LOS DERECHOS HUMANOS EN EL CIBERESPACIO

Dra. Esc. María José Viega

SUMARIO

1. Introducción

Cuando pensamos en la problemática y en los desafíos que el ciberespacio plantea nos encontramos con algunas novedades, pero son las menos. Normalmente Internet ha agravado ciertos problemas, los a redimensionados, pero son temas que ya venían siendo tratados, incluso con una importante normativa, que deberá ser actualizada, si ya no lo ha sido, para regular las nuevas facetas que este nuevo espacio nos ha traído.

En el presente trabajo voy a tratar tres temas principales, que en mi opinión han sido los más relevantes, ellos son: la protección de la privacidad, la libertad de expresión y de información, su repercusión en la protección de la infancia y por último el tema referido a la seguridad relacionada con la encriptación de datos. Para terminar con un panorama del derecho positivo uruguayo en esta área.

2. Privacidad

2.1. La privacidad en Internet

Hoy por hoy se entiende que la vida privada no se limita a la intimidad, sino que este concepto ha sido sustituido por uno más general como es el de privacidad[1]. Internet es una amenaza en la difusión de elementos relativos a la persona, por diferentes características que encontramos en ella, las que analizaremos una a una.

Cuando pensamos en regular este tema, debemos ponderar dos intereses diferentes, por un lado la protección de la vida privada y por otro el interés de la sociedad toda, en que circule cierta información. Este punto tiene estrecha relación con la libertad de expresión y de información, así como también de la seguridad que podemos tener en nuestras comunicaciones y las herramientas que pueden ser útiles para ello.

La Red es un medio de comunicación polifacético, debido a la existencia de múltiples medios para distribuir información. Ellos son: el correo electrónico, los boletines, los foros de discusión y también la información presente en la www[2].

Para enfrentar este desafío debemos tener en cuenta los siguientes elementos[3]:

a) la infraestructura de Internet está basada en datos personales (IP),

b) un segundo elemento se refiere a los instrumentos técnicos utilizados, los software de navegación, por ejemplo, que envían más información de la requerida para realizar una conexión,

c) y en tercer lugar la cantidad de datos que nos solicitan para realizar actividades comerciales en línea.

Se nos plantea una dependencia entre la utilización de Internet y el dar datos personales. Y esta relación está signada por la desigualdad entre el proveedor y el usuario. Otro elemento relevante es la desinformación del usuario, que la mayoría de las veces no sabe que sus datos se han recopilado.

Existen tres elementos de fundamental importancia con relación al manejo de datos, que son:

1) Las **Cookies:** podemos definirlas como fichas de información automatizada, las cuales se envían desde un servidor web al ordenador del usuario, con el objetivo de identificar en el futuro las visitas al mismo sitio. Las cookies son una potente herramienta para almacenar o recuperar información empleada por los servidores web debido al protocolo de transferencia de ficheros (http). Los riesgos ya los conocemos: recopilación de gustos, preferencias, hábitos, nombre y contraseña y además que algún experto podría manipular estos archivos[4].

2) Los **Navegadores**: que suelen envíar más información que la necesaria para conectarse, como por ejemplo el tipo y lengua del navegador, que otros programas se encuentran instalados, cual es el sistema operativo del usuario, cookies, etc

3) **Contenidos Activos**: ejecución de programas con este tipo de contenidos, como por ejemplo Java y ActiveX.

2.2. Situación de la Unión Europea y EEUU

Se han buscado distintas soluciones para este tema, a nivel de la **Unión Europea** encontramos[5]:

1. En el año 1996 el Libro Verde sobre la Protección de los Menores y de la Dignidad Humana en los Nuevos Servicios Audiovisuales y de Información. Distingue el contenido ilícito, que es aquel constitutivo de delito, que estará legislado en forma interna en cada país, del contenido nocivo o dañino, que es aquel que lo es para algunas personas, pero es legal, por ejemplo la pornografía.

2. Plan de Acción para el uso seguro de Internet, el cual se instrumenta a través del fomento de un uso responsable, esto es a través del etiquetado, clasificación y filtros; el impulso de la autorregulación, con el establecimiento de códigos de conducta por parte de los proveedores de Internet y por último la sensibilización a padres y profesores respecto a estos temas.

3. Directiva 95/46/CE sobre la Protección de personas físicas, tratamiento de datos personales y su libre circulación.

4. Directiva 97/66/CE sobre el Tratamiento de datos personales y protección de la intimidad en el sector telecomunicaciones (envío de datos a terceros países).

En **EEUU** en cambio se ha buscado la protección a través de la autorregulación. Lo que ha ocasionado problemas con los países europeos porque no lo consideran un país seguro para el envío de datos. Esto a llevado a que existan propuestas basadas en los principios de puerto seguro, en el año 1999, que no han prosperado[6].

Por otra parte, el **Grupo de Trabajo sobre protección de las personas** ha dictado una Recomendación 1/1999, en la cual se establece que:

1. el navegador debería informar al usuario que información pretende transferir y con que objeto,

2. cuando existen hipervínculos, el navegador debería indicar el sitio en su totalidad

3. las cookies deberían informar cuando se está enviando una cookie, que información pretende almacenar, con que objetivo y el período de validez.

2.3. Ley Argentina de Habeas Data

A nivel Latinoamericano debemos destacar en **Argentina** la Ley de Habeas Data N° 25.326 promulgada en noviembre del 2000. “Tanto los registros manuales como los automatizados quedan incluidos en la norma. Esto último incluye bases de datos usadas “on line” para recopilar datos personales que incluyan cookies (por la referencia a datos “determinables”), números de identificadores, formularios web, correos electrónicos, bancos de datos que proveen informes a través de Internet, y cualquier otra forma de recopilación de datos en forma automatizada”[7].

Con relación a la problemática mirada desde Internet podemos destacar que:

a) La ley exige el consentimiento expreso y escrito motivo por el cual los sitios web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento en forma previa a realizar su registración, aceptando las condiciones de la misma. Los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el usuario esté informado de los datos que se recabarán.

b) Existen excepciones previstas en la ley para la exigencia del consentimiento, y una de ellas establece el fin estadístico, en estos casos cuando las cookies recopilen datos relacionados a las visitas a un sitio, si estos datos no se cruzan con otra información personal suministrada por el titular de los datos, no requeriría el consentimiento.

c) La dirección de correo electrónico no está incluída como dato básico del individuo (dentro de las excepciones) por lo cual la distribución de bases de datos de correos electrónicos (para realizar spam) requerirán el consentimiento del titular.

Los acontecimientos del 11 de setiembre en EEUU ha llevado a que este país pretenda un estricto control sobre Internet. El gobierno de Estados Unidos no sólo se propone controlar Internet, incluyendo por supuesto los correos electrónicos, sino que también a solicitado a la Unión Europea, en la carta que se enviara el 16 de octubre, se reconsidere la legislación existente en materia de

protección de datos. Se aprobó en el Senado la ley “Combating Terrorism Act of 2001, el 13 de setiembre de 2001, que multiplica las posibilidades de monitorización de las comunicaciones.

Pero esto no es un propósito a largo plazo, sino que podemos leer con sorpresa en el Diario El Mundo español como a un joven de Valencia, que había enviado unos correos electrónicos haciendo bromas sobre Bin Laden, recibió un correo de la NSA (Agencia Nacional de Seguridad de Estados Unidos) diciendo que su cuenta de correo había sido bloqueada. Su cuenta pertenece a una empresa norteamericana en la que había trabajado, lo que facilitó que sus mensajes fueran detectados[8].

Tengamos presente que la comisión de la Unión Europea encargada de determinar la existencia de una red de espionaje de comunicaciones de EEUU llamada ECHELON, entregó un informe afirmativo al respecto[9].

La privacidad es un derecho fundamental, por lo que se recomienda el uso de comunicaciones cifradas, que como veremos más adelante también presentan sus limitaciones e inconvenientes.

3. Libertades de expresión y de información

3.1. Conceptos y problemática

Para Francesc de Carreras, siguiendo el Pacto Internacional de Nueva York y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, la libertad de expresión se compone de dos derechos fundamentales: la libertad de opinión y la libertad de información[10].

Libertad de opinión y de conciencia: implica el derecho a no ser molestado ni discriminado por las ideas o creencias personales.

La libertad informática aparece como un nuevo derecho de autotutela de la propia identidad informática: o sea el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscriptos en un programa electrónico[11].

El derecho a la autodeterminación informativa es una construcción de la doctrina y jurisprudencia germanas que es equivalente a la libertad informática. El libre desarrollo de la

personalidad (reconocido en Alemania) se desglosa en dos libertades básicas:

a) la libertad general de la acción: libertad para decidir la realización u omisión de determinados actos y la consiguiente facultad para comportarse o actuar de acuerdo con esa decisión

b) la autodeterminación informativa: libertad para determinar quién, qué, y con qué ocasión pueden conocer informaciones que conciernen a cada sujeto.

Referente al Habeas Data podemos cotejarlo con habeas corpus y vemos que existe una coincidencia en cuanto a la naturaleza jurídica, ya que no se trata de derechos fundamentales, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal (habeas corpus) y de la libertad informática (habeas data).

La libertad de expresión se compone de tres elementos básicos: libertad ideológica, libertad y derecho a recibir información veraz y la libertad de expresar la propia opinión

La libertad de información podemos verla desde dos puntos de vista: activa: derecho de dar información y pasiva: derecho a recibir información

A los efectos de determinar cual es la legislación apropiada para regular la libertad de expresión y de información en Internet, resulta interesante preguntarnos a cuál de los medios hasta ahora tradicionales se asemeja más la Red.

Pensemos en una comunicación telefónica, en la prensa escrita y en la radiodifusión. El que Internet sea como dijimos anteriormente un medio de comunicación polifacético dificulta la calificación.

Internet ha cambiado el control de la comunicación, de los medios de comunicación generalizado, al usuario. Así es que se ha roto la estructura en la cual teníamos un emisor inteligente y múltiples receptores pasivos. Hoy todos y cada uno de nosotros como usuarios de Internet podemos convertirnos en un productor de información, podemos dar nuestras opiniones referentes a múltiples temas y con un alcance mundial.

3.2. Regulación de la libertad de expresión en Internet

¿Cómo –entonces- debe regularse el ejercicio de la libertad de expresión en Internet? No es privado como una llamada telefónica, respecto a la prensa escrita se ha dicho que esta carece de la interactividad que posee la Red y en último término respecto a la radiodifusión se dice que sobre esta existe un control "excesivo", que no podría o no sería apropiado aplicar a Internet. Personalmente entiendo que la radiodifusión es un medio diferente, tengamos presente el tema de la pornografía en una emisión televisiva, existe un horario de protección al menor y fuera de él puedo emitir determinados programas. Sin embargo un sitio pornográfico en Internet está allí las 24 horas del día los 365 días del año, es imposible delimitar un horario ya que la Red es mundial.

La Doctrina Española ha entendido que deben existir limitaciones mínimas para la libertad de expresión a través de Internet, igual que para cualquier otra comunicación.

La jurisprudencia europea distingue entre bases de datos de acceso restringido de las abiertas al público en general, y asimila a estas últimas a la prensa, por lo cual sería aplicable la ley de Prensa (Decreto-ley 15.672 de 9 de noviembre de 1984) en lo referente al procedimiento para corregir o cancelar datos que resulten atentatorios de la libertad informática.

3.3. Protección de los menores en Internet

Este tema está sumamente ligado a la Protección de la juventud y de la infancia, esta libertad de expresión y del libre flujo de la información en el ciberespacio lleva a que los niños y jóvenes puedan acceder a información que es perjudicial para su formación y su desarrollo sicológico y emocional.

En EEUU ha existido un intento de regulación y de limitación de la libertad de expresión en Internet. Pero la Unión Europea se ha propuesto métodos combinados como son el uso de filtros, las líneas de denuncia, estableciendo lo que denominan un Plan de Acción para el uso seguro de Internet.

Comenzando por EEUU en el año 1996 se dictó la Ley de Decencia de las Telecomunicaciones, que declaraba ilegal el uso de ordenadores y líneas telefónicas para transmitir material "indecente". Establecía penas de prisión y multas cuando el

discurso pudiera ser visto por menores. Esta ley fue impugnada el mismo día de su promulgación y limitaba el derecho a la libertad de expresión, amparado en la Primera Enmienda a la Constitución estadounidense.

Existen en este país discursos que carecen de protección constitucional, ellos son el discurso publicitario o comercial y el discurso obsceno. El discurso obsceno se diferencia del discurso indecente[12].

El Tribunal Supremo estableció unos criterios para la distinción entre material "obsceno" y material "indecente" en el famoso caso *Miller* contra *California*. La definición de Miller de discurso "obsceno" se basa en un test de tres partes: 1. Muestra o describe un acto sexual descrito en una ley del Estado contra la obscenidad. 2. Esto lo hace de un modo claramente ofensivo (*patently offensive*), apelando a sentimientos lascivos (*appealing to the prurient interest*), atendiendo al criterio de un buen padre de familia (*reasonable person*) aplicando los estándares de cada comunidad. 3. El material carece de valor literario, artístico, social, político o científico serio[13].

El concepto de discurso indecente es más amplio que el discurso obsceno. En el caso "FCC contra Pacífica Foundation" si bien no lo define, dice que debe referirse al contexto, teniéndose en cuenta los medios de comunicación, así como también los estándares de una sociedad determinada[14].

Finalmente el Tribunal Supremo la declaró inconstitucional en 1997 por ser contraria a la Primera Enmienda.

Tenemos entonces que si Internet se equipara a la prensa escrita, la libertad de expresión es más libre porque no puede limitarse el discurso indecente. Pero si la equiparamos a la radiodifusión, entonces se hubiera legitimado la limitación a la libertad de expresión, ya que el Tribunal Supremo ha permitido que se prohíba en este medio el discurso indecente.

El Tribunal Supremo norteamericano entiende que Internet se asimila más a la prensa escrita que a la radiodifusión. La radiodifusión llega al usuario de diferentes formas, mientras que en la Red la información debe ser buscada. Además, tiene en cuenta que existen modos de controlar la información nociva, como son por ejemplo los programas filtros. El Tribunal Supremo afirma también

que Internet da la misma posibilidad a los ciudadanos “de a pie” de ejercer el derecho a la libertad de expresión que a las grandes empresas de comunicación y por lo tanto se convierte en un medio democratizador de la información.

En el año 1998 se aprueban en EEUU dos leyes federales:

a) la Ley de Internet Seguro para las Escuelas, según la cual toda escuela, instituto o biblioteca que recibiera fondos públicos debe utilizar programas-filtros. Existen procesos abiertos contra esta ley[15].

b) la Ley de Protección de los Menores Conectados a Internet: la cual permite a los titulares de páginas web distribuir pornografía asegurándose que el usuario es un adulto. Ya fue declarada inconstitucional en 1999. La prohibición de aplicación fue apelada.

Como ya adelantáramos la Unión Europea siguió un camino diferente en torno a este tema, por Decisión N° 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales[16], en el artículo 3° se establece:

- fomentar la autorregulación del sector y los mecanismos de supervisión de los contenidos (por ejemplo, los relativos a contenidos tales como la pornografía infantil o aquellos que inciten al odio por motivos de raza, sexo, religión, nacionalidad u origen étnico),

- alentar al sector a ofrecer medios de filtro y sistemas de clasificación que permitan a padres y profesores seleccionar los contenidos apropiados para la educación de los menores a su cargo, y a los adultos decidir a qué contenidos lícitos desean tener acceso, y que tengan en cuenta la diversidad cultural y lingüística,

- mejorar entre los usuarios el conocimiento de los servicios ofrecidos por el sector, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet,

- llevar a cabo medidas de apoyo como la evaluación de las implicaciones jurídicas,

- realizar actividades para fomentar la cooperación internacional de los campos mencionados,

- efectuar otras actividades que contribuyan a la consecución de los objetivos establecidos en el artículo 2.

Creación de Líneas Directas, éstas son una manera eficaz de restringir la circulación de contenidos ilegales, implica establecer una red europea de centros, que se denominan líneas directas, que permitan a los usuarios notificar los contenidos que hayan encontrado al utilizar Internet y a su juicio sean ilícitos.

Plantea demás, el desarrollo de directrices de ámbito europeo para la elaboración de códigos de conducta y fomentar un sistema de “etiquetas acreditativas de sitios web de calidad” que sean visibles para ayudar a los usuarios a identificar a los proveedores de servicios de Internet que operen de conformidad con dichos códigos de conducta.

A los efectos de que los contenidos sean fáciles de identificar son útiles el mecanismo de clasificación y el uso de sistemas de filtros. La clasificación describe el contenido de un sitio y luego mediante mecanismos de filtro permite seleccionar al usuario los contenidos que desea recibir. Se fomentará que estos sistemas de filtro y clasificación sean compatibles internacionalmente.

4. Seguridad en Internet

A pesar de las normas que protegen la confidencialidad en las comunicaciones, los medios de comunicación son cada vez más vulnerables.

En el año 1980 aparece el uso de codificadores para la televisión por cable y la televisión vía satélite. Pero ya existe una industria paralela de aparatos piratas de descodificación. A nivel de comunicación telefónica existen las llamadas escuchas telefónicas. También es posible violar la seguridad de la redes informáticas de las Empresas, para acceder a datos de la competencia. Por lo tanto la seguridad es un tema que hoy por hoy preocupa sobre manera a las empresas.

Referente a las escuchas telefónicas en Sudáfrica se está por aprobar una ley que prohíbe a los ciudadanos comunes que espíen conversaciones ajenas, pero le otorga amplios poderes a la policía. El proyecto prevé que los proveedores de Internet y las empresas telefónicas creen centros de monitoreo para la policía[17].

Una de las soluciones a este problema es la encriptación, que podemos definirla como el arte de crear y usar métodos para disfrazar mensajes usando códigos, algoritmos y otros métodos de tal modo que sólo las personas que conocen esos códigos puedan acceder a la información. La encriptación garantiza la confidencialidad, la integridad de la información y la autenticidad de la misma.

La utilización de la encriptación se remonta a la antigua Roma, el primer algoritmo de encriptación utilizado fue el llamado “Cifrado de César”.

El uso más evidente (y el más importante a lo largo de la Historia) ha estado relacionado con la defensa, y su importancia ha crecido a la par de la importancia de las telecomunicaciones en los conflictos bélicos. Es algo fundamental para un ejército conocer los planes del enemigo, ocultar los propios e incluso poder confundir al bando contrario con órdenes falsas. La criptografía permite asegurar el secreto de los mensajes propios, analizar los ajenos y estudiar la posibilidad de falsificarlos. Por tanto, puede ser un arma realmente peligrosa[18].

Existe programas de encriptación, como es el caso de PGP, para el encriptado de mensajes de correo electrónico. Sin embargo, el uso del PGP está prohibido en algunos países.

Se suscribió en la Unión Europea el Arreglo de Wassenaar en el año 1995[19], el cual regula la comercialización, importación y exportación de productos bélicos y tecnología asimilada, que es la tecnología de doble uso. La denominada encriptación fuerte ha sido definida como una mercancía de doble uso. Por eso en Francia se equipara la encriptación a material bélico, en Rusia es ilegal la encriptación sin licencia de uso, en el Reino Unido existe un proyecto que prohibe el uso comercial de la encriptación sin autorización.

En EEUU la prohibición es casi total referente a la exportación de material cifrado fuerte. El Clipper o Key Escrowed System[20] es un sistema de uso voluntario, que tiene dos elementos: un chip cifrador a prueba de análisis o manipulación y el depósito de las claves secretas. Cada clave tiene 2 componentes que se entregan a 2 agencias estatales[21].

Otro sistema es el TTP (Trusted Third Parties), según el cual existe una empresa autorizada por el Estado a la que se encomienda la seguridad y confidencialidad de las telecomunicaciones. Este sistema es el que se trata de implantar a nivel europeo.

5. Normativa Nacional

a) Libertad de expresión: art. 29 de la Constitución: “Es enteramente libre en toda materia la comunicación de pensamientos por palabras, escritos privados o publicados en la prensa, o por cualquier otra forma de divulgación, sin necesidad de previa censura, quedando responsable el autor y, en su caso, el impresor o emisor, con arreglo a la ley por abusos que cometieren.”

b) Derecho a la intimidad, no está especificamente regulado, pero podemos entender que se encuentra reconocido a través del artículo 72 de la Constitución que establece: “La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno”.

En la medida que la intimidad consiste en que no se produzca ningún tipo de intromisiones en el ámbito reservado a la vida

privada de los individuos, cabe hacer caudal también del art. 10, cuyo inc, 1° dispone que “Las acciones privadas de las personas que de ningún modo atacan al orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados[22].

c) Decreto - Ley 15.672 - Ley de prensa. Consagra: libertad de expresión y comunicación de pensamientos y difusión de informaciones mediante la palabra, el escrito o la imagen, por cualquier medio de comunicación.

d) Pacto de San José de Costa Rica, ratificado Ley 15.837 de 1985. Convención Americana sobre Derechos Humanos firmada el 22 de noviembre de 1969 art. 14, art. 25 “toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio .... y que se dirijan al público en general” tiene derecho a efectuar su rectificación o respuesta.

e) Ley 16.011 - 19/12/1988 Acción de Amparo: “podrá constituirse en un instrumento eficaz de protección genérica de la libertad informática a fin de poder concretar formas de acceso, tales como la de saber que bases de datos existen, obtener respuesta afirmativa o negativa del responsable de una base de datos acerca de si existen datos personales del accionante, y obtener la versión exacta de tales datos en términos claros y accesibles a cualquier ciudadano”[23].

f) Ley 16.099[24] – 3/11/1989 Díctanse normas referentes a expresión, opinión y difusión, en comunicaciones e informaciones, consagradas por la Constitución. Esta ley se refiere a las libertades de prensa y de imprenta, al derecho de respuesta, a los delitos e infracciones cometidos por la prensa u otros medios de comunicación y al procedimiento a llevarse a cabo en esos casos.

g) Ley 16.616[25] - 20 de octubre de 1994. Sistema Estadístico Nacional. El capítulo IV de esta ley se refiere a los principios de la recolección de datos, al secreto estadístico y a la difusión de la información.

De lo antedicho surge que Uruguay no tiene una norma específica en materia de protección de datos, existe un proyecto de ley a estudio del Parlamento referente a habeas data. Sin perjuicio de lo cual podemos proteger y marcar ciertos parámetros a través de la normativa citada.

Montevideo, octubre de 2001.

[1] Delpiazzo, Carlos. "Dignidad Humana y Derecho". Universidad de Montevideo. Facultad de Derecho. Montevideo, 2001.

[2] Viega, María José. "Privacidad en Internet". Segundas Jornadas Internaciones del Instituto de Derecho Informático. Montevideo, 2000.

[3] Aragón Reyes Manuel y Fernández Esteban María Luisa. Incidencia de Internet en los Derechos Fundamentales. Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid.

[4] Mendoza Luna, Amílcar. "Los cookies: ¿amenaza a la privacidad de información en la internet?. www.derecho.org/redi

[5] Viega, María José. "Privacidad en Internet" Ob. cit.

[6] Aragón Reyes Manuel y Fernández Esteban María Luisa. Incidencia de Internet en los Derechos Fundamentales. Ob. cit.

[7] Palazzi, Pablo "La nueva Ley de Habeas Data y protección de datos personales en Argentina". Memorias del VIII Congreso Iberoamericano de Derecho e Informática. México, Noviembre del 2000.

[8] http://www.elmundo.es/navegante/2001/09/24/esociedad/1001317628.html Privacidad. EEUU interviene un correo por bromear sobre Laden. J.M. Vilar.

[9] El Parlamento Europeo demuestra la existencia de Echelon. http://www.larazon.es/lared/laredesoias.htm y El Parlamento europeo reconoce la existencia de la red de espionaje Echelon.http://idg.es/pcworld/noticia.asp?id=18239

[10] Francesc de Carreras. "La libertad de expresión: un derecho constitucional, en Libertad de Expresión. Anuario 1990, Universidad Autónoma de Barcelona, PPU, pág. 29 citado por Lluís de Carreras Serra en "Régimen jurídico de la información. Periodistas y medios de comunicación". Editorial Ariel S.A. Barcelona, 1996.

[11] Pérez Luño Antonio Enrique. "Manual de informática y derecho". Editorial Ariel S.A. Barcelona, 1996.

[12] The difference between Obscenity and Indencency. http://www.eff.org/Legal/obscenity_and_indececy_godwinxcerpt

[13] Aragón Reyes Manuel y Fernández Esteban María Luisa. Incidencia de Internet en los Derechos Fundamentales. Ob. cit.

[14] The difference between Obscenity and Indencency. Página citada.

[15] Safe Schools Internet Act of 1998. http://www.techlawjournal.com/congress/blocking/s1619.htm

[16] http://europa.eu.int/eur-lex/es/lif/dat/1999/es_399D0276.html Texto de la Decisión N° 276/1999/CE

[17] http://pmg.org.za/bills/Interception0107.htm

[18] Borja Marcos. Criptografía, privacidad y legislación. Ponencia presentada a DERIN. Primer Congreso Internacional de Derecho e Informática en Internet.

[19] Arreglo de Wassenaar – Lista de productos de doble uso.http://www.onnet.es/03005007.htm

[20] Privacy in the Digital Age: Encryption Policy – A Call for Congressional Action. David B. Walked. http://stlr.stanford.edu/STLR/Articles/99_STLR_3/contents_f.htm

[21] The metaphor is the key: criptography, the Clipper Chip, and the Contitution. A. Michael Froomkin. http://www.swiss.ai.mit.edu/6095/articles/froomkin-metaphor/text.html

[22] Delpiazzo, Carlos. "Los derechos humanos ante las nuevas tecnologías. Ponencia presentada al I Congreso Mundial de Derecho e Informática (Universidad San Francisco de Quito, 15 al 18 de octubre de 2001).

[23] Delpiazzo Carlos E. "Información, informática y Derecho". Ediciones Jurídicas Amalio M. Fernández. Montevideo, 1989.

[24] http://www.parlamento.gub.uy/Leyes/Ley16099.htm

[25] http://www.parlamento.gub.uy/Leyes/Ley16616.htm