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas

interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de carácter antijurídico y de culpabilidad presentes en la concreta actuación infractora". (Título VII, artículo 45).

En la *LOPD* se amplia el ámbito de aplicación (datos automatizados o manuales) y se añade el derecho de oposición a los anteriores derechos de acceso, rectificación, cancelación. Quizá podamos decir que este derecho de oposición al tratamiento de los datos personales o a la aparición en una base de datos estaba *implícito* en la ley anterior. El consentimiento del afectado, necesario para el tratamiento de sus datos personales (artículo 6), tiene un carácter revocable (artículo 11).

Con consecuencias sociológicas y humanitarias positivas, se establece como derecho de la persona (Título III) la impugnación de los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal y que en esa medida ofrezca una definición de sus características o personalidad (artículo 13. Impugnación de las valoraciones).

Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias, de acuerdo con el artículo 7 de la *LOPD,* y con lo establecido en el apartado 2 del artículo 16 de la Constitución. Para el tratamiento de estos datos y aquellos otros que revelen su afiliación sindical, se requerirá el consentimiento expreso del afectado. Estos datos se consideran especialmente protegidos:

"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".

Ahora bien, a pesar de que la citada ley, al igual que *LORTAD 92*, instauraron en el país ibérico un sistema cautelar y preventivo

erigido sobre los derechos de acceso, rectificación, cancelación y oposición de los datos, su contenido ha sido objeto de múltiples críticas. Para Valentín Carrascosa López, la antigua *Ley Orgánica de Regulación del Tratamiento automatizado de los Datos de Carácter Personal (LORTAD 92)* presentaba muchos puntos negros tales como:

"Vulneración del espíritu y letra de la Constitución. Excepciones injustificadas y no controladas de aplicabilidad. Dependencia del ejecutivo del director de la Agencia de Protección de Datos. Inexistencia de responsabilidades civiles y penales, ya que el proyecto contempla solamente sanciones administrativas. Desajuste respecto a la legislación comparada". (Carrascosa, 1993: 98).

La *LOPD* vigente, con ajustes evolutivos importantes, hereda algunas falencias y no se ha salvado de cuestionamientos. A pesar de que España tiene en este campo una de las legislaciones internacionales más duras y ambiciosas, las estadísticas, si bien no del todo fiables, indican que la *LOPD* se cumple en menos del 10 por ciento. La ley impone unas obligaciones legales y técnicas casi imposibles de observar por la gran mayoría de las empresas, lo cual desmotiva a quienes intentan cumplirla (Blasco. 2002). A esto se agrega que el contenido de la ley está lejos de ser conocido por la mayoría de la sociedad española (Vnunet, es, 2003).

Además de las amplias posibilidades que se han abierto en distintos ámbitos de actividad, el desarrollo de Internet ha evidenciado también vulnerabilidades y fallas de seguridad importantes. La normativa referida al flujo de datos transfronteras contenida en la *LOPD* y las garantías que se pretenden, se ha enfrentado con problemas jurídicos de aplicación. En general, las obligaciones y requerimientos legales que se establecen no se ajustan adecuadamente al tratamiento de datos a través de Internet (Prenafeta, 2000). Por ejemplo, la Agencia de Protección de Datos, en su interpretación de la LOPD, considera que la difusión de datos a través de la red de redes constituye una cesión de datos, en la medida en que implican la comunicación de datos a una pluralidad -

indefinida- de personas distintas al interesado. Por otro lado, la prestación del consentimiento puede presentar problemas, debido a la dificultad de identificar inequívocamente a quien responde afirmativamente, así como las dudas que existen en cuanto al valor jurídico de estas acciones. La misma agencia considera que las direcciones de correo electrónico son datos de carácter personal, pero es común que los mismos usuarios las divulguen sin cortapisas.

Los datos sobre foros y listas de correo, a saber, opiniones, preferencias o inquietudes, pueden rastrearse con el uso de herramientas de búsqueda, almacenarse en servidores Web durante varios años y constituir así la materia prima para la conformación de perfiles. En este sentido, diversos organismos en la especialidad recomiendan preservar el anonimato en la red:

"Tanto la Agencia de Protección de Datos como otros organismos, como el Consejo de Europa, el International Working Group on Data Protection in Telecommunications o el Grupo de Trabajo sobre Protección de Datos de la UE aconsejan ser conscientes de que las opiniones vertidas en dichos foros y listas son públicas y pueden ser malinterpretadas". (Prenafeta, 2002).

En general, en Europa ciertos analistas han argüido que el cumplimiento de las obligaciones de registro por parte de las autoridades de control son puestas en práctica de manera ineficiente. El problema es tan peliagudo que en España algunos se aventuran a proponer una *LOPD* de plástico, es decir, la emisión de varios documentos de identidad para cada ciudadano, de manera que se impida el cruce de datos por parte de las entidades públicas y privadas. Únicamente el Ministerio del Interior y el de Hacienda tendrían bases de datos completas con todos los números de cada individuo, lo que garantizaría el cumplimiento de las funciones típicas del Estado Moderno (coerción física y tributación).

Si todos tenemos un documento identificador único, la *LORTAD* y su sucesora, la *LOPD,* son papel mojado, puesto que es muy fácil

cruzar los datos de todos los ciudadanos, y dado que es un delito que se practica en la intimidad (al revés que el atraco a mano armada o el libelo, cuyas víctimas son también sus testigos), es difícil de perseguir. La emisión de tantos documentos de identidad como solicitara cada ciudadano serviría para *plastificar* la ley, y hacerla impermeable a los ataques del primer desaprensivo con una base de datos y algo de tiempo libre. (Candeira, 2000).

Con más seriedad, coincidimos con Reidenberg (1999) en que las dificultades para implementar estas leyes en los servicios de información on line plantean importantes desafíos para la efectiva protección de la privacidad. En realidad, la protección de los ciudadanos requiere de una combinación de reglas y tecnología y de una política legal que ofrezca incentivos al desarrollo expedito y ágil de tecnologías protectoras de la privacidad, que hasta ahora ha sido lenta, tímida y problemática. Un ejemplo de esto es la *Platform for Privacy Preferences,* conocida como *P3P* desde 1996 y desarrollada por el World Web Consortium, organización dedicada a la creación de estándares en Internet. Este protocolo faculta a los usuarios para obtener información acerca de las prácticas de privacidad de los sitios Web y les permite decidir si proveen o no sus datos personales. Existe disponibilidad de tecnologías protectoras de la privacidad, pero la industria ha demostrado letargo en su desarrollo.

El caso venezolano

En general, en Latinoamérica no encontramos una legislación específica y pertinente de protección de datos personales, ni la regulación inicial de los ficheros, ni la especificación de mecanismos que permitan a los responsables de los mismos adoptar las medidas pertinentes para garantizar la protección de los derechos. Ante las carencias presupuestarias, no existen órganos especializados en aplicar la normativa, sino el redimensionamiento inadecuado de las entidades judiciales existentes. No hay claridad en la definición

de las nociones básicas ni tampoco autoridades públicas de control. En algunas ocasiones, el Habeas Data latinoamericano mejora a la correspondiente figura europea, en otras oportunidades, podría implicar su estancamiento e inaplicabilidad (Castro. 2003). El caso venezolano es uno de los más pobres a pesar de habérsele dado al habeas data un claro rango constitucional.

Hasta 1961, las constituciones venezolanas consagraron en menor o mayor medida el derecho a la privacidad en su sentido tradicional, vale decir, procuraban resguardar el honor, la imagen y el honor del ciudadano, y establecían el secreto en relación a lo doméstico y a la correspondencia. En la Constitución de 1821 se instaura con rango constitucional, por vez primera, la inviolabilidad de la correspondencia privada y los papeles particulares. La Constitución de 1857 consagra la protección e inviolabilidad de todo tipo de correspondencia. La Constitución de 1858 hace alusión al término vida privada. Los principios anteriores se mantuvieron vigentes en las constituciones posteriores. La Constitución de 1914 amplía el ámbito de acción normativa por cuanto incluyó la correspondencia telegráfica.

La Constitución de 1961 establece en su artículo 59 el derecho a la vida privada: "Toda persona tiene derecho a ser protegida contra los perjuicios a su honor, reputación o vida privada". En el artículo 63 se consagra el principio de la inviolabilidad de la correspondencia:

"Así pues, el constituyente de 1961 consagró expresamente el derecho de cualquier persona a ser protegida contra intrusiones o invasiones a su esfera privada (derecho a la privacidad)". (Peñaranda, 01: 198).

En la sentencia de fecha 14/08/98, que reitera la sentencia del 20 de enero de 1998, la Sala Político Administrativa de la Corte Suprema de Justicia reconoce el derecho a la privacidad a los enfermos de SIDA, con la finalidad de proteger sus identidades y evitarles rechazos y estigmatizaciones.

A pesar del avance de las nuevas tecnologías, Venezuela se mantuvo por mucho tiempo sin una ley que protegiera los datos personales almacenados en dispositivos informáticos. Paradójicamente, la salvaguarda de los derechos ciudadanos, constituía el tercer lineamiento de la política informática estatal, establecida por la Oficina Central de Estadística e Informática (OCEI), el antiguo organismo oficial sectorial con competencias en el sector.

Sobre la base del artículo 59 de la Constitución de 1961, el 16 de diciembre de 1991 entra en vigencia *la Ley sobre Protección de la Privacidad de las Comunicaciones,* que desarrolla los principios de la anterior carta magna en materia de protección de privacidad. Dicha ley tipifica como delitos la grabación, la interrupción y la obstrucción de una comunicación, valiéndose de cualquier medio, en especial, de las nuevas tecnologías. Se trata de la protección del *secreto* de las comunicaciones y de la privacidad, entendida esta última en el sentido tradicional, vale decir, aquella que tiene que ver con *el honor, la imagen y la reputación*. Las injerencias podrían definirse como el conocimiento, la difusión, el acoso o la investigación indiscreta de la vida privada. Como vemos, dicho instrumento jurídico protegía la intimidad siguiendo la noción clásica, pero no salvaguardaba la privacidad en su concepción más moderna. El sentido de esta ley fue resumido por el siguiente titular: "intervenir un fax o un teléfono es como abrir una carta ajena".

En esta materia, la Constitución de la denominada República Bolivariana de Venezuela de 1999, desarrolla grandes avances, al menos en el papel. De la inviolabilidad del hogar doméstico habla el artículo 47, y de la inviolabilidad de las comunicaciones, reza el artículo 48 (Título III, de los Deberes, Derechos Humanos y Garantías, Capítulo III, de los Derechos Civiles). No obstante, hasta aquí no hay sino un desarrollo de lo contenido en constituciones anteriores. Por el contrario, el artículo 60, liga novedosamente el honor y la privacidad en general con la libertad informática, que es un derecho de tercera generación:

"Toda persona tiene Derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus Derechos".

Como un hito se puede mencionar también la inclusión del habeas data como mecanismo judicial, en el artículo 28 (Capítulo I, Título III):

"Toda persona tiene Derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus Derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".

Entonces, el habeas data se constituye en el medio judicial que el titular interpone ante los tribunales para la debida protección de sus datos personales. Aquí se recoge la tendencia europea de protección de datos, en la que no se establecen distinciones entre archivos automatizados o no, públicos o privados, lo cual amplia la esfera resguardada.

"En cuanto a los requisitos de fondo y de forma para interponer el habeas data ante los tribunales competentes, como del procedimiento judicial, el Constituyente omitió en el artículo 28 reservar estos aspectos a la ley..." (Peñaranda, 01:219).

Cuestión que la ley que posteriormente fue sancionada no logró resolver. Por otra parte, se establece el habeas data como único mecanismo de tutela de la libertad informática:

"Aunque hubiera sido mejor una redacción que contemplara también la tutela administrativa, como vía primaria ante los órganos administrativos y como vía secundaria, ante los jurisdiccionales, en caso de apelaciones de las decisiones formuladas por los primeros". (Op Cit: 220).

En Europa ha sido fundamental la creación de organismos especiales que custodian el tratamiento de los datos entre los Estados miembros y no miembros. Podemos decir que nuestro país ha seguido la tendencia latinoamericana de un desarrollo legislativo y jurisprudencial muy escaso.

En Venezuela no se ha formulado todavía una ley específica sobre la privacidad informática. No se puede decir que la *Ley especial contra los delitos informáticos,* de septiembre de 2001, sea un desarrollo pleno de los artículos 28 y 60 de la constitución vigente. Apenas un capítulo de esa ley está dedicado a la protección de datos de carácter personal, concretamente el capítulo III, intitulado "De los Delitos contra la privacidad de las personas y de las comunicaciones", y que incluye solo dos artículos alusivos al tema (20 y 22). El artículo 21 se refiere a la privacidad en el sentido tradicional, particularmente, a la privacidad de las comunicaciones:

"Artículo 20.- Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

"La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

"Artículo 21.- Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

"Artículo 22.- Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aun cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

"Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad".

Los delitos contra la privacidad constituyen apenas un tipo dentro de una taxonomía de delitos que parecen tener mayor prioridad, al menos por el orden y la cantidad de su articulado. El capítulo I incluye los delitos contra los sistemas que utilizan tecnologías de información (7 artículos). Los capítulos II y V incorporan los delitos contra la propiedad y contra el orden económico, respectivamente (9 artículos). El capítulo IV incluye los delitos contra niños o adolescentes (2 artículos). Como indicamos supra, no se explican los detalles de fondo y de forma para interponer el habeas data. El glosario inicial de términos está constituido por nociones técnicas del hardware y el software informático. Al contrario de otras leyes, no se explican los términos básicos de la protección de datos de carácter personal. No se establecen distinciones entre información personal, data privada en general y data sensible en particular. No se explicita el derecho de acceso, imprescindible para

ejercer los otros derechos. Tampoco se definen detalladamente los otros derechos básicos del registrado, incluidos en la Constitución vigente (actualización, rectificación, cancelación).

Esta jerarquía se explica en gran parte a que la Ley sobre los Delitos Informáticos surge dentro del marco del quinto eje de acción del Ministerio de Ciencia y Tecnología; *la economía digital*. Los otros ejes son: Capacitación, Desarrollo de Contenidos, Desarrollo de Conectividad y Gobierno Electrónico. De acuerdo con el quinto eje de acción, en febrero de 2001 fue promulgada la Ley de Firmas y Documentos Electrónicos, que tiene como meta otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico. Para Carlos Genatios, a la sazón, Ministro de Ciencia y Tecnología:

"Una vez promulgada la Ley de Firmas y Documentos Electrónicos, el paso siguiente corresponde al establecimiento de mecanismos que permitan luchar contra el delito cibernético..." (Prólogo del texto de Tablante, 01:12).

Este **marco economicista** explica el lugar secundario que ocupa la privacidad informática en la legislación. "Evita que la informática invada tu intimidad" es el lema de la Agencia de Protección de Datos española. Si es una meta difícil de lograr con una legislación de lo más novedosa y avanzada, ¿cuál será el diagnóstico para un país como Venezuela, con la situación jurídica precaria señalada anteriormente? No obstante, cabe recordar que la *solución* legal nunca será suficiente. La participación de los ciudadanos es crucial para el ejercicio de los nuevos derechos, y tiene que estar complementada con el desarrollo paralelo de tecnologías protectoras de la privacidad y su efectiva difusión.

Conceptos fundamentales

Datos personales. Son informaciones relativas a una persona física identificada o identificable, es decir, reconocible con facilidad, directa o indirectamente, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social u otra información similar.

Datos sensibles. Son aquellos que pueden perjudicar injustificadamente los derechos e intereses legítimos de ciertas personas. En principio, no son datos de interés colectivo, por ejemplo, el origen racial y étnico, las opiniones políticas, las convicciones religiosas o filosóficas, el estado de salud, afiliación sindical, vida sexual, etc.

Vida privada. Está conformada por las *actuaciones y relaciones de una persona al margen de su actividad profesional* (incluida la política) pública o privada.

Intimidad. Son los aspectos *más reservados* de la vida de la persona; su domicilio y sus comunicaciones.

Tratamiento de datos. Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, conservación, elaboración, modificación, bloqueo y cancelación, así como la cesión de datos.

Fichero de datos personales. Conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o distribuido de forma funcional o geográfica. La LOPD, dada la ampliación del ámbito de aplicación, define al fichero como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". (Artículo 3).

Responsable del fichero. Persona que decide sobre la finalidad, contenido y tipo de tratamiento de los datos.

Afectado o registrado. Persona cuyos datos son objeto de tratamiento automatizado.

Procedimiento de disociación. Todo tratamiento de datos personales en la cual la información obtenida no pueda asociarse a una persona determinada o determinable.

Encargado del tratamiento. Persona, autoridad pública u organismo que trata datos personales por cuenta del responsable del tratamiento.

Consentimiento del interesado. Toda expresión voluntaria, libre, inequívoca, específica e informada a través de la cual el afectado permite el tratamiento de datos personales que le conciernen

Cesión de datos. Toda comunicación de datos efectuada a una personada distinta del interesado.

Fuente: Datos del Estudio, Caracas, mayo 2003

Protección de los datos personales Fundamento Jurídico Europeo

Líneas directrices sobre la protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras. 23-09-1980. Consejo de la OCDE.

Recomendación No. 721 de 1980, relativa a la informática y protección de derechos del hombre. Consejo de Europa.

Recomendación No. 890 de 1980, relativa a la protección de datos de carácter personal. Consejo de Europa.

Convenio 108 del Consejo de Europa. 28-01-1981. Estrasburgo. Convenio para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal.

El Acuerdo de Shengen. 14-06-1985.

Recomendación No. 1037 de 1986, relativa a la protección de datos y la libertad de información. Consejo de Europa.

Recomendación No. R87, de 1987, sobre la utilización de datos de carácter personal en el sector judicial. Consejo de Europa.

Propuesta de Directiva de la Comunidad Europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos. 15-10-1992.

Directiva 95/46/CE relativa a "La protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los datos".

Directiva 96/9/CE sobre la protección jurídica de las bases de datos. 27-03-96.

Directiva 97/66/CE sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones. 15-12-1997.

Enmienda de la Convención ETS No. 108, para permitir el acceso a la Comunidad Europea, adoptada el 15 de junio de 1999. Consejo de Europa.

Protocolo adicional a la Convención ETS No. 108, sobre las Autoridades Supervisoras del Flujo de Datos Transfronteras. 08-11-2001.Consejo de Europa.

Directiva 2002/.../CE del Parlamento Europeo y del Consejo de Europa, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Diario Oficial C 113 E/39, de 14/05/2002.

Posición Común (CE) No. 26/2002 aprobada por el Consejo el 28 de enero de 2002 con vistas a la adopción de la Directiva 2002/ .../CE.

Fuente: Datos del Estudio, Caracas

Bibliografía

Abad, R. "Libertad informática y Nuevos Derechos. Una polémica legislación". En *TELOS*, Nº 33, 1993. Fundesco, Madrid, pp. 129-136.
"El Código Penal y la LORTAD. Variaciones terminológicas". En *TELOS*, Nº 47, 1996, Fundesco, Madrid, pp. 121-126.

Agree, P. y Rotenberg, M. (1997): *Technology and Privacy: The New Landscape*. Massachusetts, Massachusetts Institute of Technology Press..

Agudo, R. (1993): *La Reglamentación Legal de la Comunicación en Venezuela.* Caracas, Venezuela., Facultad de Humanidades y Educación de la U.C.V.

Alsius, S. "Accidente: atrapados entre el derecho a la información y el derecho a la intimidad". *Consell de l'Audiovisual de Catalunya*. 2000. Disponible en: [http://www.gencat.es/cac/estudis/c-alsius.htm]

Ambrosio, G. "Protección de datos de carácter personal" En ingenieroseninformatica.org. Disponible en: [http://www.ingenieroseninformatica.org/miscelanea/legislacion/esp/protecciondatos.php]

Araujo, J. (1999): *Derecho de las Telecomunicaciones.* Caracas, Venezuela. Universidad Católica del Táchira.

Azurmendi, A. (1999): *Derecho de la Información*. Euensa. Navarra, España.

Banisar, D. y otros. "Big Brother goes High-Tech". En *Coveraction Quartely,* 1997. Disponible en: [http://mediafilter.org/caq/CAQ56brother.html]

Blasco, J. "Hoy, 26.06.2002, es un día realmente importante para la protección de datos personales (al menos en teoría)" en *e-LegalBCN.com.* Disponibleen: [http://www.e-legalbcn.com/Articulos/Hoy %20 en% 20dia.htm]

Blejma, M. "Privacidad Privatizada. Nuevas formas de control social". 1997. Disponible en: [http://www.geocities.com/CollegePark/5025/privacidad.htm]
"La dictadura de la fibra óptica". Disponible en [http://www1.geocities.com/CollegePark/5025/dictadura].

Candeira, J. "La Lortad de plástico" en *BAQUÍA.COM*. 2000. Disponible en: [http://www.baquia.com/com/20001213/art00009.html]

Carlón, R "Los servicios de telecomunicación electrónica: un intento de aproximación jurídica". En la revista *ZER*, 1989, Gipuzkoa, servicio editorial de la Universidad del País Vasco, pp. 97-112.

Castro, A. "La protección del derecho a la intimidad en el tratamiento de datos personales: el caso de España y la nueva legislación latinoamericana". En *Alfa – Redi.* Revista de Derecho informático. Disponible en: [http://www.alfa-redi.org/areatematica/articulo.asp?idCategoria=38#]

Centre D' Investigació de la Comunicació (1993): *La protección de datos personales,* Monografías y Documentos # 8, Universitat Pompeu Frabra, Catalunya.

Colina C. "Telemática y control social", en *Anuario ININCO*, # 8, 1997. Universidad Central de Venezuela, Facultad de Humanidades y Educación, Caracas, Venezuela, pp. 151-164.
et al: "Cultura, comunicación, escritos para la CONSTITUYENTE". *Perspectivas Cosar,* Caracas, 1997, pp. 67-72.
"Comunicación, derechos y constituyente" en la Revista *COMUNICACIÓN,* Nº 106, Centro Gumilla, segundo trimestre 1999, pp. 28-31.

Dahbar, S. "Buen Vivir", *Diario El Nacional,* Caracas, Venezuela, 28 de noviembre, 1997, pp G-7

Elías, M. "Situación legal de los datos de carácter personal frente a las nuevas tecnologías. Estudio del impacto de las nuevas tecnologías en la privacidad y sus repercusiones jurídicas, económicas y sociales". En *Revista Electrónica de Derecho Informático* (REDI), 1997. Disponible en: [http://vlex.com.ar/revistas/doctrina/28]

Gorz, A. (1982): *Adiós al Proletariado.* Barcelona, España. . Ediciones 2001.

Grupo de Sistemas Inteligentes. S/título en la página Web del Departamento de Ingeniería de Sistemas Telemáticos (DIT) de la Universidad Politécnica de Madrid. Disponible en: [http://www.gsi.dit.upm.es/ fsaez/ miscelanea/pcweek031p.html]

Fisher, D. (1984): *El derecho a comunicar, hoy.* . París. UNESCO.

Forester, Tom (1992): *Sociedad de Alta Tecnología.* MÉXICO. Siglo Veintiuno editores.

Halloran J. "Entrevista sobre Comunicación y Democracia". En *Chasqui* Nº 7, CIESPAL, 1983. Quito, Ecuador, pp. 6-11

Heredero, M. "La protección de datos personales en manos de la policía: reflexiones sobre el convenio de Schengen". En Santiago Ripol i Carulla (Coord.): *La protección de los datos personales. Regulación nacional e internacional de la seguridad informática.* Centre de' Investigació de la Comunicació i Universitat Pompeu Fabra. Barcelona, 1993, España, pp. 30-47.

Lipovetsky, P. (1995): *La era del vacío.* Barcelona, España.. Anagrama. Colección Argumentos.

Lessig, L. Post, D. y Volokh, E. *CyberSpace Law.* Disponible en: [http:// www.ssm.com/update/lsn/cyberspace/csl_menu.html]
Social Science Electronic Publishing. Disponible en: [http:// www.ssm.com/update/isn/cyberspace/cs/-menu.html].

Loreti, D. (1995): *El derecho a la información. Relación entre medios, público y periodistas* Paidós. Buenos Aires.

Lyon, D. y Zureik, E. (1996). *Computers, Surveillance, and privacy.* University of Minnesota Press, Minneapolis, USA.

Macedo, R."Privacidad, mercado en información" en la *Biblioteca Jurídica Virtual.* Disponible en: [http://info.juridicas.unam.mx/publica/rev/cconst/cont/6/ard/ard6.htm] (Texto presentado en el Seminario del SELA de Teoría Constitucional y Política, Mar de Plata, Argentina, agosto de 1998).

Mancorda, P. (1982): *El ordenador del Capital.* H. Madrid, España. Blume Ediciones.

Marques de Melo, José. "Estado, sociedade civil e comunicacâo na América Latina". En *Comunicacâo & Sociedade* No. 12, 1984. Imprensa Metodista. Sâo Bernardo do Campo, pp. 97-102.

Ossandon, F.. "Democratización de las Comunicaciones". En *Chasqui* Nº 8, 1983. Comunicación Popular, CIESPAL. Quito, Ecuador, pp. 19-25.

Osset, M. (2000): *Ingeniería genética y derechos humanos.* Barcelona, España. Icaria.

Peáranda, H. (2001): *Iuscibernética: interrelación entre el Derecho y la Informática.* Maracaibo, Venezuela. Fedes.

Peñas, R. "El derecho a la propiedad sobre las bases o bancos de datos". II Seminario Internacional de Telecomunicaciones e información. 1998. FCCI. Universidad Complutense de Madrid. Disponible en: [http://www.ucm.es/infor/dinforma/activi/index.html]

Prenafeta, J. "Protección de datos de carácter personal e Internet" en *Área Digital APTICE.* Disponible en: [http://noticias.juridicas.com/external/nj_aptice/200208-5556153161023211 1.html]

Proaño, L.E. "Comunicación y Democracia". En *Chasqui* Nº 7, 1983. CIESPAL. Quito, Ecuador, pp. 4-5.

Puccineli, Ó. (1999): *El habeas data en Indoiberoamérica.* Temis. Santa Fe de Bogotá, Colombia.

Reindenberg, J. "Privacidad y Comercio Electrónico en los Estados Unidos". Disponible en: [http://reidenberg.home.sprynet.com/Privacidad-USA.htm]. Este trabajo fue presentado en el seminario realizado en la Universidad de California - Berkeley titulado "The Legal and Policy Framework for Global Electronic Commerce: A Progress Report", realizado en Marzo 4-6, 1999. El artículo fue originariamente publicado con el siguiente título "Restoring Americans' Privacy in Electronic Comerce", en el *Berkeley Technology Law Journal,* Spring, 1999 (14 Berkeley Tech. L.J. 771).

Roca, J. "El mito de la privatización". *Revista Comunicación* Nº 71-72, 1990. Trimestres tres y cuatro. Caracas, Venezuela, pp. 5-19.

Roncagiolo, R. "Comunicación y democracia en el debate internacional". En *Chasqui* Nº 7, 1983. CIESPAL. Quito, Ecuador, pp. 12-17.

Rosca, T. (1988): *El Culto a la Información.* Barcelona, España, Editorial Crítica.

"FUCK INTEL". *Revista de la RaZa para la RaZa de SysAdmins, Hackers, FreeJacks Crackers, Cyberpunks, Wannabes, Phreakers, Warez d00dz y lindas nenas.* Disponible en: [http://www.raza-mexicana.org/textos/revista/txt/raza007.txt]

Tablante, Carlos (2001): *Delitos informáticos; delincuentes sin rostro.* Caracas, Venezuela. Encambio.

Wagner, J. (1997): *In Pursuit of Privacy: Laws, Ethics, and the Rise of Technology.* Cornell University Press. New York, USA.

Sitios Web

*Boletín de privacidad on line: [*http://www.ulpiano.com/boletinprivacidad.html].

Consejo de Europa sobre protección de datos:
[http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/]
Sitio Web sobre privacidad [http://www.privacy.org/]