PROPUESTA DE LINEAMIENTOS PARA ELABORAR UN REGLAMENTO DE MEDIDAS DE SEGURIDAD PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL CONTENIDOS EN FICHEROS INFORMÁTICOS

HERNÁNDEZ RAMÍREZ, José Luis

SUMARIO: I. PROEMIO. II. METODOLOGÍA DE TRABAJO. III. ANTECEDENTES GENERALES DE LOS DATOS PERSONALES CONTENIDOS EN FICHEROS INFORMÁTICOS. A) ¿Por qué este proyecto?. B) El tratamiento en la recogida de datos. C) La obligación a cargo de los sujetos obligados en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para implementar políticas de protección de datos personales en ficheros informáticos. IV. LA EXPERIENCIA DEL DERECHO INTERNACIONAL ALEMANIA. UNIÓN EUROPEA. ESPAÑA. LA CARTA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA. V. CONSIDERACIONES FINALES. 1. PROPUESTA PARA INCLUSIÓN DE GARANTÍAS AL TEXTO CONSTITUCIONAL. 2. POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES. 3. LINEAMIENTOS PARA REGULAR LA PARTE RELATIVA AL "HABEAS DATA".

I. PROEMIO. Como en casi todos los ámbitos de la vida, la cuestión del tratamiento de los datos personales por terceros se encuentra, por así decirlo, en una situación de tensión. Esta tensión deriva de que los ficheros que reflejan circunstancias y perfiles de personas concretas han llegado a ser de tal maleabilidad y magnitud, que ostentan un indudable valor económico, y es que una base de datos de personas puede ser filtrada en términos tales que recoja sólo la lista de las personas que "dan el perfil" correcto para un negocio, como podría ser, por ejemplo, la base primaria de datos que se conforma con la información proporcionada directamente por los usuarios a las sociedades de información crediticia en México.[1] Tener esos datos es por tanto valioso para cualquier actividad de marketing y por tanto, objeto de comercio, al ser de gran valor la disposición de información personal ahí contenida. Con la aparición de la súper carretera de la información conocida como Internet, asistimos al desarrollo grandioso del *e-commerce*; y es a partir de ello que se han venido controlando día con día los procesos de adquisición, distribución y uso que se hacía de esta información, aparentemente sin ningún control legal. Lo que hasta hace poco suponía un desembolso económico elevado en campañas de publicidad por medios tradicionales, es ahora más asequible, ya que se nos ofrece la facilidad de rellenar un simple y sencillo formulario en una página que promete informar de todas las novedades del producto que se está consultando, y nos ofrece además la posibilidad de participar en un concurso tan virtual como posiblemente inexistente, en el que se puede ganar desde un súper deportivo último modelo, unas vacaciones en lugares paradisíacos, o dinero, y todo por enviar la información a varias cuentas de correo electrónico, para convertirlos en potenciales consumidores, que tal vez podrían tampoco estar interesados en los productos ofertados.

Imaginemos que desde hace un par de años nuestros padres, personas mayores, digamos 75 años, reciben incesante e insistentemente publicidad de una empresa de sistemas auditivos para que compren sus productos, supuesto que por la edad tienen problemas de esta índole, cuando por suerte hasta ahora no ha sido así. Evidentemente, esta empresa ha tenido que obtener y hacer uso de unos datos de carácter personal que les han permitido segmentar el mercado adecuadamente, sin que nadie sepa cómo los obtuvo, ni cómo han llegado a diagnosticar un potencial problema auditivo. Esta situación imaginaria nos permite pensar qué otros estudios y conclusiones se pueden derivar de este tipo de tratamiento de la información. Cualquiera de nosotros podría ser clasificado por estas técnicas atendiendo a la salud, ideología, religión, sexo, edad, etcétera, atentando brutalmente contra nuestra intimidad. Y es que con una tecnología tan poderosa como el Internet, que en principio permite un enorme grado de libertad individual, también permite comportamientos que van en contra de esa libertad. Por supuesto, la sociedad debe disponer de los mecanismos necesarios para protegernos de todo esto. En México disponemos de escasa legislación relativa a la protección de datos de carácter personal, amén de las garantías constitucionales consignadas en los artículos 14 y 16, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, así como de la inviolabilidad del domicilio y papeles.[2] Por otro lado estamos hablando de datos de personas, que no son

[1] Secretaría de Hacienda y Crédito Público. *Decreto por el que se expide la Ley para Regular las Sociedades de Información Crediticia*. Diario Oficial de la Federación del 15 de enero del 2002. Primera sección, página 1, artículo 2 fracción I. De la lectura de esta ley, podemos deducir a grandes rasgos que las empresas que se dedican a la prestación de servicios de información sobre la solvencia patrimonial y el crédito de las personas físicas, sólo pueden tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

[2] Nuestra Constitución reconoce estos derechos, pero curiosamente en ninguna parte del texto dispone con afirmación clara y rotunda que el domicilio es inviolable. Se deduce la inviolabilidad del domicilio, por lo

cosas y que tienen una natural dignidad,[3] y por tanto, tienen derecho a ser tratadas como tales: **a que se respete su condición, a saber qué se está haciendo con su nombre, a saber qué se está haciendo con sus datos personales. En una palabra, a la intimidad.**[4] Los ficheros que afectan a la vida de las personas, y que tratan información de carácter personal, han existido desde siempre, sólo que en papel. El cambio que opera la informática, es que multiplica para cualquier organización o persona la posibilidad de realizar un tratamiento automático y racional de la información.[5] Esta se encuentra recogida en archivos informáticos llamados bases de datos que sustituyen a los antiguos ficheros de papel. Estos ficheros informáticos, las bases de datos, son también ficheros. Lo único que cambia es el formato: son ficheros (archivos) informáticos.

Vemos así que una de las bondades que nos brinda la automatización de los procesos de tratamiento de datos, es, sin lugar a dudas, el haber mejorado y aumentado, tanto la productividad personal, como la de las empresas. Y es que no resulta difícil darse cuenta de que la Red se ha convertido en un espacio perfecto de regulación, y del papel que el comercio ha desempeñado en esta transformación.[6] Y es que la era del acceso también llega con un nuevo tipo de ser humano. Los jóvenes de la nueva generación se encuentran cómodos dirigiendo negocios y desarrollando su actividad social en los mundos del comercio electrónico y el ciberespacio, y se adaptan con facilidad a los múltiples mundos simulados que configuran la economía cultural, donde el suyo es un mundo más teatral que ideológico y más orientado por un *ethos* del juego que por un *ethos* del trabajo.[7] La tecnología está para aumentar nuestra capacidad de desarrollo tanto personal como profesional, permitiéndonos alcanzar metas impensables tan sólo hace unos años. Los beneficios que reporta su uso exceden con mucho los problemas, como los derivados de la impersonalización en el tratamiento de los datos que manejamos. Por eso debemos poner límite al grado de intrusión en nuestra privacidad que el tratamiento automatizado de datos puede generar. Y es ésta la preocupación de un gran número de usuarios de Internet: **la revelación de la información personal que les afecta, se genera, recolecta, almacena, interrelaciona y se pone a disposición de muchos usos automáticamente, incluidos los fines comerciales.**[8] ¿Es tan importante la intimidad como la libertad o la vida?. En un mundo digitalizado y globalizado, entiendo que deben ponerse al mismo nivel, y ello porque la intimidad es el último reducto del ser humano frente al sistema. Si se suprime la libertad de prensa, el derecho de reunión y asociación, sólo nos queda la intimidad para conspirar frente al poder. Sin intimidad no hay revolución posible. En el futuro mundo feliz que construyen los medios de comunicación al servicio de las corporaciones multinacionales, a través de los Reality Shows, la última posibilidad de resistencia reside en el derecho a la

---

dispuesto en la parte final de su artículo 16 que dispone: **"En toda orden de cateo, que sólo la autoridad judicial podrá expedir y que será escrita, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse , y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia".** Referente a la garantía de protección a la correspondencia y papeles de las personas, resulta también relativamente protegida constitucionalmente, ya que ésta se encuentra señalada en forma muy general, aunque lo suficiente como para afirmar que existen garantías constitucionales que toman en cuenta a esos papeles, y al más alto nivel son preservados del abuso de las autoridades de toda clase.

[3] Hay ficheros informáticos de datos que son cosas (químicos, programas, etcétera) que también son valiosos y están protegidos. Pero por otras reglas, no menos estrictas, pero distintas.

[4] **Microsoft**. *La protección de datos personales. Soluciones en entornos Microsoft*. (documento electrónico) http://www.microsoft.com/spain/seguridad. **HERNÁNDEZ RAMÍREZ, José Luis.** *Análisis sobre la responsabilidad civil, el daño moral y el daño a la persona en el Derecho Civil Mexicano*. Revista Electrónica de Derecho Mexicano, número 3, octubre y noviembre de 1999. Dirección electrónica: http://publicaciones.derecho.org/redm/

[5] Artículos 3-I; V; XIII; 13-IV; 18-II; 20; 21, 22-V; 23; 37-VIII; IX; XII; XIII; XIV. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y artículos 1, 2; 37 al 40; y 47 al 48 del Reglamento de la Ley de Transparencia (...) **PONJUÁN DANTE, Gloria**. *Gestión de información en las organizaciones. Principios, conceptos y aplicaciones*. 1ª edición 1998. CEPACI-Vicerrectoría, Universidad de Chile, Serie: Gestión de Información.

[6] **CASTELLS, Manuel**. *La Era de la Información. Economía, Sociedad y Cultura*. Colección Fin de Milenio, Volumen III, capítulo 2: **El cuarto mundo: capitalismo informacional, pobreza y exclusión social.** Siglo Veintiuno Editores, México; 2ª edición en español 2000, traducción de Carmen Martínez Gimeno. **LESSIG, Lawrence**. *El Código y otras leyes del ciberespacio*. Taurus Es digital, España 2001. Traducción de Ernesto Alberola.

[7] **RIFKIN, Jeremy.** *La era del acceso. La revolución de la nueva economía*. PIADOS – Estado y Sociedad (BARCELONA, BUENOS AIRES) año 2000, página 23. **IANNI, Octavio**. *La era del globalismo*. Siglo Veintiuno Editores, 1ª edición en español 1999, página 11.

[8] Las negritas son del que escribe.

intimidad: Nuestra última barricada.[9] Y es que ahora la economía ha puesto sus miras en la última esfera de la actividad humana que restaba por mercantilizar: **la cultura**. Los rituales culturales, las actividades comunitarias, las reuniones sociales, el arte, los deportes y los juegos, los movimientos sociales y la actividad cívica, todo resulta invadido por la esfera comercial.[10]

Es indudable que el ciudadano deja un rastro indeleble de su paso por todas y cada una de las actividades cotidianas, desde que tiene acceso a los cajeros automáticos hasta cuando hace sus pagos por medio de tarjetas de crédito; desde que decide pedir un crédito o solicita un cambio de aceite para su vehículo; o hasta cuando plantea su gestión para obtener una pensión o accede a su página favorita en Internet. Con todo esto, tenemos millones de ojos vigilándonos en el ciberespacio, ¿quién nos protege en Internett?[11] es la pregunta. No existe una posibilidad de convertirnos en un Robinson Crusoe y mantenernos alejados del peligro de ser parte de un banco de datos, ya que por el solo hecho de ser ciudadano y tener una partida de nacimiento, nos podemos considerar incluidos en un ingente flujo de información, cuyas corrientes fluyen desde los bancos de datos de la administración hasta los de los particulares, y el proceso no parece tener límites.

Es un hecho también el que las autoridades utilizan los mecanismos de las tecnologías de la información y la comunicación para vigilar y controlar a los ciudadanos en una red que no diferencia entre personas respetuosas de la ley y aquellos sospechosos de cometer un delito, pero con total apego al Estado de Derecho, donde el Estado tiene perfectamente definido su campo de acción y donde los gobernados tienen enunciados y garantizados sus derechos fundamentales. Es así que en las redes de los sistemas de comparación de datos no existe forma de sostener un principio formal de inocencia y es probable que, en el transcurso de nuestra vida, a pesar de haber reconocido el valor de los dictados normativos, alguna vez hayamos formado parte de un elenco arbitrario, sutil y poderoso, orquestado por un computador y su software de comparación de datos, pero también gozar de las bondades que nos proporcionan las tecnologías de la información, al brindar, en lo aquí comentado, como el que los implicados en procesos judiciales en Yakima, Washington, declaren vía correo electrónico, de forma tal que no tendrán que personarse ante la Corte para dar fe de sus alegatos, pudiendo así agilizar los trámites,[12] a través de un servidor seguro. El Juez abre una audiencia en una sala de la Corte, lee el correo electrónico y procede al veredicto. Posteriormente el funcionario de la Corte remite el veredicto.

Es obvio. Estamos viviendo en el mundo del ciberespacio, en la red de redes, conocida como Internet. El ciberespacio nació como un proyecto de investigación del Departamento de Defensa de los Estados Unidos que conllevaba un cierto grado de ausencia de arquitecturas de control,[13] donde el desplazamiento de la geografía al

---

[9] El derecho a la intimidad, recordemos, abarca muchas circunstancias de la vida personal. Últimamente, con el desarrollo de la Informática, la intimidad ha expandido el ámbito que a ella misma se refiere y se ha ido observando que las nuevas herramientas informáticas pueden suponer una intromisión en la vida privada de las personas. Por ello el concepto ha ido aproximando al de "privacidad". Es más que nada una cuestión de palabras. Lo que se denomina correctamente en castellano "intimidad", muchas veces la gente, empleando un anglicismo, lo llama "privacidad". El anglicismo trae causa de que los británicos denominan "private" a lo que no es "public", esto es, a aquellos ámbitos de la vida en los que los demás no tienen derecho a inmiscuirse, a lo íntimo. **HERNÁNDEZ RAMÍREZ, José Luis.** *El derecho a la intimidad en la legislación civil* (borrador), 2003. **ROJINA VILLEGAS, Rafael.** *Derecho Civil Mexicano*, Tomo V, Volumen II, Editorial Porrúa, página 138. **SILVINA DORREGO, Claudia**. *Libertad de expresión: La intimidad de las cámaras WEB*. http://www.derecho.org, consultado el 9 de diciembre de 1999. *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

[10] **RIFKIN, Jeremy**. *Opus cita*, página 21.

[11] **SÁNCHEZ ALMEIDA, Carlos.** *España: Intimidad: Un derecho en crisis. La erosión de la privacidad*. Artículo publicado en la Revista Electrónica de Derecho Informático, 1999. El autor es miembro de Fronteras Electrónicas-España, Bufete Almeida, http://www.bufetealmeida.com, consultado el 24 de junio del 2001.

[12] *La Vanguardia Digital*. **"Los implicados en un proceso judicial en EE.UU. declararán vía email"**. LVD – 19.11 horas – 03/10/2002. http://www.lavanguardia.es, consultado el 4 de octubre del 2002. En Argentina, el Consejo de la Magistratura suscribió un convenio con el fin de facilitar la comunicación a través de medios electrónicos entre los distintos poderes judiciales del país, denominado: **"Convenio de Comunicación Electrónica Jurisdiccional"**. Información proporcionada por Ivonne Valeria Muñoz Torres del Tecnológico de Monterrey (imunos@campus.cem.itesm.mx), vía correo electrónico del día 18 de julio de 2002

[13] **LESSIG, Lawrence**, *opus cita*. "*El anillo cerrado y de finalidad única de las redes telefónicas con que se creó el ciberespacio, pronto se vio desplazado por la estructura abierta y de finalidad múltiple de las redes basadas en la transferencia de paquetes de datos, y con ello la antigua arquitectura de distribución de la información del tipo de un emisor a muchos destinatarios (como la televisión, la radio, los periódicos o los*

ciberespacio, del capitalismo industrial al capitalismo cultural y de la propiedad al acceso, forzará una reconsideración global del contrato social. No olvidemos que la institución central de la era industrial ha sido la moderna noción de propiedad como algo privado, exclusivo e intercambiable en el mercado. Ella ha dictado los términos en que se desarrolla la vida cotidiana, ha sustentado el discurso político y se ha utilizado para calibrar el estatus de los seres humanos. Sin embargo, las nociones de acceso y redes están comenzando a redefinir la dinámica social de manera tan potente como en los albores de la era moderna lo hicieron las ideas de propiedad y mercado. Por ejemplo, hace poco la palabra acceso (*access*) se utilizaba en el mundo de habla inglesa solamente de forma esporádica y normalmente restringida a cuestiones relacionadas con la admisión a los espacios físicos.

En este sentido, la octava edición del *Concise Oxford Dictionary* de 1990, incluyó por primera vez la acepción del término *access* como verbo, indicando así una utilización más amplia: ***Access* es ahora una de las palabras más utilizadas en la vida social.** Cuando las personas oyen la palabra acceso es probable que piensen en aperturas hacia una totalidad de nuevos mundos de posibilidades y oportunidades. El acceso se ha convertido en la etiqueta o símbolo general para la realización y el avance personal, de forma tan poderosa como la idea de democracia lo fue para generaciones previas. Es una palabra con una gran carga simbólica, llena de significación política. Después de todo, el acceso es algo que hace referencia a distinciones y divisiones, que se refiere a quién está incluido y a quién queda excluido. **El acceso aparece como una potente herramienta conceptual para reconsiderar nuestras concepciones del mundo y de la economía, como la metáfora más potente de la próxima era.**[14] Por doquier existen cámaras de video que graban nuestras actividades económicas, nuestros paseos por el supermercado, por los parqueos de los centros comerciales o siquiera cuando nos interesamos por una prenda de vestir en numerosos comercios. Hasta nuestro interés momentáneo en artículos anodinos[15] como una específica marca de cereales o de galletas, genera un interés comercial y de ahí su observación minuciosa por expertos de mercadotecnia.

Ya se han desarrollado tecnologías que permiten, mediante una técnica denominada minería de datos, recopilar también los comportamientos de las personas en el diario transitar por la red de redes Internet. Con los datos e informaciones obtenidas se pueden perfilar hábitos de consumo, intereses, actividades, pasatiempos y hasta investigaciones, los cuales pueden ser utilizados para los más diversos fines: por ejemplo, envió de correos con información de interés comercial, como para que las páginas de Internet "recuerden" nuestro paso e identidad y nos saluden efusivamente, invitándonos a otra partida emocionante de compras y diversión, o para motivar causas de despido a trabajadores, al espiar el e-mail de los empleados por parte del patrón[16], a través de programas que violan el derecho a la privacidad, como el eBlaster[17], que lanzó al mercado en el 2002 la Empresa *Spector Soft* (http://www.spectorsoftt.com) fabricante de programas informáticos. Este programa está diseñado para espiar lo que otros hacen en Internet, incluyendo qué sitios visitan, sus correos electrónicos y conversaciones en el chat, con un costo de 99.99 dólares y su instalación no requiere de la autorización del usuario que será sujeto de espionaje, porque éste ni siquiera se da cuenta de que lo han instalado en su sistema. La información recabada por este software es enviada de manera automática a la dirección de correo del propietario del programa espía y éste recibe del mismo modo, y cada 60 minutos un completo informe resumido de la actividad en la Red del usuario espiado, y entre las múltiples especificaciones y ventajes que se le

---

libros) se vio complementada por otra arquitectura en la que cada persona podía ejercer como su propio redactor-jefe y publicar lo que desease, y es así que las nuevas tecnologías de la información nos llevan de la mano a una nueva cultura de la modernidad, donde los requisitos necesarios para construir una sociedad de la información en el siglo XXI ya están presentes en nuestra vida, y no podemos dar un paso sin que estén a nuestro lado".

[14] **RIFKIN, Jeremy**. *Opus cita*, páginas 25 a 27.

[15] Adjetivo que significa: Insignificante, insustancial: una película anodina. EL MUNDO.ES Diccionarios, http://www.estudiosjuridicos.turincon.com, consultado el 9 de Octubre del 2003.

[16] Chile: *Privacidad laboral*. Revista Electrónica de Derecho Informático, número 49, SNI 1576-7124. publicado en VLEX España. http://v2.lex.com/global/redi/detalle_doctrina_redi.asp?articulo=165796. Consultado el 20 de octubre del 2002. *A Interceptacao do Correio eletrónico*. Mario Antonio Lobato de Paiva. Revista Electrónica de Derecho Informático, número 51. Consultado el 29 de octubre del 2002. *Trabajo: El secreto del correo electrónico, también en el puesto de trabajo*. IURIS LEX, 11 de noviembre del 2002. dirección electrónica: http://www.iurislex.net

[17] Clara violación del derecho a la privacidad, este programa se justifica, de acuerdo con el anuncio que hace la compañía en su página web: **"Está dirigido a los padres preocupados y jefes, interesados en reducir el uso inadecuado de Internet en sus casas u oficinas".** Así, el Eblaster se instala en las computadoras de sus amigos, familiares o empleados y es capaz de registrar y guardar todos sus mensajes instantáneos, participaciones en chats y correos electrónicos, además de los botones que sean pulsados en el teclado y las direcciones electrónicas que sean visitadas, según informa orgullosamente la empresa.

atribuyen, el software puede ser programado para reconocer palabras clave y sólo almacenar la correspondencia o direcciones electrónicas que las contengan. Eso sí, apelando a la más rigurosa ética comercial, *Spector Soft* advierte a los posibles compradores que sólo deben utilizar el programa en máquinas de su propiedad, de otra forma estarían incumpliendo las condiciones de uso especificadas en las de compra.

Concluyo. La red de redes, conocida también como el ciberespacio o Internet, es la infraestructura sobre la que se está montando la nueva economía del conocimiento[18]. Para acceder a sus bondades, las reglas de la nueva cultura de la información deberán construirse, tomando en cuenta la dimensión e intensidad de los cambios que se están produciendo en todos los niveles de la vida de convivencia,[19] y es que en una economía basada en el conocimiento en el que las nuevas tecnologías avanzan a velocidad de vértigo, corremos el peligro de la despersonalización, por lo que urge la protección del individuo frente a los riesgos de pérdida de intimidad y privacidad.

En el ciberespacio debemos llegar a comprender cómo el código regula –la manera en que el *hardware* y el *software*, que hacen del ciberespacio lo que es, regulan el ciberespacio tal como es-. En palabras de William Mitchell, **"El código es la "ley" del ciberespacio"[20].** *El Código es la ley.* Este código representa la mayor amenaza para los ideales progresistas o libertarios, al mismo tiempo que su mayor promesa. **Tenemos ante nosotros dos posibilidades:** Por un lado podemos construir, desarrollar la arquitectura del ciberespacio o codificarlo para que en su seno se protejan los principios y valores que consideramos fundamentales, y por otro, podemos construir, desarrollar su arquitectura o codificarlo de modo que dichos principios y valores desaparezcan. No hay punto medio. Estas opciones conllevan un tipo u otro de construcción, pues, en efecto, el código jamás se encuentra; sólo se elabora; y somos nosotros los encargados de elaborarlo. Debemos, como ciudadanos conscientes y responsables, conocer la legislación vigente no sólo para su obligado cumplimiento, sino para participar tanto en su desarrollo como en la elaboración de nuestro propio código deontológico, para abonar el desafío de nuestra generación, que es precisamente lograr reconciliar estas dos fuerzas, pero ¿de qué modo podemos proteger la libertad cuando las arquitecturas del control están gestionadas tanto por el Estado como por el sector privado?. ¿Cómo podremos asegurar la privacidad cuando la Red está espiándonos continuamente?. ¿De qué manera podremos garantizar el pensamiento libre cuando la tendencia es etiquetar la propiedad de cada idea?. ¿Cómo garantizamos la autodeterminación cuando las arquitecturas del control se determinan siempre en otro lugar distinto al ciberespacio?.[21] La respuesta no se encuentra en la retórica del pasado. La realidad supera en dureza a la ficción; los gobiernos resultan necesarios para proteger la libertad, incluso a pesar de bastarse por sí solos para destruirla.[22] Esta nueva materia que vivimos no puede aprenderse en las bibliotecas. Lo poco que he aprendido es a través de conversaciones que he mantenido con una extraordinaria comunidad virtual de académicos, alumnos y personas interesadas en comprender lo que es el ciberespacio, así como para mejorarlo, a través de los grupos de noticias de Yahoo! de Derecho Informático (derecho-informatico@yahoogroups.com.mx), desde el año de 1999.

Las sociedades modernas se encuentran ante el dilema de proteger la intimidad en su versión patrimonialista, pero, al mismo tiempo, deben crear condiciones para mejorar la comunicación de los ciudadanos, así como su autodeterminación. Tienen que velar por un mayor intercambio de informaciones y hacer transparentes muchos de sus usos, y al mismo tiempo garantizar realmente la privacidad de cantidad de ciudadanos afectados por dichas políticas. Estos dilemas enfrentan a las sociedades modernas ante una complicadísima y difícil ponderación de intereses, donde entran en juego no solo las necesidades de información de la sociedad, y la nueva configuración de las relaciones económicas entre los países. El papel del Derecho ante el avance y aparición de estas novedades tecnológicas con que vivimos, debe ser el servir como elemento disciplinador de todo el proceso, porque **"el Derecho será quien en medio de la vorágine tecnológica provea de los dos grandes valores que persigue: seguridad jurídica y justicia"[23]** para el bien de la comunidad, reflexionando sobre la conveniencia de dar cabida a un proceso más jurisdiccional ante la aparición de los cambios que la vida moderna está viviendo. No ignoremos ni hagamos de lado que fenómenos tales como la informática, las telecomunicaciones y el desarrollo de nuevas tecnologías han venido a revolucionar la vida de las colectividades

---

[18] **CEBRIÁN, Juan Luis**. *La Red*, Barcelona, Punto de Lectura, Santillana de Ediciones S.A., 3ª Edición, año 2000, página 19.
[19] *Ibidem,* página 35.
[20] Citado en **LESSIG, Laurence**, *opus cita, página 25.*
[21] *Íbidem*, página 21.
[22] *El rol del Estado en la nueva economía digital.* Trabajo preparado por los cursantes del Posgrado en E-Bussiness Management de la Universidad del Salvador, Argentina – Georgetown University, USA, dentro de la Cátedra Marco Legal, año 2002.
[23] **C. MEJÁN, Luis Manuel**. *El Derecho a la Intimidad y la Informática*. Editorial Porrúa 1994, México.

y ponen en revolución también conceptos del Derecho. Es aquí donde debemos actuar y replantearnos a partir de nuestra interpretación, ***la función del Derecho en función de la intimidad y publicidad: el Derecho sirviendo a la informática y la informática sirviendo al Derecho***, donde el concepto de intimidad personal versus libertad de información, por señalar un ejemplo, nos lleva a una profunda reflexión psicológica, la que nos recuerda que un individuo es uno solo. Es primero lo que es y que sólo Dios conoce; es, en segundo lugar, el que él cree que es; es también el que los demás creen que es; y por último, es el que él cree que los demás creen que es.[24] La ciencia del Derecho debe ser capaz de controlar, por un lado, tanto la infraestructura de las comunicaciones como las vías de acceso y los portales que cientos de millones de personas emplearán para comunicarse, así como por otro, buena parte de los contenidos que fluyen a través de los cables y el espacio radioeléctrico, les proporciona a las empresas mediáticas mundiales un poder sin igual, donde las compañías de telecomunicaciones se están volcando en asegurarse las vías de acceso a Internet y el ciberespacio, en la esperanza de controlar un mundo electrónico en el que cientos de millones de personas pasarán la mayor parte de su tiempo (de ocio y negocio).[25]

Tal parece que con los nuevos datos que arroja la Ley de Transparencia respecto al tema del tratamiento de datos personales en ficheros informáticos, los mexicanos estamos luchando por alcanzar un estándar aceptable de tutela ante los cambios que experimenta el mundo de lo tecnológico, en choque con lo ideológico. Sin embargo, tengo claro que si no se inicia el camino hacia la tutela de los ciudadanos frente al tratamiento de sus datos personales, México perderá una importante ventaja en el proceso de integración a un mundo cada vez más dependiente del conocimiento. No podemos continuar con un enfoque tradicional en la forma de protección de la intimidad, limitándola a proteger los papeles privados y las comunicaciones telefónicas y telegráficas de los ciudadanos, sino que debe ser considerada en una nueva dimensión: (…) **de tutela de las posibilidades de participación reales del ciudadano en una sociedad que se informatiza**. Esta nueva perspectiva de la intimidad se manifiesta, entonces con la autodeterminación y las facultades de control que un ciudadano debe tener sobre el flujo de informaciones que circulan sobre sí mismo. Este derecho se vincula no sólo con la intimidad, sino también con derechos constitucionales de gran valor como la dignidad humana, la libertad individual, la autodeterminación y el principio democrático, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho. Se trata de brindar nuevas condiciones de participación social a los individuos, pero, al mismo tiempo, asegurarles el resguardo de su autodeterminación. Como bien lo postula un Comisionado de la Protección de Datos de Alemania: **"La protección de los datos es un presupuesto funcional de la sociedad de la información organizada bajo los supuestos de una sociedad de mercado que desea satisfacer las exigencias democráticas y de derechos civiles. El ser humano 'no automático' debe ser protegido en un mundo que se automatiza".**

II. METODOLOGÍA DE TRABAJO. Para llevar a feliz término la propuesta presentada en este trabajo, quiero decir que de acuerdo a la lectura de los artículos 3-I; V; XIII; 13-IV; 18-II; 20; 21, 22-V; 23; 37-VIII; IX; XII; XIII; XIV de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en adelante la Ley, y de los artículos 1, 2; 37 al 40; y 47 al 48 del Reglamento de la Ley de Transparencia (...), en lo que se refiere a datos personales, los sistemas de datos personales contemplados y a la protección de éstos, la Ciencia del Derecho de la mano del legislador, emprenderá nuevamente el tortuoso y difícil camino hacia la regulación del tratamiento de datos e informaciones personales, y lo hace justo cuando ya se empiezan a resquebrajar muchas de las instituciones tradicionales vinculadas al control institucional del tratamiento de datos. Haré énfasis en el Derecho comparado sobre este tema, y me permitiré incluir una propuesta de redacción a la Constitución Política de los Estados Unidos Mexicanos, con el objeto de dejar establecida la garantía del derecho al honor, a la intimidad personal y familiar y a la propia imagen, así como a la inviolabilidad del domicilio y correspondencia, con limitación expresa del uso de la informática para garantizar ésta, atendiendo a lo establecido ya en los artículos 14 y 16 constitucionales, y la inclusión de la figura jurídica de estos derechos,

---

[24] **PRECIADO HERNÁNDEZ, Rafael.** *Filosofía del Derecho*. Editorial JUS, México 1960. *"Los derechos fundamentales son esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana, justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado Social y de Derecho o en el Estado Social y Democrático de Derecho, según la fórmula de nuestra Constitución".*

[25] Como la industria de las telecomunicaciones, el ciberespacio fue desregulado en 1995, cuando la National Science Foundation, dependiente del gobierno estadounidense, traspasó la gestión de la red a proveedores comerciales. Hoy día éstos son los que garantizan nuestro acceso al ciberespacio. Mañana estará en manos de los grupos mundiales constituidos por los gigantes de las telecomunicaciones, los medios de comunicación y la informática, donde su objetivo principal, será el de controlar la transmisión digital de voz, video, datos y otros productos en cada región y mercado del mundo.

conocida como Habeas Data.[26] La propuesta se antoja difícil: plasmar en un espacio de 30 cuartillas las ideas centrales y la propuesta general, representa un reto extraordinario, donde se pondrá a prueba nuestra capacidad de análisis y síntesis, esperando no dejar nada en el camino de la discusión, y antecediendo mil disculpas si la propuesta excede unas cuartillas de lo solicitado.

III. ANTECEDENTES GENERALES DE LOS DATOS PERSONALES CONTENIDOS EN FICHEROS INFORMÁTICOS. La protección de los datos personales en México es un tema que ha empezado apenas a ser objeto de debate y discusión, y prácticamente no contamos todavía en la materia con un marco legal integral que establezca los instrumentos y mecanismos diseñados para tal fin. En la actualidad, nuestro sistema jurídico cuenta con la Ley Federal de Acceso a la Información Pública Gubernamental, que acaba de entrar en vigor el 12 de junio del 2002, en donde en un breve apartado regula la protección de los datos personales derivada de los archivos que se manejan para hacerlos públicos a los interesados.

Entra en esta materia, la Ley para Regular las Sociedades de Información Crediticia, publicada en el Diario Oficial de la Federación el día 15 de enero de 2002, la cual dispone que quienes manejan la información personal de los usuarios de los servicios financieros, en donde se conforman historiales crediticios, deben obedecer a reglas especiales, para evitar el uso indiscriminado e injustificado que pudiera darse a dicha información con que cuentan éstas sociedades en sus bases de datos. El proyecto inicial disponía las reglas básicas para este tipo de sociedades en materia de datos personales, sin embargo, se suprimió para evitar cualquier conflicto de normas que pudiese suscitarse. En el océano de la legislación mexicana encontramos también normas protectoras de los datos personales en la materia de protección al consumidor, cuando se trate de la recolección de información por las empresas de mercadotecnia relacionadas con esa actividad, así como reformas a los registros de datos en el Registro Público de la Propiedad y otras reformas introducidas al Código Civil Federal en mayo del 2002.

A) ¿Por qué este proyecto?. Lo formulo debido, en principio, a la ausencia de un marco regulatorio de esta naturaleza en México. En su concepción, he buscado que el marco de su desarrollo sea protector de las garantías y derechos del ciudadano, en atención, tanto a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, como en la Ley Federal de Transparencia y Acceso a la Información Pública y su reglamento; y por otro lado, brindar los instrumentos necesarios para hacer valer los derechos inherentes a esa tutela. La protección jurídica que se plantea se encamina a proteger y resguardar valores como el honor, la intimidad de las personas y la repercusión familiar que éste pudiere tener por la información contenida en las bases de datos y el tratamiento que deba dárseles, así como la propuesta para incluir en el texto, la figura del *Habeas Data,* entendida como la **acción procesal que permite al ciudadano defender su derecho al respeto y a su vez el acceso a su información personal, atendiendo al principio de consentimiento**, es decir, que sólo se pueden recolectar datos personales destinados al reparto de documentos, publicidad, venta directa, o bien cuando se trate de encuestas de opinión, investigación científica u otras actividades análogas, mediante el previo consentimiento del titular de esos datos. Se establece, que al recolectar previo consentimiento del titular, se deben destinar los datos al objeto exclusivo que originó la recolecta.

B) El tratamiento en la recogida de datos. No se pueden recoger datos personales porque sí. Sólo pueden recogerse ***mediando determinadas circunstancias***. La primera de todas, que es una declaración de principios establecida en la Ley, es que sólo se pueden recoger y tratar datos personales, **sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido, además de que requieren del consentimiento de los individuos para su difusión, distribución o comercialización;**[27] (fracción II artículo 18 y 21; fracción III, artículo 20 de la Ley), así como el poner a disposición de los individuos el documento en el que se establezcan dichos propósitos para su tratamiento, en términos de los lineamientos establecidos por el IFAI o la instancia equivalente (fracción IV, artículo 20). Es éste un criterio muy general, pero que sirve para conocer los criterios en que la Ley se basa. Los datos no se pueden obtener indiscriminadamente por el puro placer de obtenerlos. Pueden obtenerse, sí, pero en un contexto

[26] **CHIRINO SÁNCHEZ, Alfredo, Dr. /CARVAJAL, Marvin, Dr.** *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. Año 2003.

[27] Vale como consentimiento manifestado por el interesado, toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos que le conciernen. No es preciso, sin embargo, cuando se refieran a las partes de un contrato o precontrato de una relación negocial o laboral y sean necesarios para su mantenimiento o cumplimiento, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

adecuado, mediando buena fe por parte de quien los obtiene.[28] Y agrego, ***el consentimiento puede ser revocado por el interesado cuando exista causa justificada para ello, sin efectos retroactivos***. Y además éste, en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal y siempre que una ley no disponga lo contrario, podrá oponerse a su transmisión cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero está obligado a excluir del tratamiento, los datos relativos al afectado. Por ejemplo, está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos, como lo prevé el artículo 21 de la Ley. Es una prohibición muy general, pero que con un poco de sentido común resulta fácil de concretar. Pero hay otra cosa clara: determinados datos están además **especialmente protegidos también para su recogida**. Cuando se trata de solicitar datos que puedan tener cualquier relación, por remota que sea, con la ideología, religión o creencias, o afiliación sindical, es una obligación legal recabar de modo expreso y por escrito el consentimiento del afectado para el tratamiento de sus datos, y además, debe advertirse igualmente de modo expreso, que tiene derecho a no prestar su consentimiento.[29] En materia de cesión de datos personales rige el mismo principio, **previendo que la cesión se hará a persona con interés legítimo, informando de manera cabal sobre la identidad del cesionario y la finalidad que persigue la cesión** (fracción IV, artículo 22 de la Ley). Así mismo se permite que se revoque la cesión, mediante una notificación al titular del archivo, registro, base o banco de datos. Sin embargo, el proyecto permite que no se requerirá del consentimiento cuando la propia ley así no lo exija, se realice entre dependencias y organismos públicos y el registro conste que la información en cuestión sea de consulta pública y gratuita.

En teoría, el responsable del fichero en el momento en que se efectúe la primera cesión de datos, debe informar de ellos a los afectados, indicando la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. Podemos encontrar que en la práctica esta obligación no exista, cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros[30]. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. Tampoco será aplicable, si la comunicación se efectúa previo procedimiento de disociación, entendido éste como **"Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable".**

C) La obligación jurídica[31] a cargo de los sujetos obligados en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para implementar políticas de protección de datos personales en ficheros informáticos. Culturalmente hemos asumido la percepción de que si no tenemos nada que ocultar, tampoco debemos preocuparnos porque otros sepan sobre nosotros, acerca de nuestros gustos o apetencias. En general, consideramos que si entregamos datos a empresas financieras y bancarias, lo que estamos haciendo es contribuir al buen servicio que nos prestan, sin tomar en cuenta los riesgos que afrontamos ante tal liberalidad. Los inmensos bancos de datos del Estado, pero también los construidos por los particulares, ofrecen un muestrario sorprendente de posibilidades de control, no sólo para desestimular a los que realizan actividades

---

[28] Piénsese en el caso de recoger los datos de nombre, apellido, domicilio, CURP, cuenta bancaria y estado civil de una persona, cuando ésta decide comprar un electrodoméstico. La finalidad de recoger estos datos personales en este supuesto parece claro. Es decir, pueden ser útiles para la entrega del electrodoméstico comprado en el domicilio de la persona, también pueden ser adecuados para la realización de la factura o como datos contables para el vendedor. No obstante, existe un dato (estado civil) que no tiene relación alguna con las finalidades expuestas, por lo que considero, este dato es inadecuado, no pertinente y excesivo en relación con la recogida.

[29] Hay una excepción, contemplada en el artículo 22 de la Ley, a lo comentado. Entre los datos mencionados, pueden ser objeto de tratamiento los necesarios para la prevención o el diagnóstico médicos, la prestación de asistencia médica o la gestión de servicios de salud; los necesarios por razones estadísticas, científicas o de interés general previstas en la Ley, previo procedimiento **por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;** cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos; cuando exista orden judicial; a terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales, quienes no podrán utilizar con propósitos distintos los datos transmitido, y en los demás casos establecidos por las leyes.

[30] **En este caso no se considerará comunicación de datos el acceso de un tercero a éstos, cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.** Por ejemplo, cuando una empresa subcontratista tiene que reparar el equipo informático del responsable del fichero.

[31] **PONCE SOLE, Juli**. *Deber de una buena Administración y Derecho al Procedimiento Administrativo Debido. Las bases constitucionales del procedimiento administrativo y del ejercicio de la discrecionalidad.* 1ª edición, febrero 2001.

ilícitas, sino también para controlar a aquellos que eventualmente manifiesten algún interés sospechoso, y es por ello que la Ley prevé estas situaciones, al garantizar la protección de los datos personales en posesión de los sujetos obligados (artículos 3 fracción XIV, 4 fracción III, y 20 fracción VI de la Ley). El gran reto de la nueva era de la información lo constituye, sin duda, como lo expone el Comisionado Federal para la Protección de datos de Alemania, Joachim Jacob[32] **"La interconexión que es posible alcanzar con la ayuda de la moderna tecnología, muy especialmente a nivel de los ciudadanos y sus hogares"**. Este reto nos obliga a repensar los medios utilizados hasta ahora para proteger la intimidad y la autodeterminación informativa de los ciudadanos. El desarrollo vertiginoso de la tecnología ha llevado a la moderna sociedad de la información a convertirse en una verdadera aldea global, la cual ha superado, con creces, la velocidad de adaptación que fue necesaria para alcanzar un uso global del teléfono o del fax. Hoy día, más personas hacen uso de la Internet y la cantidad de información que circula en la Red se duplica cada cien días, según datos del Ministerio de Comercio de los Estados Unidos[33]. Desde una doble perspectiva, reconocemos que es nuestro derecho como ciudadanos la protección adecuada de nuestra privacidad, y nuestro deber como suministrador de tecnología, en caso de así serlo, de servir como facilitadores al acceso a las tecnologías que ayuden en la consecución este derecho. ¿Quién no se ha preguntado alguna vez si aquellos que tratan sus datos personales no tendrán demasiada información sobre su vida privada y cotidiana?. Es obvio que debe existir un control sobre nuestros datos personales para que podamos sentirnos protegidos. Sería importante obligar a los administradores de los sitios web, a tratar en forma adecuada los datos personales de sus usuarios, además de imponer con carácter de obligatorio la generalizada costumbre de incluir a pie de página una mención a la *Política de Privacidad*[34] con un enlace a una página que detalle sus lineamientos, lo que en la práctica es sólo una promesa normalmente incumplida.

IV. LA EXPERIENCIA DEL DERECHO INTERNACIONAL

ALEMANIA. Hoy la protección de datos experimenta un proceso muy interesante de reformas, algunas de las cuales han permitido el desarrollo internacional de las disposiciones de tutela. La Ley Federal de Protección de Datos de Alemania ya ha incluido dentro de sus disposiciones algunos principios largamente acariciados por los expertos y los ciudadanos como el principio de evitación de datos y de ahorro de datos, que no son otra cosa que la aplicación en la práctica del principio de proporcionalidad en esta materia, concretamente del subprincipio de necesidad. Se incluye en el texto de la Ley la llamada auditoría de protección de datos (*Datenaudit*), que no es más que una regulación complementaria a las ya establecidas de orden institucional y que persigue que haya auditorías llevadas a cabo por expertos particulares, quienes observen en los sistemas la efectiva realización de los principios vigentes en la materia. Todos estos cambios han sido bien recibidos por los comisionados de la Protección de Datos,[35] quienes las observan como pasos decididos hacia una modernización del estándar de la protección de datos en Alemania y también en Europa, cuyos lemas de campaña son: **"protección de datos por medio de la técnica", y "mayor transparencia del procesamiento de datos"**[36].

UNIÓN EUROPEA. La Unión Europea ha avanzado hasta poner en vigencia una reglamentación sobre protección de datos, y lo mismo ha sucedido en la famosa "Carta de la Unión Europea" que ha reservado un lugar privilegiado para la autodeterminación informativa. Debe distinguirse esta reglamentación de la así denominada "Línea Directiva de la Unión Europea en materia de protección de datos"[37], la cual, en realidad, se

---

[32] Comunicado de prensa, en: http://www.bfd.bund.de/aktuelles/pm19990504.html

[33] Junto a este crecimiento exponencial de los usos de Internet, debemos contar la creciente velocidad de procesamiento de los computadores y de los chips que les permiten las fantásticas prestaciones que hoy tienen. Los chips han visto incrementada su capacidad de procesamiento de una manera sorprendente, pasando de ejecutar 60.000 instrucciones por segundo a hacerlo en cientos de millones. En palabras de Nathan Myrvald, Vicepresidente para Tecnología de Microsoft, se trata de un panorama impresionante: "Dentro de veinte años, una pc realizará en treinta segundos las tareas para las que hoy necesita doce meses. Dentro de cuarenta años, llevará a cabo en treinta segundos aquello para lo que hoy necesitaría un millón de años". Myrvald, Nathan, Intervención en el foro organizado por Variety y Time Warner, Nueva York, 1994.

[34] Artículo 20 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. **Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán: **I. (...) dar a conocer información sobre sus políticas en relación con la protección de tales datos (...)**, y artículos 47 y 48 del Reglamento de la Ley.

[35] Resolución emitida por los comisionados de Protección de Datos de Alemania del 10 de octubre de 2000.

[36] Quinto Informe del Comisionado de la Protección de Datos de Mecklenburg-Baja Pomerania, página 29.

[37] Directiva del Parlamento Europeo y del Consejo sobre la Protección de Personas Físicas frente al procesamiento de sus datos personales y el libre tránsito de datos del 20 de febrero de 1995.

refiere a temas que deben ser puestos en vigencia por los Estados miembros de la Unión Europea, así como por sus órganos e instituciones. La reglamentación tiene el fin de proteger a las personas objeto de tratamiento de datos por parte de órganos e instituciones de la Unión Europea. Contiene, entre otras regulaciones, la prohibición para los referidos órganos e instituciones de enviar datos personales a países fuera del ámbito de vigencia de esta reglamentación, que no tengan un nivel de protección similar al europeo[38]. Los datos respecto de temas sensibles, como el origen o las convicciones religiosas de las personas, únicamente pueden ser tratados de manera automática en casos excepcionales. También contempla regulaciones sobre el aseguramiento técnico de los datos, los cuales, desgraciadamente, deben contemplarse como superados, no obstante la importancia de considerar este tema en la misma reglamentación[39]. Otros aspectos interesantes de esta normativa lo son: **a) Inclusión de un Comisionado de la Protección de Datos**, al que, entre otras funciones, le corresponde velar por el cumplimiento de la reglamentación a lo interno de la oficina a su cargo. Junto a este Comisionado, se ha decidido nombrar una **b) autoridad de control constituida por el Comisionado Europeo de la Protección de Datos**, quien aconseja y controla a los órganos e instituciones de la Unión Europea en esta materia. Para cumplir con esta tarea se le conceden amplios poderes de acceso a todas las oficinas y centros de procesamiento, a todos los datos personales y a todas las informaciones generadas en el ámbito de la Unión. Contra las decisiones de este alto Comisionado sólo se puede iniciar demanda ante el Tribunal Europeo. Las personas afectadas por procesamiento de datos prohibidos en el ámbito de la Unión, tienen derecho a solicitar información, a obstruir datos y a solicitar y lograr la eliminación de datos e informaciones que le afecten. También pueden acudir directamente ante el Comisionado Europeo. Más importante que lo anterior es que el ejercicio de los derechos que contempla la reglamentación no generan costos para el afectado, lo que indica que esta reglamentación es mucho más amigable con el ciudadano afectado que la misma Línea Directiva del Consejo de Europa[40], la cual indica que las normativas que se dicten, según la mencionada Directiva, no deben incluir costos que sean "exagerados" para el afectado.

ESPAÑA. Existen una serie de antecedentes que son fundamentales para comprender la legislación vigente en materia de protección de datos de carácter personal. Estos antecedentes se remontan a finales de la década de los 70, lo que indica el grado de preocupación que este tema ha suscitado ante la sociedad. La Organización de Naciones Unidas recoge hace tiempo una serie de principios rectores aplicables a los ficheros automatizados de datos personales que han sido la base de la actual legislación. Estos principios son: **a)** Principio de licitud y lealtad; **b)** Principio de exactitud; **c)** Principio de finalidad; **d)** Principio de acceso a la persona interesada; **e)** Principio de no discriminación; **f)** Facultad de establecer excepciones; **g)** Principio de seguridad; **h)** Control y sanciones; **i)** Flujo transfronterizo de datos; **j)** Campo de aplicación. Asimismo, encontramos una serie de convenios internacionales que han influido también tales como: **La Declaración Universal de los Derechos Humanos** adoptada y proclamada por la ONU el 10 de diciembre de 1948. **Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales** de 4 de noviembre de 1950. **Convenio 108 de 28 de Enero de 1.981**, del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal. Donde al igual que en la ONU se establecen una serie de principios fundamentales referentes a la calidad de datos, la sensibilidad de los mismos, las medidas de seguridad, las sanciones y recursos y los flujos internacionales de datos. En este ámbito nos podemos remontar a las resoluciones y recomendaciones del Consejo de Europa: **Resolución 721/80.** Informática y protección de los derechos del hombre. **Recomendación 890/80.** Protección de datos de carácter personal. **Recomendación 1037/86**. Protección de datos y libertad de información. Otras recomendaciones aplicables a datos médicos, de investigación científica y estadística, de marketing directo, de seguridad social, de policía, de empleo, etc. En el ámbito español podemos encontrar antecedentes en la propia Constitución española (artículo 18.4 donde se emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos) y más concretamente en: **Ley 9/1986**, de 5 de abril, sobre Secretos Oficiales; **Ley 62/78**, de 26 de diciembre, de Protección Jurisdiccional de los Derechos Fundamentales de la Persona; **Ley Orgánica 1/82**, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad personal y familiar y a la propia imagen, modificada por Ley Orgánica 3/85, de 29 de mayo; **Ley Orgánica 3/86**, de 14 de abril, de Medidas especiales en materia de Salud Pública, y **Ley 14/86**, de 25 de abril,

[38] La Ley de Protección de Datos de Inglaterra (UK Data Protection Act de 1998, Schedule 1, Part. 1, Section 8) incluye una norma similar: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

[39] Quinto Informe del Comisionado de la Protección de Datos de Mecklenburg-Baja Pomerania, página 30. Están superados si se toma en cuenta el nivel de seguridad técnica con el que cuentan algunas leyes de los Länder luego de las reformas posteriores al año 2000.

[40] *Quinto Informe del Comisionado de la Protección de Datos de Mecklenburg-Baja Pomerania*, página 31.

General de Sanidad; **Ley 12/89**, de 9 de mayo, de la Función Estadística Pública; **Ley 22/87**, de 11 de noviembre, de Propiedad Intelectual, modificada por la Ley 20/92, de 7 de Julio.

En la década de los 90 en España, como país interesado en regular el uso de los datos personales, cobra mayor auge la necesidad de legislar acerca del tema que nos ocupa. En el año 1992 nace la conocida LORTAD (*Ley Orgánica del Tratamiento Automatizado de Datos*), que ha dado lugar a un desarrollo normativo en los que cabe destacar: **Ley Orgánica 5/92** de 29 de Octubre de Regulación del Tratamiento Automatizado de Datos; **Real Decreto 1332/1994**, de 20 de junio, por el que se desarrolla 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**, de 1 de marzo, de la Agencia de protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito; **Directiva 95/46** del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; **Instrucción 1/1996**, de 1 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 de 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; **Real Decreto 994/1999**, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal; **Ley Orgánica 15/1999** de 13 de diciembre de Protección de Datos de Carácter Personal; **Real Decreto 1906/1999** de 17 de diciembre por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación; **Real Decreto 195/2000**, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio.

La Ley Orgánica 15/1999 de 13 de Diciembre viene a renovar a la LORTAD. Evidentemente tiene por objeto el mismo que el mencionado artículo 18.4 de nuestra Constitución y es de aplicación tanto a los ficheros públicos como privados que contengan datos de carácter personal. Existen unas excepciones a dicha Ley que son los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, los ficheros sometidos a normativas propias sobre protección de materias clasificadas, y los ficheros para la investigación del terrorismo y formas graves de delincuencia organizada, aunque es necesario que el responsable de este tipo de ficheros comunique la existencia, características y finalidad del mismo a la Agencia de Protección de Datos. Además, determinadas materias se rigen por disposiciones propias tales como el Régimen Electoral, la Función Estadística Pública, la Legislación Autonómica, el Régimen del Personal de las Fuerzas Armadas, el Registro Central de Penados y Rebeldes y las de imágenes y sonidos procedentes de las Fuerzas y Cuerpos de Seguridad. **En cuanto a los principios que rigen la protección de datos, la ley establece los siguientes en los artículos del 4 al 12:**

a) La Calidad de los Datos, en referencia a que los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido.
b) El derecho de información en la recogida de datos, mediante el cual en el momento de la recogida de los datos se deberán expresar precisa e inequívocamente la existencia del fichero, su finalidad, los destinatarios de la información, el carácter obligatorio de las respuestas a las preguntas planteadas, las consecuencias de la obtención de los datos o de la negativa a facilitarlos, la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y la identidad y dirección del responsable del fichero.
c) El consentimiento del afectado, cuya regla general es que el tratamiento requerirá el consentimiento inequívoco del afectado salvo determinadas circunstancias.
d) Los datos especialmente protegidos, referente a la obtención de datos con determinados orígenes. Así se clasifican como datos de protección máxima aquellos referentes a ideologías, afiliación sindical, religión o creencias, y como datos de protección media aquellos referentes al origen racial, salud o vida sexual. Respecto a los primeros se garantiza que nadie puede ser obligado a declarar sobre estos datos, salvo que el afectado consienta expresamente y por escrito, y además existe la obligación de advertir al interesado de su derecho a no prestar su consentimiento. Respecto a los de protección media sólo se recogerán cuando una Ley lo disponga por razones de interés general o el afectado lo consienta expresamente.

e) Los datos relativos a la salud. Estos pueden ser objeto de tratamiento por los profesionales a los que se acuda para ser tratados por los mismos.
f) La seguridad de los datos, en referencia a que el responsable de los mismos debe adoptar las medidas necesarias para mantener su seguridad, evitando la alteración, pérdida y tratamiento o acceso no autorizado. Además se prohíbe el tratamiento en lugares y sistemas que no reúnan las condiciones adecuadas para garantizar la integridad y seguridad de los datos.
g) El deber de secreto, cuya obligación afecta al responsable del fichero y demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, incluso después de haber finalizado la relación con el titular o el responsable del fichero.
h) La comunicación de datos. Esta comunicación a terceros solo se puede hacer para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario con previo consentimiento del interesado. Además se establecen determinadas salvedades.
i) El acceso a los datos por cuenta de terceros, regulando este tipo de accesos.

Otro aspecto a destacar en la Ley, en cuanto a su relación con el ejercicio diario de nuestra profesión, es la de la definición y regulación de la Agencia de Protección de datos, por cuanto supone el organismo de referencia para cualquier acción relacionada con la protección de datos de carácter personal. La Agencia de Protección de Datos se define a través de los artículos 35 al 42 de la Ley Orgánica 15/1999. **Es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y cuya finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales informatizados y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.** Sus funciones incluyen inicialmente la de emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias, dictar instrucciones para adecuar los tratamientos a la Ley, atender las peticiones y reclamaciones formuladas por personas afectadas, proporcionar información acerca de los derechos en materia de tratamiento de datos de carácter personal, requerir que se adopten las medidas necesarias para la adecuación del tratamiento de los datos a las disposiciones de la Ley, ejercer la potestad sancionadora, informar de los proyectos de disposiciones generales que desarrolle la Ley, recabar a los responsables de ficheros cuanta ayuda e información sea necesaria para el desempeño de sus funciones, velar por la publicidad de la existencia de los ficheros, ejercer control y cooperación sobre los movimientos internacionales de datos, y velar por el control sobre los ficheros con fines estadísticos.

A través de su página en Internet http://www.agenciaprotecciondatos.es, el lector tiene acceso a gran cantidad de información, acceso a modelos y formularios, recomendaciones y la posibilidad de realizar consultas directas a la Agencia. Además permite la realización del registro obligatorio de los ficheros que contengan datos de carácter personal. Respecto al resto de los título que aparecen en la Ley tales como los Derechos de las Personas, las Disposiciones Sectoriales, el Movimiento Internacional de Datos y las Infracciones y Sanciones remito a lector al texto de la propia Ley, ya que sería imposible realizar un análisis en profundidad de los mismos y quizás, en algunos casos, se perdería el aspecto práctico de referencia que pretende este artículo.

LA CARTA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, que fuera anunciada el día 7 de diciembre de 2000 en Niza, contiene un artículo 8, el cual regula detalladamente aspectos relacionados con la protección de datos, siguiendo muy de cerca la normativa alemana. El texto reza: "(1) Toda persona tiene derecho a la tutela de sus datos personales. (2) Estos datos sólo deben ser procesados de buena fe para el fin preestablecido con el consentimiento de la persona afectada o para cumplir con los fines establecidos con un adecuado fundamento legal. Toda persona tiene el derecho a recibir información sobre los datos referidos a su persona que hayan sido recogidos y a lograr su rectificación. (3) El cumplimiento de estas reglas será vigilado por un centro independiente". El artículo 42 de la Carta garantiza, adicionalmente, un derecho de acceso a los documentos del Parlamento Europeo, del Consejo y de la Comisión. Aun cuando la Carta no tiene un efecto jurídico directo en la práctica, sí es una fuente de interpretación para los órganos e instituciones de la Unión Europea, y objeto de aplicación jurídica y estudio por parte del Tribunal Europeo. En todo caso, se nota la gran importancia que se le ha concedido al derecho de la protección de datos en el ámbito europeo, aspecto que terminará por trasladarse a los Estados miembros y a los países que vayan a tener una relación económica directa con la Unión Europea.

V. CONSIDERACIONES FINALES. Los sistemas de tratamiento de datos están al servicio del hombre. Deben, cualquiera que sea la nacionalidad o residencia de las personas físicas, respetar las libertades y derechos fundamentales de éstas, y en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos, ya que se recurre cada vez más al tratamiento de los datos personales en diferentes sectores de actividad económica y social, debido al avance de las tecnologías de la

información, que facilitan considerablemente el tratamiento e intercambio de dichos datos. La crisis del concepto de intimidad y las limitaciones que ofrece la tradicional consideración constitucional de éste, han llevado a la necesidad de producir esquemas legislativos que ofrezcan opciones al ciudadano para proteger sus derechos constitucionales, muy especialmente su derecho a la autodeterminación. Fue así como se promulgó la Ley de Protección de Datos del Estado de Hesse en Alemania, que ostenta el honor de ser la primera ley emitida en el mundo para garantizar al ciudadano este derecho. Otros países han preferido constitucionalizar el derecho de acceso a los datos personales[41]. Ejemplos de esta tendencia los encontramos en Colombia y Brasil, también Paraguay en la Constitución de 1992 (artículo 136) y Ecuador en la Constitución del 18 de junio de 1996[42]; y en Argentina la Constitución de las provincias de Jujuy, La Rioja, San Juan, Córdoba, San Luis, Río Negro, Tierra del Fuego y Buenos Aires han incorporado cláusulas referidas a la informática y a la protección de la intimidad. La Constitución de la República de Argentina de 1994 ha establecido la acción de amparo para **"...conocer los datos a ella referidos, así como su finalidad, contenidos en registros públicos y privados, y en caso de ser ellos falsos o discriminatorios, exigir su supresión, rectificación, actualización y confidencialidad"**.

El debate sobre la necesidad de la constitucionalización sigue vigente en Alemania y en otros países, y los ecos de esta discusión han llegado hasta el ámbito de la Unión Europea. **Las voces a favor indican la necesidad de darle un adecuado rango constitucional a este derecho que supera, en mucho, la tradicional tutela ofrecida por la intimidad en su versión tradicional.** Las voces en contra, indican que la inclusión del derecho a la autodeterminación informativa es innecesaria, y que basta con los avances legislativos hechos en campos especiales para contar con una tutela completa. La verdad que el debate parece tener interés en los países que no tienen aun una tutela legal y específica sobre el tratamiento de datos personales y pueden disponer de tiempo para lograr una adecuada conexión entre las disposiciones constitucionales y la regulación legislativa. Esto significa, por supuesto, que **existe la posibilidad –**en un corto período**– de incluir este derecho en la Constitución Política y de contar con un plazo apropiado para poner en vigencia una reglamentación específica para regular los muchos campos en que tiene incidencia la protección de datos**. Este último supuesto no suele ser alcanzable en muchos países y pone en peligro tanto el objetivo de lograr un estándar normativo aceptable y la meta de una conveniente implementación de las normas de tutela en la práctica. Por esto, constitucionalizar el derecho a la autodeterminación informativa es un primer paso, no siempre necesario, y que requiere de una actividad posterior del legislador conducente a crear las condiciones, en un plano normativo, para lograr un adecuado control del tratamiento de datos, lo que no deja de tener problemas, como observamos si tomamos en cuenta la evolución de las leyes en la materia. **La correcta posición sobre el tema, más bien sería observar las oportunidades de aprendizaje planteadas por los retos mismos derivados de las tecnologías de la comunicación y la información.** Precisamente en esta lógica es que las nuevas leyes que han venido produciéndose, han tratado de enriquecer, por ejemplo, el papel de las instancias de control, y han procurado darle cada vez más derechos a los comisionados de Protección, con el fin de que estos velen por la realización práctica de los principios que informan la protección de datos y que son el "núcleo duro" dentro del cual aun se mueve el proceso de reforma. Otros aspectos interesantes en este proceso de aprendizaje lo han sido, sin duda, las diversas experiencias de los países en cuanto a la regulación planteada a partir de la forma del procesamiento, tanto manual como electrónico (lo que plantea la cuestión de cuándo se está en presencia de uno u otro), y la difícil cuestión de dar alguna respuesta a la pregunta de si ciertos datos personales pueden o no tratarse, es decir, en concreto, la referencia a los caracteres que permiten definir cuándo un dato es sensible o no.

En todo caso, estas leyes demostraron ser esenciales como complemento de las garantías generales del Estado de Derecho. Permiten un control no sólo de los así denominados centros de procesamientos públicos, sino también de los privados, garantizando al mismo tiempo derechos a recibir información, a borrar u obstruir el uso de datos que afecten el derecho del ciudadano a saber quién, cuándo y bajo qué circunstancias tiene acceso a sus datos personales. El concepto tradicional de intimidad está envuelto en una crisis evidente.[43] Ya no es posible

---

[41] Para la consulta de estas constituciones: http://www.estudiosjuridicos.turincon.com

[42] Artículo 30 de la Constitución de la República de Ecuador, Ley 000.R0/969 de 18 de junio de 1996. **"Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad. Igualmente podrá solicitar ante funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellas si fueran erróneas o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional"**.

[43] **SÁNCHEZ, Chirino y ALFREDO, Eric.** *Autodeterminación informativa y Estado de Derecho en la sociedad tecnológica*, San José, CONAMAJ, 1997, página 16 y ss., en el mismo sentido, y planteando la cuestión en el contexto español: **CASANOBA ROMEO, Carlos María.** *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*. En: *Revista del Poder Judicial de España*, número 31, septiembre, 1993, pp. 163-204.

mantener una tutela basada en los conceptos decimonónicos y burgueses de la intimidad, sino que es necesario dar algunos pasos y comprender el grado de contaminación que ha sufrido este derecho, producto del desarrollo tecnológico.

1. PROPUESTA PARA INCLUSIÓN DE GARANTÍAS AL TEXTO CONSTITUCIONAL

> **Artículo ....** La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
>
> Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar, así como a conocer toda información que sobre ella hayan registrado las autoridades federales, estatales, municipales, así como el derecho de saber por qué y con qué finalidad tiene esta información.

2. POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES. En el texto del reglamento de la Ley ***se deberá establecer un límite sobre la tenencia y utilización de este tipo de datos así como sobre el tráfico de los mismos, con niveles de seguridad, para garantizar el control de acceso a los sistemas de información en el tratamiento de dichos datos***.[44] De esta manera, la instancia que tenga a su cargo el tratamiento de los mismos, se encarga de facilitar al ciudadano el derecho a conocer quién está utilizando sus datos personales y para qué, y negar el permiso sobre el uso de sus datos a quien considere oportuno. Esto es, detallar en el texto de la misma, que los datos personales son cualquier información referida a personas físicas o jurídicas –morales- determinadas o determinables, con la protección de los datos personas asentados en archivos, registros, bancos de datos u otros mecanismos técnicos de tratamiento de datos, sean éstos públicos o privados, destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre las mismas se registre. Lo que buscamos es **proteger aspectos de la personalidad[45] que individualmente no tienen mayor trascendencia, pero que al unirse con otros, pueden configurar un perfil determinado de las personas.[46]** Las condiciones en que debe regularse el contenido de la parte relativa a los datos personales, recogida de datos, tratamiento de datos, mantenimiento de las bases de datos, criterios de selección y demás elementos, podemos resumirlas en las siguientes características[47]:

a) Todo procesamiento automático de datos debe contemplar su objetivo concreto, así como sus fundamentos jurídicos, de tal manera que puedan reconocerse, fácilmente, los usos antijurídicos de información.
b) Deben concebirse conceptos de seguridad que tomen en cuenta las condiciones personales y organizatorias disponibles, de tal manera que se le impida a personas no autorizadas el acceso a dispositivos de almacenamiento de información, en donde se encuentren grabados datos personales. De esta manera se pretende evitar que dichos datos lleguen a manos no autorizadas y puedan ser procesados afectando a las personas a las que hacen referencia. También se pretende con este tipo de

---

[44] *Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal,* publicado en el Boletín Oficial del Estado (ESPAÑA) número 298, artículo 3 inciso c), y *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*. Real Decreto 994/1999 del 11 de junio, publicado en el Boletín Oficial del Estado (ESPAÑA) número 151 del 25 de junio de 1999, artículo 2.

[45] **ESPADA RAMOS, María Luisa**. *Tendencias actuales de la responsabilidad.* Anuario Jurídico X, año 1983, UNAM-México, página 463 y ss. **CARDENAL MURILLO, Alfonso, y SERRANO GONZÁLEZ DE MURILLO, José Luis**. *Protección penal del honor*. Monografías CIVITAS, España, 1ª edición 1993. **GUTIÉRREZ Y GONZÁLEZ, Ernesto.** *El Patrimonio*. México 1992, 4a edición, Editorial Porrúa.

[46] Los Derechos de la Personalidad, como lo enseña el Doctor Gutiérrez y González, "... son normalmente extrapatrimoniales, intransmisibles e inembargables, se tienen por sí, *erga omnes*; existe un deber universal de respeto hacia ellos. (...) deben catalogarse como derechos patrimoniales. No hay razón para negar esta afirmación. (...)

[47] *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995*, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Ley Orgánica 15/1999,* 13 de diciembre, de Protección de Datos de Carácter Personal, publicado en el Boletín Oficial del Estado (ESPAÑA) número 298, del 14 de diciembre de 1999.Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contienen Datos de Carácter Personal (ESPAÑA). **MICROSOFT**. *La protección de datos personales. Soluciones en Entornos Microsoft.*

medidas tener claridad de la amplitud del procesamiento de datos, así como de la dimensión temporal dentro de la cual se realiza.

c) El uso de sistemas técnicos de información solamente puede ser autorizado una vez que el usuario de turno demuestre su condición de tal (normalmente esto se demuestra una vez que la palabra clave ha sido autorizada mediante un procedimiento de autenticación automática).
d) El derecho a intervenir a nivel del sistema solamente puede ser concedido a un número limitado de personas (nivel de administrador). A estos administradores se les debe llevar un control personalizado, así como una protocolización de sus intervenciones en el sistema.
e) Todo tipo de acumulación de datos que se encuentre grabada en dispositivos de almacenamiento, y que deba ser mantenida fuera del ámbito de seguridad de un lugar de procesamiento, tal y como sucede en supuestos de "teletrabajo" o en el servicio exterior, debe ser encriptado, principalmente con el fin de evitar los daños que podrían ocasionarse a los afectados en caso de robo.
f) Si los datos deben ser grabados exclusivamente de manera electrónica, entonces debe llevarse un control en los registros magnéticos mismos (ante la ausencia de respaldos en papel) de los cambios que se hayan hecho a las informaciones, así como de las personas que los realizaron.
g) Todos los componentes de hardware y software utilizados en un lugar de procesamiento, deben ser adecuadamente registrados con el fin de que se pueda reconocer cualquier tipo de componente ilegal: todo aquello que no esté registrado debe ser desactivado.
h) Deben protocolizarse las personas que tienen acceso, desde cuándo y qué tipo de derechos de uso han tenido y a qué parte del hardware o de los componentes de software del sistema, a fin de que puedan ser corroborados mediante comparación con los datos que hayan colocado los responsables del acceso.
i) El procesamiento automático debe ser probado acorde con su "uso real" y ha de ser puesto a disposición por los encargados del sistema. Con el fin de lograr esto es que se debe documentar su uso, de tal manera que sea comprensible para un experto en un tiempo razonable.
j) El "uso real" del proceso automático debe ser vigilado de tal manera que se determine si las instrucciones de la dirección están apegadas a las disposiciones vigentes. Toda desviación de las autorizaciones para el procesamiento debe ser corregida.

Habrá, como es normal, reacciones diversas de las personas encargadas del desarrollo de software, así como administradores de centros de cómputo, usuarios y otros expertos del campo en la implementación de estas políticas. En realidad, el problema de fondo radica en que las actitudes frente a bancos de datos manuales son bastante claras: los expedientes suelen ser conservados en un solo lugar y completados con toda la información pertinente. Las personas que tienen acceso a él están predeterminadas y se acostumbra llevar un control de aquellos que son autorizados a tener acceso. Lo mismo se estipula sobre archivos de respaldo. No obstante, no puede esperarse que estos viejos principios del manejo de archivos se mantengan siempre cuando los funcionarios tengan acceso a herramientas de procesamiento de datos, en máquinas individuales a su completa disposición y con acceso a los datos almacenados en sus propios discos duros o en cualquier otro medio de almacenamiento, tanto magnético como óptico. Estos usos, accesos y procesamientos individuales pueden llevar a una situación caótica y sin control, que puede hacer que muchas personas se vean afectadas. Por ello es que las decisiones del legislador deberán estar bien dirigidas, apretando clavijas donde sea necesario, estableciendo una serie de reglas específicas sobre el acceso a la información y al tipo de tratamiento que se le puede dar a un banco de datos por un grupo de personas en un lugar específico de procesamiento, tanto fuera del lugar como dentro de él. Esta propuesta de políticas, más que un principio regulatorio, lo considero un instrumento adicional para garantizar seguridad en el tratamiento de datos personales. Su desarrollo no depende directamente de la normativa, sino de la actitud individual de los lugares de tratamiento, por ello, puede verse como una desiderata conducente a crear mejores condiciones para el procesamiento de estos datos, por lo arriba expresado.

3. LINEAMIENTOS PARA REGULAR LA PARTE RELATIVA AL "HABEAS DATA". En la discusión del problema del procesamiento de datos en América Latina surge casi por asociación inmediata el concepto, derivado en gran medida del concepto de Habeas Corpus, **éste** –Habeas Data- **hace referencia a la posibilidad jurídica de proteger el derecho de los ciudadanos a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales, con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados.** No se trata de un derecho del ciudadano a poseer los datos, ni tampoco de exigirlos, como si se tratara de un ejercicio derivado del derecho a la propiedad. **Se trata de instrumentar una verdadera garantía procedimental para que realice un derecho sustantivo que, a su vez, intenta proteger el derecho del ciudadano a saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales**. Esta articulación suele ser difícil, ya que el Habeas Data no es más que una garantía procedimental, esto es, una garantía para acudir a una determinada vía y ahí solicitar los datos o las informaciones que se entiende son lesivas a los derechos protegidos, y como pretensión solicitar la anulación, borrado, obstrucción o corrección de los datos que afectan a la persona. **Se**

trata de un derecho reactivo y no de uno preventivo. Funciona cuando ya ha sucedido un daño, que puede ser, en algunos casos, de incalculables proporciones, por la afectación que recibiría una persona al producirse interconexiones automáticas de los bancos de datos.[48] Desgraciadamente el Habeas Data latinoamericano se ha concentrado en un derecho reactivo de índole procesal constitucional[49], y decimos desgraciadamente, porque ha hecho que la figura dependa de la amplitud y generosidad de la interpretación de los tribunales constitucionales de los diversos supuestos o constelaciones de casos. Los modelos europeos y norteamericanos se inspiran en diversos puntos de partida. En el caso europeo, como ya hemos visto, se ha puesto el acento en establecer deberes, la mayor parte de ellos preventivos, para salvaguardar a la persona antes de que suceda una posible afectación a su derecho a la autodeterminación informativa. Los Estados Unidos han preferido tutelar acciones individuales bajo el amparo de una ley que defiende específicamente la privacidad de los hogares y de las personas.[50]

El Habeas Data en nuestra concepción, se queda a medio camino, entre la tutela integral de los ámbitos de autodeterminación del ser humano, y la posibilidad de construir una tutela preventiva de las lesiones que, como inmensos riesgos, se ciernen sobre las posiciones jurídicas de los ciudadanos en una sociedad orientada a la información. No debe dejarse de lado que los derechos de la tercera generación,[51] en la clasificación de Pérez Luño, surgen ante el fenómeno inevitable de la "contaminación" provocada por ciertos usos de las nuevas tecnologías.[52] El derecho a la autodeterminación informativa es uno de estos derechos, y exige que la regulación normativa sea coherente con su naturaleza. Es por ello que han de tomarse en cuenta no sólo los derechos de acceso y control, sino también previsiones de carácter técnico que salvaguarden, con efectividad, los derechos involucrados. La inevitable limitación que ofrece una garantía exclusiva en el ámbito procedimental se manifiesta muy especialmente en Brasil, donde la Constitución misma restringe el ejercicio del Habeas Data contra incorrectos datos e informaciones contenidos en bancos de datos públicos, lo que es una decisión incorrecta, si se le evalúa, por ejemplo, desde la perspectiva del cambio de posiciones acaecido en la década de los ochenta y noventa del pasado siglo, cuando los sujetos particulares adquirieron un enorme poder informático y lo utilizaron para vender datos personales y con ello generar un riesgo insospechado para la capacidad de autodeterminación de las personas.

---

[48] En la literatura latinoamericana es recurrente la referencia al Habeas Data como forma de tutela de los ciudadanos frente al tratamiento de sus datos personales. La vinculación del Habeas Data con el Habeas Corpus es mucho más que casual, y puede encontrarse literatura que defiende un concepto de Habeas Data como una acción similar al Habeas Corpus, esto es, que en lugar de "traer el cuerpo", se trata de "traer los datos". Qué se hará con ellos y qué amplitud de tutela se ofrecerá es algo que va a depender, en casi todos los casos, de la regulación normativa específica o de la interpretación que den los tribunales, usualmente constitucionales, a la cuestión. Suele vincularse a su núcleo de tutela los derechos a la honra, a la buena reputación, a la intimidad y al derecho a informarse. Concebir al Habeas Data como un derecho absoluto sobre los datos o un medio procesal para ejercer un poder cuasi patrimonial sobre ellos, sería incorrecto. Tan incorrecto, como concebir a la autodeterminación informativa como otra forma para el derecho a poseer los datos. El derecho a la autodeterminación informativa no le concede al ciudadano un definitivo y absoluto poder sobre sus datos, sino el derecho a estar informado del procesamiento de ellos y de los fines que se pretende alcanzar, junto con los derechos de acceso, corrección o eliminación en caso de que se cause un perjuicio. Aquí se pone el interés, entonces, en la "autodecisión" o en la "autodeterminación" del individuo, lo que se desea es garantizarle su posibilidad de participación como ciudadano frente a un procesamiento de datos personales que lo puede hacer transparente para el control y reducirlo a un mero objeto del ambiente informativo.

[49] Sobre el carácter indudablemente constitucional del hábeas data: **GOZAÍNI, OSVALDO Alfredo.** *El proceso de hábeas data en la nueva ley*, en: http://www.abogarte.com.ar/hábeasdata1.html

[50] Así Gozaíni, Proceso, *opus cita*.

[51] Las leyes de la primera generación serían, según este autor, las leyes que se concentraban en una autorización previa de los bancos de datos, lo que tenía sentido ya que estas leyes surgieron cuando el procesamiento de datos era centralizado, los equipos voluminosos y fácilmente localizables. Luego surgieron las "leyes de la segunda generación", las cuales pusieron el énfasis en los datos sensibles, a fin de evitar daños a la privacidad y ofrecer alguna garantía frente a posibles prácticas discriminatorias que pudieran tener su origen en el uso de esos datos "sensibles". Luego vendrían las leyes de la tercera generación, interesadas en el "uso" y "funcionalidad" de las informaciones. Aquí ubica Pérez Luño, por ejemplo, a la LORTAD española. **Pérez Luño.** *La tutela de la libertad informática,* páginas 97-98.

[52] *Ibidem*, página 97.

El Habeas Data poco va a lograr si conserva esa naturaleza de mera garantía procedimental,[53] ya que obligará a poner todas las cartas en el ejercicio *ex post* de la jurisdicción. Sería mucho más práctico avanzar en dirección del reconocimiento de un derecho del ciudadano a desarrollar un plan de vida, de crear las condiciones de su autorrealización en una sociedad de conocimiento. Si el problema se visualiza desde allí, podrá comprenderse que lo que hay de por medio constituye realmente el viejo problema de otorgar un verdadero y efectivo *status civitatis* a la persona, para que pueda desarrollar su personalidad y definir las condiciones dentro de las cuales interactuará con sus semejantes. Es por ello que consideramos que un ejercicio del Habeas Data sin un correlativo derecho de información sobre las formas en que se realizará el procesamiento, los objetivos y fines del mismo, la extensión, el destino final de los datos personales, le quita transparencia, por un lado, al procesamiento mismo de los datos y, por el otro, hace imposible que el ser humano tome nota de que sus datos serán objeto de manejos más allá de su decisión, con incalculables consecuencias para él, tanto dentro como fuera de las fronteras de su país. Sin embargo, el voto objeto de análisis de no se queda únicamente en las facultades de acceso, actualización y confidencialidad, que pueden ser otorgadas mediante la interposición de un Habeas Data, sino que también puede cubrir a aquellas personas afectadas por datos que han sido desviados del fin original de su recolección, o cuando el tratamiento de este sea prohibido, planteando incluso la opción del derecho al olvido, es decir, los plazos dentro de los cuales un dato pierde interés y hay que borrarlo pues de nada sirve mantenerlo en el banco de datos. Es así como postuló que el derecho a la exclusión tiene las siguientes características:

> **d.) Derecho a la exclusión:** Se refiere a la recolección de la denominada información sensible, de manera que por medio del hábeas data la persona puede solicitar la cancelación de los datos consignados y evitar así los eventuales tratos discriminatorios por parte de las personas que tengan acceso a ella. El sujeto puede solicitar la cancelación del dato registrado cuando su recolección ha sido prohibida, cuando sea impertinente para la finalidad perseguida por la base de datos o en el supuesto de que, por el transcurso del tiempo, no resulte necesario mantener el dato en el registro"[54].

Este voto hace un valioso aporte a la discusión nacional sobre los principios reguladores del tratamiento de datos personales. **Al postular la necesidad de transparencia, está indicando no solo que las condiciones del procesamiento tienen que ser conocidas por las personas afectadas, sino también recibir información sobre las etapas del procesamiento y de las posibilidades de intervención que le competen.** Todo esto con el fin de que el ciudadano pueda ejercer control en cuanto a los datos que ha entregado y sobre el posible destino que estos puedan tener. No se trata únicamente de poder "corregir" o "actualizar" datos e informaciones, como podría esperarse de una simple gestión procesal de Habeas Data. Aún es indispensable que haya condiciones para que el tratamiento de datos pueda cumplir con altas exigencias constitucionales que implican, a su vez, el acatamiento de otras garantías y derechos individuales. La separación de poderes informáticos, por ejemplo, que implica, entre otras cosas, que las diversas secciones o lugares de procesamiento estén separadas, resulta una consecuencia práctica de este aserto, como lo podría ser, también, en caso de que esto llegue a convertirse en una práctica consecuente: en producir una verdadera tutela sistémica.

En cuanto al tema de la información al afectado, mucho se ha discutido si es consecuente proveerle con una gran cantidad de indicaciones técnicas sobre cuál será el destino de sus datos, y las diversas etapas de procesamiento que serán necesarias, así como los detalles de hardware y software implícitos; temas todos que podrían ser incomprendidos por el ciudadano. Más bien, la información que es necesario proveerle, para que el tratamiento de datos sea transparente, es la indispensable para que la persona pueda ejercer ampliamente sus derechos, es decir, conocer quién es el responsable del fichero o del banco de datos, adónde debe acudir en caso de necesitar

---

[53] El artículo 5, inciso LXXII de la Constitución brasileña postula: "...ceceder-se-á hábeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros de bancos de dados de entidades governamentais ou de caráter público; b) para a retificação, quando não se prefira fazê-lo por processo sigiloso judicial ou administrativo".

[54] Principios que han venido siendo reconocidos en normativas internacionales como en la Directiva sobre Protección de Datos de la Unión Europea y, por ejemplo, en la Ley de Protección de Datos de Inglaterra. Dichos principios se orientan a la creación de instancias de control y vigilancia, condiciones dentro de las cuales puede considerarse un tratamiento de datos legal, reglas sobre procesamiento de datos sensitivos sobre la raza, preferencias sexuales, historia clínica, filiación política o religiosa de una persona, provisiones de carácter procedimental para la notificación, registro e información a los afectados, tutela específica a los periodistas y a quienes hagan valer válidamente su derecho a expresarse, así como las regulaciones sobre transferencias allende las fronteras de datos personales. **GUADAMUZ, Andrés.** *Habeas Data: The Latin-America Response to Data Protection*, en: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html

información, así como cuál es el fin al que quedarán sometidos los datos que entrega.

La obligación de confidencialidad de aquellos que laboran en centros de acopio de información también es considerada por este importante fallo, y establece claramente la correlación de este deber con el de prohibir el acceso a los datos a aquellos no autorizados. Por ello, ha de existir un verdadero código de ética interno en el Centro de Tratamiento de Datos, de tal manera que se garantice *"…que los datos que se manejan sean tratados en forma confidencial de manera que se limite el acceso de terceros a la información y la tergiversación de los fines por los que fue creado el registro..."*[55]

1. El principio de calidad instruye que los centros de tratamiento de datos personales deben *"…asegurar la máxima veracidad y precisión de las informaciones contenidas en el banco de datos, manteniéndose completas y actualizadas…"*[56]

2. El derecho a la información del afectado implica, ciertamente, proveerle con detalles *"…sobre la finalidad y uso de los datos así como el derecho de acceso y rectificación de la información que sobre su persona consta en el registro..."*[57]

3. El principio de proporcionalidad, en concordancia con los subprincipios de necesidad, idoneidad y prohibición de exceso en el tratamiento de datos personales, establece una serie de condiciones para el procesamiento de datos, principalmente con la razón de ser de la recolección de datos. Es por ello que, correctamente, se establece en el fallo que los datos deben tener una "justificación social", es decir, *"… los datos deben tener un propósito general y de uso específico socialmente aceptable"*[58].

4. El principio de licitud exige no solo normas claras para regular el procesamiento de datos, sino también respeto al principio de proporcionalidad. Consecuencia de ello, los medios empleados para la recolección deben ser lícitos. El afectado no debe ser engañado. Debe prestar su consentimiento libre e informado para que dicho tratamiento de datos esté acorde con los principios constitucionales. La Sala señala este compromiso de principio de la siguiente forma: *"Principio de limitación de los medios de recolección: los mecanismos de recolección de información deben ser lícitos, es decir con el consentimiento del sujeto o con la autorización de la ley"*[59].

En cuanto a este último aspecto, el del consentimiento, con razón el Tribunal Constitucional de Costa Rica[60] hizo importantes consideraciones, quizá por el tipo de datos que eran objeto de cuestionamiento: los de la historia crediticia. Este tipo de datos, calificados como de interés público por la importancia de la materia en el sector bancario y financiero, son los que más recursos de amparo, en cuanto a Habeas Data, han generado en los últimos años. Los recurrentes suelen ser personas afectadas por datos incorporados en ciertas protectoras de crédito, que luego venden acceso a su banco de datos a empresas bancarias y financieras. Algunas veces este tipo de consultas hacen referencia a información desactualizada o no concordante con la realidad económica del afectado, quien muchas veces debe gestionar directamente ante la protectora de crédito o ante la institución bancaria para demostrar que su historial de crédito está limpio y que es una persona digna de obtener ayuda para sus proyectos económicos.[61] En constelaciones de casos donde esté planteado un problema de principios, habría,

---

[55] *Ibídem*
[56] *Ibídem*
[57] *Ibídem*
[58] *Ibidem*

[59] *Íbidem*
[60] **CHIRINO, Alfredo.** *La tutela de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado*. E*l caso del proyecto de Código Penal de Costa Rica de 1995*, en: Revista Nueva Doctrina Penal, Buenos Aires, Argentina. *Sala Constitucional, V-5736-94, Constitución Política de la República de Costa Rica. Concordada, anotada y con resoluciones de la Sala Constitucional*, San José, Costa Rica, Asamblea Legislativa 1996, p. 101.
[61] Respecto de estas informaciones, considera la Sala que no se puede poner como expreso requisito el consentimiento de una persona que tiene deudas y no las honra para autorizar un procesamiento. Aun cuando esto tiene lógica, debe tenerse en cuenta que no todos los datos de carácter crediticio tienen una relevancia totalmente pública. Las posibilidades reales de dañar a una persona hasta reducirla a una verdadera *capitis diminutio* social son muy grandes cuando los datos de su historial crediticio reciben manejo sin respeto a los principios del tratamiento de datos, esbozados en este fallo. Entre los más importantes podemos citar los principios de sujeción al fin y el principio de calidad, que obligan a las empresas protectoras de crédito a seguir

a pesar de la fuente pública donde se obtuvo la información, exigencia de declarar con lugar el recurso de amparo por la afectación que se ha provocado al derecho a la autodeterminación informativa del afectado.[62] Más recientemente, la sentencia número 00754-02, una de las últimas resoluciones de fondo dictadas en la materia, muestra la evolución de la jurisprudencia constitucional en la delimitación conceptual del derecho a la autodeterminación informativa. **El elenco de principios rectores derivados de dicho fallo puede ser descrito de la siguiente forma:**

> **Cabe el recurso de amparo tanto para la protección de los datos personales contenidos en bases de datos públicas como para los almacenados en archivos privados. Las agencias particulares que almacenan este tipo de datos (empresas protectoras de crédito, por ejemplo) pueden ser accionadas por entenderse que se encuentran, respecto del particular, en una situación fáctica de poder, debido a la enorme cantidad y calidad de datos que pueden almacenar en medios cada vez más eficientes y difíciles de rastrear Los datos pertenecientes al fuero interno de la persona, conocidos generalmente como "datos sensibles", referidos a los aspectos propios de su individualidad (preferencias sexuales, ideología, creencias religiosas, etcétera) no pueden del todo ser recolectados sin el expreso consentimiento del titular, mucho menos almacenados y difundidos.**

Respecto de los otros tipos de datos que aunque referidos a particulares tienen una finalidad pública (informaciones contenidas en los archivos médicos, policiales, judiciales, etcétera), su acceso se encuentra restringido a los órganos de la Administración Pública directamente autorizados, así como a los propios dueños de los datos. Los datos estrictamente públicos contenidos en bases de datos, igualmente públicas, pueden ser accedidos por cualquier persona que así lo solicite, siempre que no se trate de secretos de Estado u otras situaciones calificadas ─descritas en acto motivado─ en que la revelación de los datos podría afectar gravemente el interés general.[63] Informaciones referentes al historial bancario y crediticio de la persona son de acceso restringido. Sin embargo, el incumplimiento de obligaciones reviste interés supraindividual, con la finalidad de mantener el clima de confianza necesario en el mercado financiero, y evitar así el aumento del riesgo y sus efectos en la fijación de las tasas de interés.[64].

---

un estándar mínimo de veracidad de los datos, que garantice a los ciudadanos no ser objeto frecuente de injustas negativas de crédito, solo porque la base de datos no es precisa ni veraz.[61] Referente a la relevancia pública de las informaciones crediticias, ha dicho la Sala que estas informaciones son públicas, en virtud de que han sido recopiladas de registros y fuentes con tal naturaleza, consistiendo el servicio de estas empresas protectoras de crédito en un simple poner a la orden estas informaciones a quien las necesite para decidir sobre el otorgamiento de un crédito. La jurisprudencia de este alto tribunal indica que si las fuentes son públicas, la información obtenida no daña el derecho a la intimidad. Así lo ha reconocido en los fallos 2563-1999 y 4847-1999. Claro está, esta apreciación proviene de la mera consideración de las fuentes de donde se origina la información. Muy distinto sería si lo que hay que valorar es si el tratamiento de datos ha seguido los principios sentados por la misma jurisprudencia constitucional, como el de calidad, el de sujeción al fin o el de proporcionalidad.

[62] Sobre el tema de la exactitud y precisión a la que están obligadas estas protectoras de crédito se refirió el voto 1119─2000.

[63] Tal fue el caso conocido por la Sala al dictar la sentencia 07265-99, rechazando la solicitud de un periodista para que se ordenara al Ministerio de Seguridad Pública publicar el contenido de un informe elaborado por la DEA y que contenía datos relativos a las rutas de entrada y salida de las drogas en el país, que luego serían usadas en el combate contra el narcotráfico.

[64] **CARVAJAL PÉREZ**, **Marvin**. *La protección de los datos personales en Costa Rica.* En Hermenéutica. Número 11, agosto de 2002, p. 12.