LA PROTECCIÓN DE DATOS PERSONALES Y EL HÁBEAS DATA

Elementos para iniciar una discusión en Costa Rica

M.Sc. Jenny Quirós Camacho
Abogada costarricense
Juez de Juicio
San José, Costa Rica

SUMARIO:

INTRODUCCIÓN

La protección de la persona frente a la recolección y tratamiento de información personal es un tema de gran actualidad en Europa, Estados Unidos y América Latina. Es claro que el tema cobra importancia en el supuesto en que reconozcamos el valor de un cierto ámbito personal reservado al individuo. No obstante, las soluciones encontradas en las distintas áreas geográficas distan mucho de ser congruentes entre sí.

Así por ejemplo, la Unión Europea tiene uno de los modelos más elaborados de protección de la privacidad y de datos. El resto de los países europeos y americanos tiende a aprobar leyes de protección de datos personales, no sólo con el objetivo de preservar la privacidad sino también con la finalidad de asegurar que el flujo de datos personales no se detenga, como veremos a lo largo de este trabajo.

Estados Unidos por su parte, que tiende a ser un centro de empresas dedicadas al tratamiento de datos personales con los negocios que ello implica, tiene una visión que ciñe sus alcances al tema de la privacidad. No obstante, empresas norteamericanas radicadas en Europa han tenido que ajustarse a las exigencias de la Directiva Europea, tal es el caso de American Airlines, que fue forzada a detener la transmisión de información que realizaba sobre pasajeros europeos en el sistema mundial de reservas on line Sabre, pues la autoridad sueca la obligó a usar una base de datos separada en Europa, que cumpliera con todos los requisitos exigidos en ese continente.

Latinoamérica se acerca más al modelo europeo de protección de datos que al norteamericano, pero la disparidad de legislaciones en los diversos países del mundo en cuanto a las requisitos de protección, implica que los mismos lineamientos del modelo europeo pueden ser burlados con sólo trasladar la información fuera de Europa para evadir los alcances de la Directiva Europea. Existe un Proyecto de Convención Americana para la Autodeterminación Informativa, y las Agencias Europeas de protección de datos en el seno de la Comisión, celebraron una reunión en una oportunidad con el propósito de difundir las normas europeas en iberoamérica.

Se estima que en el caso de la Argentina, la ley 25.326 y el régimen de privacidad en general cumplen en buena medida con los principios establecidos por la Unión Europea. Otros países latinoamericanos solo tienen el habeas data que permite un control limitado de los datos personales por parte del individuo, como veremos.

De manera que la apariencia de una cierta tendencia hacia la uniformidad, no pasa de ser un largo camino por recorrer, y aspectos de importancia como la aplicación del principio de puerto seguro aún no son de aplicación general.

Costa Rica no cuenta con una ley de protección de datos personales, ni se ha discutido el tema con amplia participación.

Este trabajo pretende ofrecer al lector un panorama amplio de la problemática de la protección de los datos personales. Es nuestro deseo llevar a cabo una descripción sobre la legislación existente, pero no limitarnos a ello. Pretendemos sobre todo aportar elementos para iniciar una discusión en Costa Rica que parta de los vértices de la democracia, del desarrollo y de la protección de la persona humana, pues concebimos la erosión del derecho a la autodeterminación informativa como un problema social que urge soluciones.

SECCIÓN 1: UBICACIÓN DE LA PROBLEMÁTICA PELIGROS DE LA SOCIEDAD DE LA INFORMACIÓN

Se cuenta que hace unos años el gobierno de los Estados Unidos pidió a Rand Corporation que ideara en teoría una forma de mantener bajo vigilancia a ciertos ciudadanos sin que éstos lo sospecharan. El propósito era prevenir que otras personas hicieran lo mismo. Es así como los ejecutivos de Rand Corporation informaron al gobierno que tal sistema ya existía, pues los cajeros automáticos de los bancos registran fielmente los datos de fecha, hora, lugar y transacción financiera que hacen los ciudadanos, lo cual, sumado al rastreo del movimiento del dinero, hace posible conocer mucho sobre los patrones de conducta y la vida de las personas. Además si se relaciona esa información con otra, derivada por ejemplo del uso de las tarjetas de crédito, sería posible obtener un perfil completo de las actividades y gustos de las personas.

El ejemplo ilustra las potencialidades de la tecnología de la información.

Tal y como han dicho varios autores,[1] el conocimiento se ha constituído en la mayor posesión y por tanto es la principal mercancía en

---

(1) Podemos citar a Luis Joyanés, Román Gubern, Alvin Toffler entre otros.

un mundo globalizante que impone desde las metrópolis la vigencia de las leyes del libre mercado hacia fuera.

Es aceptado normalmente bajo el paradigma de la neutralidad científica, tecnológica e informativa que la moderna tecnología de la información contribuye al desarrollo más completo de la persona y a alcanzar algunas metas de la democracia, como la posibilidad de que cada ciudadano se interese por los asuntos públicos y e intervenga directamente en las decisiones que puedan afectar sus derechos. También se ha dicho que la tecnología de la información conlleva graves peligros, pues facilita el manejo de los datos de las personas que pueden ser así utilizados para controlar y dominar, haciendo nugatoria la realización del modelo democrático.

Dicho lo anterior, tenemos lo siguiente: si el sujeto pensante se posiciona concibiendo a la tecnología de la información como un instrumento neutro cuyo uso para bien o para mal depende de las personas, y a esto le suma la concepción general de que las personas no son "malas" y que nos movemos dentro de cierto ámbito de "normalidad", no verá gran peligro. Posiciones como esta llevan a conformarnos con soluciones paliativas al problema del manejo de la información, y a entender las violaciones que se dan por estos medios como problemas individuales, o a los sumo sectoriales que se bastan con mecanismos reactivos e indemnizatorios para el afectado.

Por el contrario, si partimos de que en sí misma la tecnología de la información es peligrosa, que es esencialmente el lado opuesto de la intimidad de la persona, y que por encima de los usos positivos que se le puedan extraer ya representa una amenaza, –al igual que lo entendemos sin dificultad para el caso de las armas de guerra en relación con la vida–, no escatimaríamos en desplegar esfuerzos para proteger a las personas del manejo de sus datos, entenderíamos que no se trata de un problema individual o sectorial, sino social, y que las soluciones deben pasar desde la educación y la prevención hasta el castigo.

Indica el autor Cassese que los países industrializados antes no se interesaban tanto en proteger la intimidad, pero que esto ha ido cambiando. "El debate sobre este tema fue promovido por Francia, en el seno de las Naciones Unidas, durante los años setenta. Para dicho Estado y para otros países occidentales se trataba de estudiar y limitar los desarrollos perniciosos que puede tener la tecnología moderna, hasta poner en peligro la "intimidad" de los individuos, cada vez más sus-

ceptible de verse invadida mediante los modernos instrumentos que utilizan órganos públicos o grupos privados. Pero ese problema no fue en absoluto visto del mismo modo por los países no industrializados, para los cuales el desarrollo de la tecnología es, por el contrario, deseable: lejos de auspiciar una restricción de los posibles usos del ordenador, esos países propugnaban y propugnan la introducción del progreso científico y tecnológico en sus comunidades. Una vez más, se asistió en las Naciones Unidas a un debate entre sordos."(2)

Veremos en este trabajo que luego de las palabras escritas por Cassese, en América Latina se han producido esfuerzos por dar solución al problema del tratamiento de los datos personales que no han culminado en óptimos resultados. El propósito de este estudio es aportar elementos para la discusión nacional sobre el problema del tratamiento de datos en el entendido de que "La ética no adquirirá sus derechos más que en la medida en que se abran espacios de discusión en el seno de los cuales puedan confrontarse las diferentes convicciones sociales y de donde puedan emerger progresivamente un cierto número de principios que aseguren la legitimidad de nuestras acciones en este dominio. Así las cuestiones vitales a plantearse para una ética real de la informática serían relativas a cómo reducirán las prácticas informáticas la vulnerabilidad social y a cómo las personas serán protegidas frente a la globalización económica y tecnológica."(3)

La discusión democrática que proponemos resulta imprescindible si tomamos en cuenta lo afirmado para el fenómeno de desarrollo tecno científico en general: "...los peligros, la evaluación de los riesgos en el mejor de los casos, pueden ser competencia de los expertos, pero, de hecho, las catástrofes las podemos sufrir todos. Esta asimetría hace más que razonable mantener que, aunque los cálculos de riesgo pueden y deben hacerlos los científicos, las decisiones sobre el control y los límites de las intervenciones tecnocientíficas nos competen a todos. El problema de nuestras sociedades del riesgo es que en ellas se defiende, el más puro estilo positivista, la unión del poder espiritual y político; es decir, los productores de conocimiento, los que deciden y quienes evalúan los posibles impactos de esas decisiones son los mismos; los expertos."(4)

---

(2) CASSESE, Antonio. *Los Derechos Humanos en el mundo contemporáneo.* Ariel, Barcelona, España, 1991, p. 74.

(3) JOYANES AGUILAR, Luis. *Cibersociedad. Los retos sociales ante un nuevo mundo digital*. Mcgraw-Hill, España, 1997, p.282.

(4) MOYA, Eugenio. *Crítica de la razón tecnocientífica.* Biblioteca Nueva, S,L, Madrid, 1998, p. 257.

El manejo de la información luego del 11 de setiembre de 2001

Si decimos que en la sociedad actual el conocimiento es la posesión más estimada y por tanto es la principal mercancía en un mundo globalizante que impone desde las metrópolis la vigencia de las leyes del libre mercado hacia fuera, conviene preguntarnos qué ocurre con el conocimiento y el manejo de la información después de los actos terroristas de setiembre del año antepasado.

Es claro que aún y cuando materialmente los atentados ocurrieron en los Estados Unidos, sus efectos políticos, económicos y sociales se esparcen por el mundo, pues como indica Ulrich Beck, en el modelo cosmopolita los Estados nacionales ceden parte de su poder, de modo que "se socava la soberanía del Estado en materia de información y fiscalidad –y por ende, su autoridad propiamente dicha".(5)

Para el profesor Saxe después de setiembre de 2001 el control del conocimiento se fundamenta en mantenerlo alejado de competidores, subordinados, amigos y enemigos",(6) y citando a Fareed Zikaria, editor internacional y columnista, escribe: "El nuevo paradigma modelo de globalización perdurará. Pero para prosperar debe adquirir una nueva dimensión: un acuerdo mundial para instalar controles, limitaciones e inspecciones, mientras que a la vez permita el libre flujo del comercio". Nada ha cambiado en el objetivo fundamental del capitalismo neoliberal, "el libre flujo comercial", las cosas convertidas en sujetos históricos. Mas algo sí ha cambiado en el orden institucional que sustentará ahora esa universal alienación. Hace falta instalar "controles, limitaciones e inspecciones", no solamente para las mercancías sino sobre todo sobre el libre flujo de las personas y sobre el pensamiento y las comunicaciones…"(7)

Si ello es así, puede afirmarse que después de setiembre de 2001 el contexto se vuelve aún más adverso a la protección del individuo frente al tratamiento de los datos personales, porque el interés por el

---

(5) BECK, Ulrich. *¿Qué es la globalización? Falacias del globalismo, respuestas a la globalización.* Piados, Barcelona, 1998, p. 81

(6) SAXE FERNÁNDEZ, Eduardo. *Militarización de la crisis mundial: costos de la hegemonía, colapsos mundiales y pensamiento oficial,* en Documentos de estudio, número 15, ERI, UNA, Nueva Época, 2002, p. 29.

(7) SAXE FERNÁNDEZ, *op cit*., p. 46.

control y la seguridad ha desbordado los límites anteriores. En un régimen de seguridad nacional como el que se impone en los Estados Unidos y vierte sus efectos a nivel general después de setiembre de 2001, ciertamente el control de la información resulta históricamente central.

"…la extensión de la filosofía de la guerra total y permanente presupone la realización hasta sus últimas consecuencias de una cultura mediática de video vigilancia global, en la que la seguridad es consagrada como principio rector de la vida pública, en nueva disciplina de regulación y acomodamiento social de la conciencia cívica a las necesidades de orden y control político militar por razones preventivas. La pedagogía militar de la guerra de la información consiste precisamente en la calculada y ambigua extensión de la lógica bélica a la vida civil y política."(8)

Tenemos entonces tres condiciones históricas muy claras que hacen necesario el esfuerzo por proteger a las personas frente al tratamiento de los datos personales. Estas condiciones son: el vertiginoso desarrollo de tecnologías de la información, los grandes intereses comerciales de las empresas dedicadas o favorecidas con el tratamiento de la información, a los que se sumó, después del 11 de setiembre antepasado, el control reforzado impuesto y cubierto con el discurso nacionalista y de seguridad de las metrópolis.

Democracia, desarrollo y protección de datos

Si partimos –como lo hemos hecho– de que el manejo de datos personales conlleva un peligro para esa esfera del ser humano que debería ser regida por su voluntad sin intromisión externa, y si tenemos ejemplos de la potencialidad de la tecnología de la información para el control individual y social, será fácil concluir que sin una correcta protección del manejo de datos personales muchos derechos individuales podrían quedar en la letra de la ley.

Así, por ejemplo, la libertad de pensamiento y de culto, la libertad sexual, la libertad de expresión, la libertad de sindicalización, la libertad de afiliación política, el secreto de las comunicaciones, el ámbito de intimidad y de privacidad, corren el riesgo de ser anulados. El jurista

(8) F. SIERRA, citado por Saxe, *op. cit*., pp. 48 y 49.

nacional Rubén Hernández ha indicado "...la violación de este derecho puede afectar los derechos de la personalidad (intimidad, imagen, honor, etc.), así como también la libertad informática, derecho que proviene directamente de la libertad personal la cual garantiza un trato no discriminatorio tanto en la esfera comercial como en el ámbito laboral."(9)

Pensemos por ejemplo en el temor que tendrían los ciudadanos de ejercer tales derechos a sabiendas de la posibilidad de ser estigmatizados y controlados. Ello redundaría sin duda en la disminución de la capacidad de autodeterminación y en la negación de la posibilidad de realización de cada proyecto de vida.

Lo que exponemos no es ficción, y ni siquiera una previsión a largo plazo. Es una realidad actual puesto que los avances en la tecnología de la información permiten la construcción de perfiles de personalidad, preferencias, tendencias. Para esta construcción de perfiles y tendencias los datos no tiene que revestir un especial carácter en contra de la privacidad entendida en el sentido tradicional. Datos que podemos considerar irrelevantes o insignificantes desde ese punto de vista, tienen la capacidad de coadyuvar en la realización de estos medios de control social mediante la comparación, reunificación y redefinición de los mismos.

Si el modelo democrático parte de que cada ser humano es un fin en si mismo y que los medios de control sólo han de justificarse en la medida en que coadyuven a evitar el desbordamiento en el ejercicio de un derecho en perjuicio de otro y en la medida en que eviten las lesiones al derecho de cada persona, comprenderemos que la relación entre la democracia y la protección de datos personales es muy estrecha: Afirmamos que existe una relación de proporcionalidad directa entre la vigencia del modelo democrático y la tutela a la autodeterminación del ser humano mediante la protección de sus datos personales. Cuanta mayor tutela de la persona frente al tratamiento de sus datos, mayor vigencia del modelo democrático en una sociedad determinada.

Esta visión que proponemos no riñe con la visión de democracia expuesta por organismos oficiales como la Organización de Naciones Unidas a través de sus publicaciones del PNUD. Así por ejemplo, al partir del paradigma democrático para la evaluación del desarrollo de las

---

(9) HERNÁNDEZ VALLE, Rubén. *El Régimen Jurídico de los Derechos Fundamentales en Costa Rica.* Editorial Juricentro, 2001, San José, Costa Rica.

naciones, el informe del PNUD de 2002 hace alusión a las posibilidades de participación democrática, y a la calidad de vida.

"Irónicamente, el enfoque de desarrollo humano del desarrollo ha sido víctima del éxito de su índice de desarrollo humano (IDH). El IDH ha reforzado la interpretación restringida y demasiado simplificada del concepto de desarrollo humano, como si se tratara únicamente de mejorar la educación, la salud y los niveles aceptables de vida. Ello ha oscurecido el concepto más amplio y complejo de desarrollo humano como expansión de capacidades que amplía las posibilidades de la gente de vivir la vida que deseen y valoran. A pesar de cuidadosos esfuerzos por explicar que el concepto es más amplio que su instrumento de medición, el desarrollo humano continúa siendo identificado con el IDH mientras se ignoran a menudo las libertades políticas, la participación en la vida comunitaria y la seguridad física. Sin embargo, esas condiciones son tan universales y fundamentales como poder leer o disfrutar de buena salud. Todos las valoran –y sin ellas se cierran muchas otras opciones. No se incluyen en el IDH porque son muy difíciles de medir de manera adecuada, no porque sean menos importantes para el desarrollo humano."(10)

Esta visión del desarrollo en democracia nos lleva entonces a sostener tres afirmaciones, siguiendo la lógica del texto: La primera es que el concepto de desarrollo humano es más grande que el índice.(11) La segunda es que para determinar el desarrollo, es posible (y decimos que necesario) incluir categorías distintas de las que se han utilizado hasta el momento siempre que no ofrezcan dificultades de medición. Y la tercera es que la protección de la persona frente al tratamiento de sus datos personales puede (y debe) constituirse en una categoría de la medición del desarrollo en democracia, puesto que, como vimos, de ello depende en gran medida la vigencia del modelo democrático.

Derecho a la información versus protección de datos personales

Desde el punto de vista jurídico debemos comprender la necesaria armonización del derecho a la autodeterminación informativa y la

---

(10) Informe de PNUD 2002. *Profundizar la democracia en un mundo fragmentado*, p. 53.

(11) En este mismo sentido ver Informe de PNUD 2002, recuadro 22.

protección de datos personales, con el derecho a la información contemplado en el numeral 19 de la Declaración Universal de Derechos Humanos de las Naciones Unidas de 1948 que establece: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

Desde meses antes de la aprobación de la Declaración Universal de Derechos del Hombre, -del 23 de marzo al 21 de abril de 1948- se había celebrado la Conferencia de la ONU sobre la libertad de información. Es decir, la existencia de éste derecho tiene bases históricas muy fuertes pues políticamente se ha concebido como una extensión de la libertad de pensamiento, que es una base esencial del modelo democrático.

En Costa Rica, por ejemplo, el numeral 28 Constitucional reza: "Nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que infrinja la ley. Las acciones privadas que no dañen la moral o el orden público o que no perjudiquen a tercero, están fuera de la acción de la ley." El artículo 29 expresa "Todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura; pero serán responsables de los abusos que cometan en el ejercicio de este derecho, en los casos y del modo que la ley establezca. Y el 30 indica: "Se garantiza el libre acceso a los departamentos administrativos con propósito de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado."

Lo que afirmamos es que es necesario, como lo es para el resto de derechos, hacer un balance entre el derecho a la información y otros derechos, puesto que ningún derecho reconocido constitucionalmente es absoluto, y el numeral 1 Constitucional ya impone el deber de interpretación democrática del texto.

En efecto, "frente al derecho a la información genéricamente reconocido a los ciudadanos usualmente invocado como fundamento de la libertad de prensa, se alza un derecho sobre la información, que compete a cada cual respecto de ciertos datos que se le reconocen como privados y que lo autoriza a restringir su conocimiento o su uso por terceros. La evolución de este derecho se ha visto bruscamente conmovida por la aparición de las computadoras. Ellas se utilizan en la preparación de las nóminas para el pago de sueldos y jornales, en las

reservas de pasajes de tren o de avión, en el control bancario del estado de nuestras cuentas, en la vigilancia de los datos de interés fiscal, en el campo de la medicina y en muchas otras actividades, sin olvidar una de las más recientes, que es precisamente la jurídica."(12)

Entonces, si el derecho a la información no es absoluto, como no lo es ningún derecho humano, una de sus limitaciones consiste precisamente en el derecho a la protección de datos personales y la autodeterminación informativa.

En igual sentido se pronuncia la autora María Cruz Llamazares Calzadilla al comentar el conflicto que existe entre las libertades de expresión e información y otros derechos. Según esta autora "...un derecho al honor entendido como un derecho absoluto e intocable implicaría una libertad de información y, sobre todo, de expresión, vaciada de parte de su contenido. Y unas libertades de información y de expresión ejercidas de forma abusiva sin ninguna limitación, impedirían la existencia efectiva de un derecho al honor, a la intimidad o a la propia imagen. Es lógico que los derechos de uno y otro grupo colisionen constantemente, puesto que en el ejercicio, no siempre legítimo, de las libertades de expresión y de información frecuentemente se hacen incursiones en el ámbito propio del honor, de la intimidad y de la propia imagen."(13)

¿Por qué optamos por hablar de protección de datos personales y de autodeterminación informativa más que de habeas data?

Cuando se habla de habeas corpus, en un sentido literal, se trata de "traer el cuerpo" de la persona afectada por una detención ilegítima, de modo que para la materia en estudio se adoptó el paralelo de hábeas data como "traer los datos".(14)

---

(12) GUIBOURG, Ricardo A. y otros. *Manual de informática jurídica*. Astrea, Buenos Aires, 1996, p. 263.

(13) LLAMAZARES CALZADILLA, María Cruz. *Las libertades de expresión e información como garantía del pluralismo democrático*. Departamento de Derecho Público y Filosofía del Derecho. Universidad Carlos III De Madrid, Civitas, Madrid, España, 1999.

(14) CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación informativa y Estado de Derecho en la Sociedad Tecnológica*. CONAMAJ, San José, Costa Rica, 1997, p. 20.

Así ampliamente entendido, el hábeas data podría referirse a una construcción conceptual para englobar todos aquellos elementos sustantivos y procedimentales creados para la protección de la persona frente al tratamiento de sus datos personales. Por ejemplo, el hábeas data podría comprender toda una tesis sobre la problemática de la invasión en la personalidad a través del tratamiento de datos, pasar por la creación de un nuevo bien jurídico a tutelar y finalmente idear los institutos procesales para su protección. No obstante, en el derecho latinoamericano, el "habeas data" se ha convertido en una mera garantía procedimental para proteger al derecho que tiene la persona al acceso y conocimiento de sus datos personales en registros públicos y privados.

Es lo cierto que el esfuerzo latinoamericano por otorgar al ciudadano un medio de tutela implica ya una conciencia de la importancia del tema de la protección de os datos personales. La falencia radica en que así concebido, el habeas data tiende a funcionar después de realizada la transmisión de los datos, dejando por fuera la prevención y el control anterior a la realización del riesgo. Por ejemplo, la acción puede ser interpuesta por el particular cuando se traten datos de los llamados sensibles, que incluyen las preferencias religiosas, políticas sexuales, las características genéticas y de salud. Pero se deja por fuera la posibilidad de obtener información sobre el procesamiento de los datos y el derecho del ciudadano de otorgar el consentimiento para el tratamiento electrónico de sus datos.

No debemos olvidar que en "...la industria de las bases de datos intervienen diferentes personas. El creador de la base que, partiendo de un fondo documental adecuado genera la propia base; el distribuidor de la base que, disponiendo de un soporte técnico y comercial, crea y proporciona el servicio y, por último, el usuario de la base. Si la base de datos es consultada por el sistema denominado "on line", a distancia, interviene también el operador de comunicaciones."(15)

Las diferencias apuntadas entre el amplio espectro de la protección de datos y el hábeas data entendido como garantía procesal, ha llevado a algunos a establecer entre ambos una relación de género a especie: "Existe una relación de género y especie entre el hábeas data y el derecho de acceso a la información, como derechos humanos

---

(15) DAVARA RODRÍGUEZ, Miguel Angel. *Manual de Derecho Informático*. Aranzadi. Madrid, l997, p. 30.

referidos a la accesibilidad de datos. El derecho de acceso a la información interpreta una necesidad general, mientras que el habeas data se vincula a una necesidad especial y personal, siendo ambos incuestionables, pero dedicados a espectros y casos diferentes."(16)

Lo importante en nuestro criterio es que junto a la garantía procesal se prevea para la verdadera protección del ciudadano, el derecho a la información sobre las formas en que se realizaría el tratamiento de los datos, los objetivos del mismo y su destino final, a efecto de que la persona esté o pueda estar en condiciones de conocer que sus datos serán objeto de manejos más allá de su voluntad, y poder evitarlo. Es por ello que acogemos la afirmación de que hablar de hábeas data no es suficiente, y que es preferible referirse a la necesidad humana de protección de los datos personales, misma que tiene como correlativo bien jurídico la autodeterminación informativa.

¿Por qué la autodeterminación informativa es un bien jurídico?

Los problemas derivados de los bancos de datos tradicionalmente se han situado como un ataque al derecho a la intimidad.(17)

Consideramos importante no perder de vista lo apuntado por el presidente del Tribunal Europeo de Derechos Humanos en el discurso de apertura de la XIII Conferencia de Comisarios de Protección de Datos: "aunque hablamos de protección de datos, de legislación de protección de datos y de Autoridades de protección de datos, no deben existir dudas respecto a la verdadera naturaleza del objetivo que motiva la creación de las normas de protección de datos o de las instituciones que garantizan el cumplimiento de las mismas. Su finalidad real no es tanto la protección de datos sino la protección de las personas: más precisamente aún, es la protección de la vida privada de las personas en una nueva era que impone la recogida y almacenamiento de más y más datos sobre sus

---

(16) PIERINI, Alicia y LORENCES, Valentín. *Derecho de acceso a la información. Por una democracia con efectivo control ciudadano, Acción de Amparo.* Editorial Universidad, Buenos Aires, 1999, p. 38.

(17) FERREIRA RUBIO, Delia Matilde. *El derecho a la intimidad.* Editorial Universidad, Buenos Aires, 1982, pp. 61 y 62.

vidas privadas y hace aumentar las posibilidades de manipulación y mal uso de tales datos."[18]

De manera que, en apego a la tesis que propone que los bienes jurídicos obedecen su existencia a la valoración de necesidades humanas, y que siempre el titular último de los bienes jurídicos ha de ser el ser humano,[19] afirmamos que si la persona humana se desenvuelve en una sociedad que evoluciona, la existencia de bienes jurídicos necesariamente irá aparejada a los cambios sociales que afecten el núcleo de derechos principales de la persona. Si ello es así, los vertiginosos cambios ocurridos por el avance en el manejo de la información, imponen la necesidad de proteger al ser humano de ese manejo, no con una simple indemnización o reparo, sino fundamentalmente impidiendo que trasciendan datos y uso de los mismos contra su voluntad. Pero he aquí un problema de gran importancia: Aquellos datos a proteger no son solamente los que atañen a la vida "privada o íntima" del individuo en el sentido tradicional. La sociedad actual impone ser muy amplios en cuanto a los datos que se protegen, porque un dato por nimio que parezca cobra importancia ante las posibilidades técnicas, comerciales y psicológicas publicitarias de crear perfiles, prever conductas y anticipar comportamientos. Es por ello que el bien jurídico que nace en estas sociedades de la información, rebasa el bien jurídico de la intimidad y de la privacidad entendidos de manera clásica.

Ahora bien, el tema no es pacífico en doctrina, y la discusión que proponemos a lo interno de nuestro país deberá pasar por este tema. Así por ejemplo, se ha dicho que "No es pues la autodeterminación una noción distinta de, aunque relacionada con, el derecho a la intimidad, sino un elemento definidor de éste. Todo intento de escindir el ámbito del derecho a la autodeterminación informativa del ámbito del derecho a la intimidad, como los que a veces ha llevado a cabo nuestra doctrina., carece de base conceptual alguna, a menos, claro está, que se quiera desvincular la intimidad de toda idea de control. Pero en ese caso su

---

(18) RYSDALL, R. Protección de datos y el Convenio Europeo de los Derechos Humanos. Discurso de apertura dela XIII Conferencia de Comisarios de Protección de Datos, Novática, marzo de 1992, citado por Campuzano Tomé, Herminia, *Vida Privada y Datos Personales, su protección frente a la sociedad de la infomación*, Tecnos, Madrid, España, 2000. p. 56.

(19) Así, FERRAJOLI, Luigi. *Derecho y razón. Teoría del garantismo penal.* Editorial Trotta, Madrid, 1995.

objeto no iría más allá de situaciones del tipo de la de una persona aislada en una isla desierta. Ni tampoco es la autodeterminación una noción nueva en la definición del derecho a la intimidad, sino una idea que lo ha informado desde siempre, ya antes incluso de que hiciera aparición como derecho específico."[20]

Proponemos que en última instancia lo trascendente no es la forma en que se denomine el bien jurídico, sino la amplitud de contenido que se le de al concepto, lo cual resulta, como queda expuesto, irrenunciable.

SECCIÓN 2. SITUACIÓN NORMATIVA GENERAL

No es el propósito de esta sección detenernos en la evolución de la protección de la persona frente al tratamiento automatizado de la información que le afecta. Nos limitaremos a exponer la situación actual en líneas muy generales.[21] Sin embargo, consideramos de primer orden ubicar al lector en cuanto a que en este tema no se trata –como en otros temas legales y normativos– de comparar legislaciones a efecto de que un país opte por la normativa más completa o por la combinación de varias. En este tema resulta imprescindible conocer la legislación existente en el mundo bajo la siguiente perspectiva: Las legislaciones regionales o nacionales ya de por sí tienen la debilidad de que al establecerse limitaciones en un ámbito territorial, es posible burlar la protección saliendo virtualmente de las fronteras. Internet se constituye en la herramienta adecuada para ello: "El código fuente de la página visitada puede contener un sencillo Javascript que ordena el envío voluntario de un mensaje de correo electrónico a una dirección determinada. De esta manera, sin que el usuario lo haya autorizado, ha

---

(20) RODRÍGUEZ RUIZ, Blanca. *El secreto de las comunicaciones, tecnología e intimidad*. McGraw Hill, Madrid, 1997, p. 16.

(21) Sobre la evolución de la protección de la persona frente al tratamiento de la información ver GARRIDA DOMÍNGUEZ, Ana, *La protección de los datos personales en el Derecho Español*. Universidad Carlos III de Madrid, Dykinson, Madrid, 1999, pp. 45 a 115. Esta obra contiene una descripción cronológica de las principales normas relativas a la protección de los datos personales en el mundo. Ver además, Campuzano Tomé, Herminia, *Vida Privada y Datos Personales, su protección frente a la sociedad de la infomación*, Tecnos, Madrid, España, 2000, p. 56.

facilitado su dirección de correo electrónico al solicitante. Ello va a permitir a la empresa receptora de dicha dirección crear una base de datos de visitantes que han demostrado su interés por un tema específico y que, por lo tanto, pueden ser segmentados en función de sus preferencias, con el fin de efectuar posteriormente envíos de publicidad por correo electrónico."(22)

Protección de datos en Europa

En la década de los años setenta los países de Europa aprobaron leyes sobre protección de datos, debido a los desarrollos tecnológicos que se daban. En la década de los años ochenta fueron aprobados algunos acuerdos internacionales, especialmente directrices de la Organización para la Cooperación y el Desarrollo Económicos y el Convenio del Consejo de Europa, que es el Convenio para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal, abierto a la firma en Estrasburgo el 28 de enero de 1981.

En la década de los noventa la Unión Europea (UE) dictó una Directiva cuyo propósito general era armonizar las legislaciones de los países de la Unión. Fue así como se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, publicada en el Diario oficial No. L, 281, del 23 de noviembre de 1995. La Directiva obliga a los Estados miembros a adaptar a ella sus leyes de privacidad y protección de datos personales y parte de la visión de que la privacidad es un derecho humano.

El considerado 10 de la directiva indica: "Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respecto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, así como los principios generales del derecho comunitario; que, por tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la comunidad".

---

(22) Rivas Alejandro, Javier. Riesgos legales en Internet. Especial referencia a la protección de datos personales, *en Derecho de Internet. Contratación electrónica y firma digital*, Aranzadi, España, 2000, p. 154.

Ya el numeral primero de la Convención Europea de Derechos Humanos partía de esta concepción, y aunque esa convención no ha sido incorporada oficialmente a la Unión Europea, la Corte de Justicia Europea la ha aplicado para reconocer distintas facetas del derecho a la vida privada.

El artículo 8 del Convenio para la Protección de los Derechos del Hombre y las Libertades Fundamentales, firmado en Roma en 1950, establece que toda persona tiene derecho al respecto de su vida privada y familiar, de su domicilio y de su correspondencia, y no puede haber injerencia de la autonomía pública en el ejercicio de este derecho, excepto cuando esté prevista por la ley y constituya una medida necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral o la protección de los derechos y las libertades de los demás, en una sociedad democrática. Tales limitaciones al derecho de la privacidad también ha sido reconocidas por la Corte Europea de Justicia y están presentes en la Directiva.

Según la Directiva, los Estados miembros dispondrán que el tratamiento de los datos personales sólo puede efectuase si el interesado ha dado sus datos de forma inequívoca, o cuando es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o cuando es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o cuando es necesario para proteger el interés vital del interesado, o cuando resulte necesario por un interés público o para la satisfacción de un interés legítimo del responsable del tratamiento o de terceros a los que se comunique los datos cuando no se perjudique los derechos fundamentales del interesado. Es decir, la licitud para el tratamiento de datos personales sólo es posible si el interesado ha dado su consentimiento o si nos encontramos frente a las excepciones previstas en las misma norma. (artículo 7 de la Directiva)

Por otra parte, hay que destacar que el numeral 10 establece obligaciones para el responsable del tratamiento o su representante cuando se obtenga datos, en cuyo caso los Estados miembros deben disponer que el responsable del tratamiento o su representante deben comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información siguiente: la identidad del responsable del tratamiento y, en su caso, de su representante; los fines del tratamiento

de que van a ser objeto los datos; cualquier otra información, tal como: i) los destinatarios o las categorías de destinatarios de los datos; ii) el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa al responder; iii) la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado

Distinto es el caso en que los datos no hayan sido recabados del propio interesado, pues aunque la Directiva enuncia los mismos requisitos expuestos, las obligaciones rigen desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de estos datos.

La Directiva también garantiza el derecho de acceso. Los Estados miembros deben garantizar a todos los interesados el derecho de obtener del responsable del tratamiento, libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: i) la confirmación de la existencia o la inexistencia del tratamiento de los datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de los datos a que se refieran y los destinatarios a quienes se comuniquen dichos datos; ii) la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; iii) el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en el caso de las decisiones automatizadas al que se refiere el apartado 1 del artículo 15 de la Directiva. También el interesado podrá obtener la rectificación, la supresión, o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto de los datos y la notificación de los terceros a quienes se hayan comunicado los datos de toda rectificación o bloque efectuado de conformidad con lo dispuesto en el párrafo anterior, si no resulta imposible o supone un esfuerzo desproporcionado.

Ahora bien, tales derechos y obligaciones no son absolutos. El artículo 13 prevé la posibilidad de que los Estados miembros adopten medidas legales para limitarlos y para limitar todos los derechos contemplados en los numerales 6 apartado 1, 10 y 11, 12 y 21, referentes a los principios generales, a la información en caso de obtención de datos

recabados del propio interesado, al derecho de acceso y a la publicidad de los tratamientos. De acuerdo con el numeral 13, las limitaciones pueden ser establecidas cuando sea necesario para garantizar la seguridad de Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas, un interés económico y financiero importante de un Estado miembro o de la UE, incluidos los asuntos monetarios, presupuestarios y fiscales, una función de control, de inspección o reglamentaria relacionada con el ejercicio de la autoridad pública en los casos de seguridad pública, prevención, investigación, detección y represión penal y profesional, y en el caso de los intereses económicos y financieros ya aludidos, la protección del interesado o de los derechos y libertades de otras personas. También los Estados pueden limitar el derecho de acceso por medio de ley, cuando se trata de fines de investigación científica durante un periodo que no supere el tiempo necesario para la elaboración de estadísticas.

Por otra parte, la Unión Europea aprobó una directiva relativa a la protección de datos en el sector de las telecomunicaciones.

El Parlamento Europeo elaboró la Carta Europea de Derechos Humanos que incluye un nuevo artículo relativo a la protección de datos, confirmando que este es un derecho humano. También en diciembre del 2000 fue aprobado en Niza por todos los miembros de la UE el rango de derecho humano de la protección de datos, por destacar algunos de los principales pronunciamientos.

Consideramos importante la descripción del modelo europeo por cuanto su efecto fue expandir este esquema de legislaciones de protección de datos fuera de Europa, aún y cuando no fue su propósito inicial. En países como Argentina, Paraguay, Nueva Zelanda, Hong Kong y Taiwán, Chile, Canadá y la provincia de Québec han seguido en sus legislaciones los estándares europeos en materia de protección de datos, en tanto otros países como Venezuela, Perú, Brasil y la India, han llevado a cabo esfuerzos para hacer lo mismo. En la misma Europa, los países como Polonia y Hungría que han solicitado su ingreso están en un proceso de adecuación de su legislación interna a la Directiva y en general a la legislación comunitaria. La caída del régimen comunista también influyó para que países del Centro y del Este de Europa incluyeran en sus constituciones y en sus leyes a la protección de datos como derecho humano.

Protección de datos en Estados Unidos

Al igual que en Europa, en los años setenta se inició una preocupación por el tema de la protección de los datos personales. En 1993 el gobierno llevó a cabo un estudio en el que finalmente recomendó la aprobación de principios para el tratamiento de datos personales. Si bien tales principios no fueron aprobados por el Congreso como una ley, sí existían dos leyes. La primera es la Privacy Act aprobada en 1994 y la segunda la Fair Credit Reporting Act aprobada en 1970. Estas regulaban lo relativo a los datos almacenados por el gobierno y a los registros de informes crediticios. Posterior a ello, Estados Unidos ha dado un tratamiento casuístico al problema, sin legislar mediante una ley general de privacidad. Los sectores en que se ha legislado son los registros estatales, los informes crediticios, los registros de conducir, los registros sobre alquileres de video, las comunicaciones electrónicas, la información sobre suscriptores de televisión por cable, la recolección de datos por parte de menores en línea y la privacidad financiera.

En cuanto a la cláusula de puerto seguro, la Comisión Europea había iniciado hace más de dos años las negociaciones destinadas a abordar el problema de la falta de protección de la privacidad en Estados Unidos. En junio del 2000 la Comisión emitió un Acuerdo de Puerto Seguro que pretende garantizar que la transferencia a un tercer país de datos personales únicamente puede efectuarse cuando el tercer país garantice un nivel de protección adecuado y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados Miembros.

Protección de datos en América Latina

En América Latina algunos países no cuentan con una ley de protección de datos, pero varios han incluido en sus constituciones normas sobre la privacidad o habeas data y han aprobado leyes de privacidad, además de que a nivel interamericano se esta negociando una convención basada en el Convenio del Consejo de Europa.

Este fenómeno ocurre en parte porque, como vimos, el artículo 25 de la Directiva europea establece que la transferencia de datos sólo puede tener lugar si el país destinatario cuenta con una legislación "adecuada".

En 1997 se celebró en Madrid la Conferencia Euroiberoamericana sobre Protección de Datos Personales a la que asistieron autoridades de protección de datos europeas y representantes de países iberoamericanos. En ella se demostró la falta de una legislación relativa a la protección de los datos personales por lo que se acordó impulsar ante los gobiernos de los respectivos países el desarrollo de medidas en materia de protección de personas físicas en lo que respecta al tratamiento de datos personales, entre otros acuerdos para impulsar la creación de esa legislación.

Desde la década de los ochenta la OEA ha investigado el problema de la protección de los datos personales pero principalmente desde 1997. También el Comité Jurídico Interamericano realizó estudios sobre el derecho a la información y la libertad de expresión. El Comité Jurídico Interamericano propuso en 1997 elaborar una convención americana de protección de datos basándose en el modelo del Convenio para la Protección de las Personas del Consejo de Europa y en la ley española de 1992. Fue elaborado un borrador de la Convención Americana sobre Autodeterminación Informativa. En su preámbulo se recuerda la importancia de la protección de la vida privada establecida en la Declaración Americana de los Derechos y Deberes del Hombre, de 1948 y en la Convención Americana sobre Derechos Humanos de 1969. Estas establecen que toda persona tiene derecho al respecto de su honra y al reconocimiento de su dignidad; que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio, o en su correspondencia ni de ataques ilegales en contra de su honra o reputación; y que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

También se expresa que “el peligro en contra de la vida privada y el pleno ejercicio de otros derechos se ha acrecentado por el aparecimiento de nuevos medios técnicos de injerencia y control sobre los derechos y libertades, particularmente por el tratamiento automatizado de datos de carácter personal, que permiten el conocimiento general de la historia de cada ser humano, creándose la posibilidad de que por medio de los ficheros, registros o de bancos de datos no sólo se conozca lo más privado de las personas y se les controle y dirija atentándose así contra su dignidad , libertad e igualdad y contra la estructura misma del sistema democrático, situación que vuelve necesario dar a las personas una ulterior protección a la ya prevista en el derecho interno, en las declaraciones y convenciones internacionales citadas”.

Se indica que la normativa debe tender a "lograr un justo equilibrio y armonía entre la protección a los derechos, y libertades de las personas, con los derechos que emanan del poder informativo especialmente, con la libre circulación de la información entre los pueblos y la necesidad del progreso y desarrollo nacional en una economía posindustrial globalizada e informatizada".

El fin de la Convención es garantizar, en el territorio de cada Estado parte, a cualquier persona física o jurídica sean cuales fueren su nacionalidad o residencia, el respeto de sus derechos fundamentales, su derecho a la autodeterminación informativa. Sin embargo, a diferencia del modelo europeo se pretende que la Convención sea de aplicación también a los datos de las personas naturales o jurídicas o a sus bienes que figuren en registros, ficheros o bancos de datos de los sectores público y privado, sean estos automatizados o manuales. Por otra parte, establece varios principios en líneas generales congruentes con los señalados por la Directiva Europea.

Ahora bien, la normativa interna de los países latinoamericanos se comenzó a desarrollar en 1988 cuando se incluyó en los textos constitucionales de Latinoamérica la garantía de habeas data, con el propósito de otorgar o los individuos un derecho de acceso a la información personal que fuera recogida y tratada en bancos de datos personales. En algunos casos esta acción permitía corregir o actualizar la información y suprimir cierta clase de datos. La limitación principal que presentan estas normas es que, si bien se reconoce un derecho de acceso a los datos personales, y en caso de falsedad, inexactitud u otros motivos, autoriza a reclamar la corrección de la información, es lo cieto que no cubre el resto de los principios acordados por la Directiva Europea.

Desde 1994 se desarrolló un movimiento para aprobar leyes de protección de datos personales en Latinoamérica. En Colombia, por ejemplo fue aprobada una ley que fue declarada nula por la Corte Constitucional. En Argentina fueron presentados varios proyectos a raíz de la inclusión del Habeas data en su Constitución. En Chile se comenzó a discutir una ley de protección a la vida privada. Uruguay, Colombia y Perú también tuvieron proyectos de ley. En el año de 1996 Argentina aprobó una ley de protección de datos que fue vetada por el Poder Ejecutivo, y luego un proyecto nuevo fue aprobado como ley a fines del 2000, que es la ley número 25.326. Chile aprobó la primera ley de protección de datos de Latinoamérica, en 1999. Uruguay tiene varios proyectos de leyes referidos al problema de los informes de crédito.

Colombia, Venezuela, Perú y algunas provincias argentinas se vieron influenciados por la Constitución española, en tanto las leyes de protección de datos de Chile y Argentina están inspiradas en la ley de protección de datos española.

Casi todas las Constituciones latinoamericanas se refieren a la privacidad, protegiendo la correspondencia epistolar, el domicilio, el secreto de las comunicaciones y, en algunos casos, a la conciencia. Algunas Constituciones prevén la sanción de normas para la protección de la privacidad frente a la amenaza de la informática, como son las constituciones de Colombia , Perú y Venezuela.

En Guatemala, por ejemplo, el habeas data garantiza el acceso, la rectificación y la corrección de los datos sobre la persona y sus bienes, incluyendo en algunos supuestos la posibilidad de suprimir información. En este país, al igual que en Nicaragua, y Paraguay el derecho de acceso es visto como una extensión del derecho a la privacidad, en tanto en Argentina, Brasil, Perú y Venezuela se concibe como una nueva acción constitucional.

En Latinoamérica además de las constituciones se han aprobado leyes procesales y leyes sustantivas. Chile y Argentina tienen leyes que luego vamos a comentar, Brasil, Uruguay y Perú tienen proyectos de leyes, México adoptó recientemente una ley de comercio electrónico que incluye reformas a la Ley Federal de Protección al Consumidor e incluye disposiciones para el tratamiento de datos personales en las transacciones electrónicas. Brasil regula parcialmente los datos relativos a los consumidores a través del Código del Consumidor.

En Brasil, el numeral 5 de la Constitución establece “se concederá habeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo."También a Ley Federal de Protección al Consumidor regula el acceso a los datos personales del consumidor y su finalidad, así como la obligación de comunicarle la apertura de su registro personal en un banco de datos y prevé el derecho a la corrección de datos personales sobre deudas y la obligación del archivista de comunicar las correcciones a eventuales destinatarios. Se establece en cinco años el “derecho al olvido”, es decir la prohibición de comunicar datos prescritos. En 1997 el habeas data fue reglamentado procesalmente

y se presentó un proyecto de ley de protección de datos personales al Congreso pero no se le dio trámite.

En Chile la Constitución de l980 establece el derecho a la privacidad pero no tienen normas sobre protección de datos. Una ley de protección de datos fue aprobada en 1999, convirtiendo a Chile en el primer país de Iberoamérica que aprueba una ley de ese tipo.

En Colombia, la Constitución de 1991 indica que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar, incluyendo que "De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas", en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución." En este país se han producidos interesantes pronunciamientos judiciales que demuestran gran conciencia sobre el tema de la protección de datos, especialmente de la Corte Constitucional, pero no existe una ley como tal.

En México la Constitución Política contiene una cláusula general de privacidad pero no una alusión al habeas data. En junio de 2000 México incorporó en su legislación normas sobre comercio electrónico. Por ejemplo el artículo 4° reforma la Ley Federal de Protección al Consumidor regulando las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. Esta es la primera legislación en Latinoamérica sobre protección de datos personales en sistemas y servicios on line pero respecto de las otros sectores de actividad no existen leyes.

Por su parte, la Constitución de Venezuela de 1999 incluye al habeas data de la siguiente manera en su artículo 28: "Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización , la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".

Y el artículo 60 indica: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos". El numeral 281 establece: "Son atribuciones del defensor o defensora del Pueblo:...3. Interponer las acciones de inconstitucionalidad, amparo, habeas corpus, habeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los ordinales anteriores, cuando fuere procedente de conformidad con la ley..." Sin embargo, el habeas data aún no se ha desarrollado legislativamente.

SECCIÓN 3: SITUACIÓN DE ARGENTINA

Desde la década de los años 80 las provincias argentinas realizaron esfuerzos para reformar sus constituciones, para incluir normas sobre protección de la privacidad informática y habeas data, aunque sólo Buenos Aires denominó así al instituto.

La reforma Constitucional Federal de l994 incluyó al habeas data como una acción para permitir el acceso a bancos de datos personales y para corregir información falsa o discriminatoria. Surgió así la necesidad de legislación y en 1996 nace el proyecto basado en la L.O.R.T.A.D. española, que fue vetado por el Poder Ejecutivo por considerar que la ley tenía una errónea atribución de funciones al Defensor de la Nación y que restringía la libre circulación de datos personales.

A nivel provincial, el habeas data fue reglamentado procesalmente en varias provincias y existen varios proyectos en la Ciudad de Buenos Aires. Córdoba aprobó una ley sustantiva (ley No. 889l) al mismo tiempo que se sancionaba la ley de protección de datos a nivel nacional, pero el gobernador vetó esa ley.

Varios senadores presentaron al Senado una propuesta que culminó, en noviembre de 1998, con la aprobación de un proyecto de Ley de Habeas Data y Protección de Datos Personales. El l4 de septiembre de 2000, la Cámara de Diputados aprobó su versión de la Ley de Protección de Datos Personales y finalmente la Ley fue aprobada y promulgada en noviembre de 2000 que es la Ley Número 25.326.

En sus numerales 18 y 19 la Constitución establece que el domicilio y la correspondencia son inviolables, y se establece la privacidad de conciencia. Por otra parte, varios tratados internacionales de derechos humanos fueron incorporados en la reforma constitucional de l994 con jerarquía constitucional.

Es importante destacar que la ley se aplica a personas individuales. En esto, la ley argentina se diferencia de la ley chilena de Privacidad, así como también de la Directiva europea y de la nueva Ley Orgánica de Protección de Datos de Carácter Personal, lo cual podría ser considerado un avance desde cierta perspectiva si se toma en cuenta que un estudio encomendado por la Comisión Europea concluyó la necesidad de ciertos principios de la protección.datos personales a las personas jurídicas.

También la ley se aplica a ficheros manuales y automatizados. El autor Pablo Palazzi ha hecho una descripción de los principios que se encuentran presentes en la ley Argentina, tomando como base la descripción que el Grupo de Trabajo de la Unión Europea ha hecho de los principios que en su criterio rigen la materia: El Principio de limitación de objetivos según el Grupo de Trabajo de la Unión Europea, implica que los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. El Art. 43 de la Constitución Argentina, en su párrafo 3° indica: Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad" Entonces mediante una acción de habeas data es posible conocer la finalidad para la cual un registro o banco de datos trata datos personales, pero no era posible limitar dicho tratamiento por alteración de la finalidad con la que los datos fueron recolectados inicialmente. El autor expresa que en la práctica no se han incoado demandas de habeas data para obtener la finalidad del tratamiento de datos personales por lo que no existe jurisprudencia sobre la materia.

El artículo 4.3 de la ley establece que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Y el artículo 4.7 indica que “los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recabados”. Por su parte, según el artículo 11.1 los datos de carácter personal objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del

titular de los datos al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. Y el artículo 11. 2 indica que "La cesión de datos a terceros debe ser comunicada a los titulares en la primera oportunidad en que ello ocurra. El consentimiento para la cesión es revocable".

Según los principios europeos establecidos en la Directiva, las únicas excepciones al principio de limitación son las necesarias en una sociedad democrática, por alguna de las razones expuestas en el artículo 13 de la Directiva. La ley argentina en su artículo 11.3 establece que el consentimiento para la cesión no es exigido cuando: a) así lo disponga una ley, b) en los supuestos previstos en el artículo 5°; c) se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean identificables.

El artículo 25 de la ley contiene el principio de limitación de objetivos para el caso de prestación de servicios por cuenta de terceros, y el artículo 26 se refiere a la información crediticia.

En cuanto al principio de proporcionalidad y de calidad de los datos, se trata de que los datos deben ser exactos y actualizados, deben ser adecuados, pertinentes y no excesivos con relación al objetivo, exactos, actualizados. El artículo 43 de la Constitución Nacional establece el habeas data como garantía para lograr tales efectos. Es importante destacar que estos principios se aplican tanto a registros del sector público como a los del sector privado. Asimismo, el principio en cuestión se encuentra recogido en los numerales 4.1, 4.4 y 4.5 de la ley. Este principio implica además el establecimiento de normas que limiten temporariamente el almacenamiento de datos, lo cual no se incluye en los documentos de la UE, aunque refiere Palazzi que puede derivarse del mismo, pues si los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente, fácil es concluir que pasado cierto tiempo, estos datos perderán vigencia o adecuación, y que los datos muy antiguos pueden no reflejar adecuadamente la finalidad de la recolección, de manera que estos límites pueden imponerse contractualmente al realizar una transferencia en particular.

En Argentina existe un antecedente judicial sobre el llamado "Derecho al olvido" , aplicando el numeral 1071 del Código Civil. El principio se encuentra recogido en el numeral 26 de la ley en estudio.

En cuanto al principio de transparencia, se parte de que el individuo debe saber quién y por qué efectúa tratamiento de sus datos personales. Explica Palazzi que antes de la ley que estudiamos, en Argentina no existía forma de saber qué bancos de datos tratan datos personales pues no había un registro centralizado de ellos. Tampoco se requería el consentimiento para el tratamiento de datos personales ni notificación al titular de los datos.

Este principio está contenido en el numeral 5.1 de la ley de estudio. Las excepciones a la necesidad de consentimiento se encuentran previstas en el artículo 5.2 de la ley, y el numeral 13 indica que toda persona puede solicitar información al organismo de control, referente a la existencia de archivos, registros, bases o bancos de datos de carácter personal, sus finalidades y la identidad de sus responsables.

Con relación al principio de seguridad, el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Se encuentra regulado en los numerales 9 y 10 de la ley argentina.(24)

---

(24) Según tales numerales, las personas que actúen bajo la autoridad del responsable del tratamiento, incluido el encargado del mismo, no deben tratar los datos salvo por instrucción del responsable. En la ley se incluyen dos delitos al Código Penal argentino. Se sanciona al que insertare o hiciere insertar a sabiendas, datos falsos en un archivo de datos personales. La pena se aumenta al que proporcione a un tercero a sabiendas información falsa contenida en un archivo de datos personales y en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena. También se prevé la prisión de un mes a dos años el que: 1) a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales,; 2) revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá , además, pena de inhabilitación especial de uno a cuatro años.

Con respecto a los derechos de acceso, rectificación y oposición, el interesado debe tener derechos a obtener una copia de todos los datos a él relativos y derecho a rectificar aquellos datos que resulten ser inexactos y en determinadas situaciones el interesado también debe poder oponerse al tratamiento de los datos que le conciernen.

Como podemos apreciar del texto constitucional argentino, el numeral 43 no limita el alcance de la oposición al tratamiento de datos personales. Por ello consideramos con Palazzi que el individuo puede oponerse al tratamiento de datos falsos o discriminatorios, y también los sensibles. Sin embargo, en relación con cualquier otro dato que no sea falso, ni discriminatorio existe discusión sobre la posibilidad de ejercitar la acción constitucional, pues algunos afirman que el habeas data no se limita sólo a las causales de falsedad y discriminación. La jurisprudencia argentina en todo caso, ha limitado esta acción a las causales literales del texto constitucional, salvo contadas excepciones.(25)

Por otra parte, los artículos 4.6, 33, 15, 14 y 19 contienen normas referidas al derecho de acceso y sus excepciones y el titular de los datos cuenta con un derecho de rectificación, actualización o cancelación, según lo establece el numeral 16. No obstante, el derecho de acceso y oposición tiene previstas en la ley algunas excepciones: "1. Los responsables o usuarios de bancos de datos públicos pueden denegar el acceso, rectificación o la cancelación en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos de carácter personal también puede ser denegada cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo

---

(25) Como ya se había indicado, según el artículo 43 de la Constitución Argentina: "Toda persona podrá interponer esta acción (se refiere a la de amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodísticas.

establecido en los incisos anteriores, se debe brindar acceso a los registros en cuestión en la oportunidad en que el afectado deba ejercer su derecho de defensa."

En este sentido cabe indicar que la Directiva europea expresa en el artículo 9° que "en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente Capítulo, del Capítulo IV y del Capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".(26)

En el numeral 26.3 existe también un derecho de acceso previsto de servicios de información crediticia. (artículo 26.3).

El artículo 33 contiene la acción para tutelar estos derechos que denominó "De protección de los datos personales".

Con relación a la transferencias de datos a terceros países, en el numeral 12.1 se estableció en la ley la restricción de que el país receptor tenga un nivel de protección adecuado. Según Palazzi las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva,(27) no obstante, es claro que el artículo l2.2 de la ley contempla supuestos más amplios.

Sobre los datos sensibles la Directiva establece que deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para su tratamiento. Estos datos sensibles según el artículo 8 de la Directiva son los que se refieren al origen racial o étnico, a las opiniones políticas, a las convicciones religiosas o filosóficas, a la pertenencia a sindicatos, así como al tratamiento de los datos relativos a la salud o a la sexualidad. La ley argentina no tiene un artículo específico que contemple este principio, pero la jurisprudencia ha establecido que el tratamiento de datos sensible no es posible y puede ser suprimido mediante una acción de habeas data. El artículo 2° de la ley define lo que se entiende por datos sensibles,

---

(26) PALAZZI, *op. cit*., pp. 153 y 154.

(27) Las normas contenidas en los artículos 25 y 26 de la Directiva.

y el artículo 7° establece que ninguna persona está obligada a proporcionarlos. También el artículo 8 de la ley contiene protección en lo relativo a los datos de la salud. Esta coincide con lo dispuesto por el artículo 8.3 de la Directiva que dispone "El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto."

Importante es destacar el derecho que tiene el interesado, según la ley, de negarse a que sus datos sean utilizados con el propósito de mercadotecnia directa. Este derecho está contemplado en los numerales 27 y 28 de la ley, aunque el artículo 28.2 establece la posibilidad de utilización de datos mediante la técnica de disociación.

En lo referente a la autoridad encargada de la supervisión de todos estos derechos, el Grupo de Trabajo europeo sugirió la necesidad de contar con una "supervisión externa" en forma de una autoridad independiente. La ley en estudio estableció la existencia de una autoridad de control independiente al estilo de las agencias de datos europeas en los numerales 29 y 30.

En este sentido, la ley prevé sanciones tanto administrativas como Penales en los numerales 31 y 32.

SECCIÓN 4: SITUACIÓN DE COSTA RICA

En Costa Rica, fue presentado un proyecto de ley de habeas data por parte del Diputado Dr. Constantino Urcuyo en el año 1996. Este proyecto pretendía reformar la Ley de Jurisdicción Constitucional No. 7135 del 19 de octubre de 1989, adicionando un Capítulo IV que se denominaría "Habeas Data" en el Título III sobre los recursos. Se contemplaba esta garantía como una forma de amparo específico en materia de tutela de la identidad o libertad informáticas.

En Argentina, antes de la ley vigente, existió controversia sobre la necesidad de exigir para el habeas data los recaudos del recurso de amparo. En Costa Rica, en cambio, al presentar el proyecto se consideró

que al ser el recurso de amparo en Costa Rica más amplio, su estructura sería adecuada para la tutela de la libertad informática.

Consideramos que aquél proyecto tiene dos características dignas de mención:

1. Por un lado potenciaría la protección como remedio procesal fundamentalmente de una violación consumada. Esto es, el proyecto fomentaría la vigencia de una garantía procesal de reacción ante la violación del derecho, sin potenciar de manera real aspectos de fondo como sería la creación del derecho mismo y sus alcances, la prevención y las posibilidades de tutela en las diversas etapas del tratamiento de datos, como son la recogida, grabación, y la transmisión de datos a otros países.

Es cierto que el numeral 77 del proyecto contempla la posibilidad de la intervención de la Sala Constitucional mediante la interposición del habeas data para la prevención y en las distintas fases del tratamiento de datos, pero la cantidad de trabajo de dicho tribunal y la velocidad con que los datos se tratan parecen hacer de esa finalidad una ilusión. Como respuesta a esta problemática, en Europa se ha propuesto la creación de órganos independientes con capacidad técnica. Consideramos que esta solución debería ser un elemento de la discusión en nuestro país, dadas sus implicaciones.

El autor nacional Alfredo Chirino analizando el proyecto, expresa: "la impresión que da el proyecto, luego de leer su articulado, es la de que constituye, principalmente, una tutela procedimental a la intimidad del ciudadano, y solo eventualmente a su derecho de ser informado. Esto se debe al énfasis puesto en la redacción del proyecto a tutelar el así llamado "habeas datas propio".

2. Por otra parte, ya limitándose al aspecto procesal, el proyecto es amplio al prever el habeas datas propio y el habeas data impropio. El primero, indica el proyecto, contempla los derechos de acceso, modificación, adecuación al fin, confidencialidad, eliminación e inclusión de datos de la persona. El segundo tutela el derecho de los ciudadanos al acceso a la información, frente a la cual se tiene un interés legítimo.

Como aspecto positivo del proyecto conviene destacar que protege al individuo del tratamiento de datos personales que aunque se realizan con un fin legítimo, luego el fin es quebrantado o los datos son utilizados con otros objetivos, así como cuando el dato no es fidedigno o

cuando se producen lesiones a la intimidad debido a escasas o inexistentes medidas de seguridad en el centro de cómputo.

Otro aspecto de importancia del proyecto es que contempla la autodeterminación informativa y la intimidad como bienes jurídicos a proteger, aunque no los define, lo que podría haber ocasionado que en la labor de interpretación se produjera una tutela reducida, que atienda sólo al derecho al acceso a los datos, es decir una tutela al dominio sobre los datos personales, cuando en esencia lo que debe protegerse es el derecho del ciudadano a saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas y bajo qué circunstancias. Este conglomerado de derechos que acabamos de mencionar son los que el autor nacional Alfredo Chirino, siguiendo la doctrina alemana llama derecho a la autodeterminación informativa(28) que rebasa el derecho a la intimidad. Tal como quedó expuesto, en Europa existe discusión sobre la autodeterminación informativa como bien jurídico. En nuestro criterio, ante las posibilidades de una interpretación restrictiva del derecho a la intimidad, conviene llevar a cabo una definición legal de los campos de tutela, que no de margen a restricciones en la interpretación, por encima de la denominación que se adopte.

En la sección primera establecimos la relación entre la protección de los datos personales y la democracia, que en líneas generales nos conduce a que ese ámbito personal o de "intimidad" entendida en sentido amplio constituye una garantía para el ejercicio de otros derechos fundamentales que definen al ciudadano como un ser racional y libre con las limitaciones estrictamente necesarias para no lesionar la moral, el orden público y a los terceros (artículo 28 constitucional) a efecto de que pueda relacionarse en sociedad pero realizando su proyecto personal de vida, lo que implica la protección frente a intervenciones estatales o privadas.

Ahora bien, el proyecto que comentamos se delegó a una comisión legislativa pelan, se aprobó en primer debate, y fue en consulta a la Sala Constitucional, la que encontró vicios e procedimiento que justificaron que el expediente fuera archivado.

Posteriormente fue presentado otro proyecto bajo el número de expediente 14778, por parte de los diputados Carlos Avendaño, Rocío

---

(28) Sobre la autodeterminación informática, ponencia del Dr. Alfredo Chirino, en el IX Congreso Iberoamericano de Derecho e Informática "Justicia e Internet" celebrado en San José, Costa Rica del 1 al 5 de abril del 2002.

Ulloa y Laura Chinchilla. Asimismo, el diputado Rolando Laclé presentó un proyecto que ocupa el expediente número 14785. Estos últimos dos proyectos se encuentran en el orden del día en la Comisión de Asuntos Jurídicos de la Asamblea Legislativa pero no se han trabajado, pues existe un proyecto de gran envergadura de otra materia que mantiene a la Comisión respectiva ocupada por largo tiempo.

La diputada Laura Chinchilla en asocio con otros diputados trabajan en este momento un texto sustitutivo del primero de estos dos proyectos, que se encuentra en borrador.

En nuestro país se han producido dos votos importantes respecto a la protección de la persona frente al tratamiento de datos: En el voto 2251-91 la Sala Constitucional rechazó un recurso de amparo de una persona que solicitaba tener acceso a "documentos que la Junta Directiva de la CCSS conoce al resolver gestiones". En el Voto 3267-95 la misma Sala declaró con lugar un recurso de amparo contra el OIJ que tenía en sus archivos de indiciados a una persona que había sido absuelta. La Sala obligó a eliminar el archivo.

SECCIÓN 5: PROPUESTA: LA PROTECCIÓN DE DATOS PERSONALES COMO INDICADOR DE DESARROLLO HUMANO

"…hay nuevas fuerzas e instituciones que ejercen gran influencia en la vida de las personas. Y hay nuevos tipos de conflicto que se extienden dentro de los países y entre ellos…Está claro que hay que actuar. Se sigue necesitando la voluntad de adoptar medidas que promuevan la democracia, fomenten el desarrollo y extiendan las libertades humanas por todo el mundo." Informe de PNUD 2002 p.9.

Hasta ahora hemos elaborado varias afirmaciones que nos llevarán a sustentar la propuesta que formulamos en la presente sección: hemos afirmado que hay un peligro intrínseco al manejo de datos personales para esa esfera del ser humano que requiere ser regida por su voluntad y sin la intromisión externa; hemos afirmado que sin una correcta protección del manejo de datos personales muchos derechos individuales corren el riesgo de ser anulados; hemos indicado que la anulación de tales derechos redundaría en la disminución de la capacidad de autodeterminación y la negación de la posibilidad de realización de cada proyecto de vida; hemos indicado que las circunstancias actuales originadas en los hechos de setiembre del año

antepasado potencian un cambio de postura política respecto del manejo de la información; afirmamos que existe una relación de proporcionalidad directa entre la vigencia del modelo democrático y la tutela a la autodeterminación del ser humano mediante la protección de sus datos personales; y por último, hemos expresado que esta visión que proponemos no riñe con la visión de democracia expuesta por organismos oficiales como la Organización de Naciones Unidas a través de sus publicaciones del PNUD.

Siendo que es sobre las ideas anteriores que desarrollaremos la propuesta que sigue, empezaremos por exponer el concepto de desarrollo esbozado por el PNUD, en el entendido de que el mismo es utilizado por nosotros como un instrumento de trabajo, pues si bien existe discusión teórica sobre el concepto de desarrollo, lo expresado por esa entidad constituye un punto de partida valioso para la discusión que proponemos. Su valor estriba en la escasa resistencia, que por razones ideológicas, ofrecen a los pronunciamientos de tales organismos nuestros posibles interlocutores en Costa Rica, lo que ya significará un punto de encuentro.

Al partir del paradigma democrático para la evaluación del desarrollo de las naciones,(29) el informe del PNUD de 2002 abre el concepto mismo de desarrollo y hace alusión a las posibilidades de participación democrática, y a la calidad de vida:

"Irónicamente, el enfoque de desarrollo humano del desarrollo ha sido víctima del éxito de su índice de desarrollo humano (IDH). El IDH ha reforzado la interpretación restringida y demasiado simplificada del concepto de desarrollo humano, como si se tratara únicamente de mejorar la educación, la salud y los niveles aceptables de vida. Ello ha oscurecido el concepto más amplio y complejo de desarrollo humano como expansión de capacidades que amplía las posibilidades de la gente de vivir la vida que deseen y valoran. A pesar de cuidadosos esfuerzos por explicar que el concepto es más amplio que su instrumento de medición, el desarrollo humano continúa siendo identificado con el IDH mientras se ignoran a menudo las libertades políticas, la participación en la vida comunitaria y la seguridad física. Sin embargo, esas condiciones

---

(29) "Para que las políticas y las instituciones políticas promuevan el desarrollo humano y protejan la libertad y la dignidad de todas las personas, se ha de ampliar y consolidar la democracia…" Informe del PNUD 2002, Profundizar la democracia en un mundo fragmentado, p. 1.

son tan universales y fundamentales como poder leer o disfrutar de buena salud. Todos las valoran –y sin ellas se cierran muchas otras opciones. No se incluyen en el IDH porque son muy difíciles de medir de manera adecuada, no porque sean menos importantes para el desarrollo humano."(30)

Esta visión del desarrollo en democracia nos lleva entonces a sostener tres afirmaciones: La primera es que el concepto de desarrollo humano es más grande que el índice.(31) La segunda es que para evaluar el desarrollo es posible (y necesario) incluir nuevas categorías distintas de las que se han utilizado hasta el momento siempre que no ofrezcan dificultades de medición (siguiendo la lógica del texto). Y la tercera es que la protección de la persona frente al tratamiento de sus datos personales puede (y debe) constituirse en una categoría de la medición del desarrollo en democracia, puesto que, de ello depende en parte la *"expansión de capacidades que amplía las posibilidades de la gente de vivir la vida que deseen y valoran"* y porque de ello depende en gran medida –como ya adelantamos– la vigencia del modelo democrático.

En contra de lo que acabamos de proponer, podría argumentarse que dadas las mismas limitaciones apuntadas para la medición del desarrollo, no es posible apartarse de una posición economicista o al menos estadísticamente sostenible. A este respecto hemos de indicar que el mismo PNUD afirma en su último texto la necesidad de apartarnos de tal visión: "El desarrollo humano trata de las personas y de ampliar sus alternativas para que puedan tener un nivel de vida que aprecien. El

---

(30) Informe de PNUD 2002, p. 53.
Sobre el índice de desarrollo humano el documento expresa: "El índice de desarrollo humano (IDH) es una medida compuesta de tres dimensiones del concepto de desarrollo humano: vivir una vida larga y saludable, recibir educación y gozar de un nivel de vida decoroso… De este modo en él se combinan la medición de la esperanza de vida, la matriculación escolar, la alfabetización y los ingresos, a fin de ofrecer un panorama del desarrollo de un país más amplio que el que resultaría si se consideraran únicamente los ingresos, que con demasiada frecuencia se equiparan al bienestar. Desde que se creó el IDH en 1990, se han creado tres índices complementarios para destacar aspectos particulares de desarrollo humano: el índice de pobreza humana (IPH), el índice de desarrollo relativo al género (IDG) y el índice de potenciación de género (IPG)" PNUD, *op. cit*., p. 34.

(31) En este mismo sentido ver Informe de PNUD 2002 recuadro 22.

crecimiento económico, el incremento del comercio y de la inversión económica internacional, y los avances tecnológicos son muy importantes, *pero son medios y no fines*. El que puedan contribuir al desarrollo humano en el siglo XXI dependerá de que sirvan para ampliar las alternativas de las personas, de que coadyuven a crear un entorno en el que la gente pueda desarrollar sus posibilidades plenamente y vivir de modo productivo y creativo. Para ampliar la gama de alternativas humanas es fundamental desarrollar las capacidades humanas: la gama de cosas que la gente puede llegar a ser o hacer…"(32)

Ahora bien, según el documento en su conjunto, la necesidad de ampliar las meras posibilidades personales, debe estar unida a la existencia de instituciones responsables de la vigencia de los derechos humanos: "…la gobernabilidad en pro del desarrollo humano exige mucho más que la existencia de instituciones estatales eficientes. La buena gobernabilidad también requiere promover instituciones justas y responsables que amparen los derechos humanos y las libertades fundamentales …los países pueden promover el desarrollo humano para todos solamente si cuentan con sistemas de gestión pública que respondan completamente ante toda la gente y si todas las personas pueden participar en los debates y las decisiones que afectan sus vidas…".(33) Estas afirmaciones sin duda abren paso a la idea de la necesidad de la vigencia de todo un sistema institucional (normativo preventivo y reactivo) que garantice la protección de la persona frente al tratamiento de sus datos personales puesto que defenderle al ser humano ese ámbito de autodeterminación, le garantiza no sólo la posibilidad de realización sino también la posibilidad de participación política y social.

En este sentido el informe del PNUD es claro cuando afirma que "El hecho de conceder a todas las personas una igualdad política oficial no basta para crear en la misma medida la voluntad o capacidad de participar en los procesos políticos, ni una capacidad igual en todos de influir en los resultados…".(34)

Así las cosas, tenemos que tanto desde un pensamiento crítico como desde un ángulo más ajustado con el pensamiento oficial, existe la

---

(32) PNUD, *op. cit.,* p. 13, el destacado no es del texto.

(33) PNUD, *op. cit.*, p. 3.

(34) PNUD, p. 4.

posibilidad de incluir dentro de la institucionalidad de nuestro país, los elementos necesarios para proteger a la persona frente al tratamiento de los datos.

Sin embargo, existe una pregunta que no hemos contestado y cuya respuesta va a tener influencia directa en la discusión que proponemos:

¿Controlan las leyes la circulación de datos o más bien la potencian?

"Y si, como observa Lord Bacon, el conocimiento es poder, se ampliarán los poderes humanos; la naturaleza, sus sustancias y sus leyes estarán cada vez más bajo nuestro control, los hombres conseguirán que su existencia en esta tierra sea más fácil y confortable; probablemente lograrán prolongar la duración de la vida y crecer más felices cada día y cada vez serán más capaces (y espero que también más proclives,) de comunicar esta felicidad a los demás..."(35)

Varios autores han destacado que el llamado avance tecnológico para estar verdaderamente al servicio de la humanidad necesita ser reorientado, pues hasta el momento, en lugar de mejorar las condiciones de vida de las personas ha significado un retroceso: "Es innegable que hay avance: pero también hay retroceso. Para la solución de un buen número de problemas de la humanidad se necesita tecnología, sin embargo ahí no se agota el asunto. En otros casos lo que se necesita es una reorientación de la tecnología (investigación y producción de ésta) hacia metas más acordes con la respuesta de desafíos surgidos, en parte al menos, por la participación de algunos despliegues tecnológicos."(36)

Justamente uno de los retrocesos relacionados con el aumento y propagación de los medios tecnológicos es la exposición del ámbito personal a la vista y tratamiento público o general, lo que viene a poner

---

(35) JOSEPH PRIESTLEY, en Mori, Georgio. La Revolución Industrial, 1983, citado por Edgar Roy Ramírez B. ¿Será mejor todo tiempo futuro? En *Tras El Término Tecnología y Otros Ensayos*, Editorial Tecnológica de Costa Rica, Cartago, Costa Rica, 1995, p. 66-67.

(36) RAMÍREZ B., Edgar Roy. ¿Será mejor todo tiempo futuro?, en *Tras El Término Tecnología y Otros Ensayos*. Editorial Tecnológica de Costa Rica, Cartago, Costa Rica, 1995, p. 66.

en cuestión los principios derivados desde las conquistas que sustentan la democracia y que ubican al hombre como un fin en si mismo. En este sentido, aunque se afirme que debido al avance tecnológico son enormes las posibilidades de acción y participación ciudadana, "…vale la pena señalar la advertencia del escritor mexicano Raúl Trejo, para quien esta acción ciudadana no puede restringirse al simple berrinche electrónico de algunos sectores, sino que debe convertirse en acción eficaz que propugne por una participación real de la sociedad en su conjunto."(37)

Pero justamente el factor de desconfianza que puede surgir sobre el amo al que están sirviendo estas leyes de protección de datos, radica en la escasa participación de la sociedad en la discusión de los temas que aborda, y correlativamente, la participación de los grandes intereses económicos en la aprobación de leyes cuyo resultado es –para la protección de la persona– dudoso.

La participación de los grandes intereses económicos en la creación de estas leyes obedece a la necesidad de garantizarse la posibilidad de continuar con la actividad del tratamiento de datos y todas las actividades que ello implica. Pero además hay quienes afirman que sin un mínimo de seguridad para el titular de los datos personales, la actividad económica relacionada con el tratamiento de datos corre el riesgo de detener su crecimiento. Así por ejemplo se ha dicho: "...las encuestas realizadas a los usuarios de Internet revelan que el futuro crecimiento del comercio electrónico a través de ésta, dependerá en gran parte de la seguridad y confidencialidad de las transacciones. Los compradores y vendedores sólo aceptarán Internet con fines de comercio electrónico si confían en que los pedidos y los pagos tendrán lugar con un riesgo mínimo de engaño y uso indebido de cualquier información proporcionada. Si temen que sus pedidos se alteren antes de llegar a su destino, que se roben los números de sus tarjetas de crédito o que la información de carácter privado sea encaminada incorrectamente, los usuarios volverán a utilizar instrumentos más tradicionales de comercio, de hecho que la utilización comercial en el pasado de las transmisiones telefónicas y por telefax se vio a menudo limitada por preocupaciones relativas a la seguridad."(38)

---

(37) Instituto Misionero Hijas de San Pablo, *El Rostro Humano de aa Cultura Digital*, Géminis Ltda., Bogotá, Colombia, 2000, p. 61.

(38) KNORR, Jolene Marie y otro, La Protección Del Consumidor En El Comercio Electrónico, Investigaciones Jurídicas S.A., San José, Costa Rica, 2001, pp. 48-49.

Hechas estas reflexiones, conviene ahora mirar a la práctica a efecto de determinar los dobleces que pueda presentar la promoción de una ley de protección de datos personales. El caso más ilustrativo que hemos encontrado es el de Chile, cuya ley fue redactada a instancias de la asesoría de los grupos y empresas relacionados con el tratamiento de datos. Según algunos, dichas empresas estaban "interesadas en asegurar el lucrativo negocio que constituye el procesamiento de datos personales, lo que se sumó a la ignorancia inexcusable de los parlamentarios que día a día siguen jactándose de su autoría con fines de marketing."(39)

Renato Javier Jijena Leiva, comentando el numeral cuarto de la ley chilena indica que es la norma más conflictiva y confusa, y de ella se deriva la afirmación de que la ley tendió a proteger y legalizar el negocio del procesamiento de datos personales desde la perspectiva de las empresas, más que a proteger a las personas titulares de los datos. Lo anterior por cuanto el artículo contiene un principio general en materia de procesamiento de datos personales que luego es burlado por la cantidad y calidad de excepciones que el mismo numeral consagra. En efecto, el artículo señala que el tratamiento de los datos personales sólo podrá efectuarse cuando esta ley u otras disposiciones legales lo autoricen, o cuando el titular consienta expresamente en ello. Entonces, la norma potencia los contratos de adhesión que prácticamente obligan al consentimiento. Además la norma establece que en determinados casos no se requiere autorización para el tratamiento de datos personales cuando los datos provengan o se recolecten de "fuentes accesibles al público" que en realidad constituyen la regla general. Dichas excepciones son las siguientes: "a) Cuando sean de carácter económico, financiero, bancario o comercial. b) Cuando se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento. La expresión "tales como" demuestra que se trata por ende de una enumeración sólo ejemplar o "numerus apertus". El uso de la expresión se traduce en que será una cuestión de hecho que en definitiva determinarán los tribunales para cada caso concreto sometido a su decisión...c) Cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Si bien es cierto

---

(39) JIJENA LEIVA, Renato Javier. *Luces y sombras de la ley chilena sobre protección de datos personales.* Flile://C:/TEMO/htm2606.htm

que desde un punto de vista comercial aparece conveniente la relación directa entre una empresa y sus clientes, la posibilidad de decidir que dicha relación exista o no, le compete a los consumidores los que pueden desear mantenerse al margen y resguardar la privacidad de sus datos personales para no ser invadidos con agresivas campañas comerciales o promocionales y recibir e-mails, cartas, folletos o llamados telefónicos, y así debiera garantizarse jurídicamente".(40)

Por otra parte, el artículo 4 de la ley indica que no se requiere autorización para el procesamiento de datos personales que provengan de fuentes públicas cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, lo que, sumado a las dos excepciones anteriores implica casi la anulación del poder de control para el titular de los datos.

Otro aspecto que determina el interés de la ley es que no se refiere a la transferencia de datos más allá de la frontera Chilena, como sí lo hace por ejemplo la ley Argentina en su artículo 12, según vimos. "…En nuestra opinión la razón es una sola: ...las empresas chilenas que han sido adquiridas por empresas transnacionales como la norteamericana Equifax pueden operar libremente y sin restricción alguna desde servidores ubicados en el extranjero y mediante la red internet, con la salvaguarda de que la norma chilena es territorial y no los puede alcanzar más allá del límite jurisdiccional de Chile.(41)

De manera que la evidencia acredita que la promoción de las leyes sobre protección de datos personales puede ser tendenciosa o interesada, pero nosotros consideramos que justamente lo que un país no puede permitirse es la ignorancia y la falta de discusión seria sobre el tema. Nosotros proponemos que en Costa Rica se produzca una discusión abierta, que aborde todos los elementos que de seguido expondremos, y que en nuestro criterio deben también estar contenidos en los cánones para determinar el desarrollo de una nación, por todas las razones expuestas a lo largo de este trabajo.

---

(40) JIJENA LEIVA, Renato Javier. *Luces y sombras de la ley chilena sobre protección de datos personales*. Flile://C:/TEMO/htm2606.htm

(41) JIJENA LEIVA, *op. cit.*

Elementos a considerar dentro del indicador de la protección de datos personales como factor de desarrollo humano

Hemos expuesto las razones por las cuales consideramos que es posible y necesario incluir como factor de desarrollo humano la protección de las personas frente al tratamiento de datos personales. Ahora bien, luego del recorrido que ha implicado esta investigación, y tomando en cuenta las experiencias prácticas que hemos conocido, sugerimos una serie de elementos que deberán ser tomados en cuenta al construir el indicador propuesto y que –junto con todas las ideas expuestas en este estudio- son puntos que deberán ser considerados para la discusión que proponemos en nuestro país:

1. Se deberá partir del derecho a la privacidad de los datos personales en sentido amplio o la autodeterminación informativa como derecho humano fundamental.
2. El indicador deberá constatar la existencia de una ley o cuerpo normativo sobre de protección de datos
3. La vigencia de la norma general de prohibición de tratamiento de datos personales
4. La existencia de acciones preventivas más que reactivas
5. Que las excepciones a la prohibición de tratamiento de datos personales no sean numerus apertus
6. La previsión de habeas data como garantía procesal o una similar, simple y desformalizada.
7. La protección no sólo frente a datos finales sino también en las diversas formas de recopilación y procesamiento y transmisión de información.
8. La existencia de una autoridad administrativa aplicadora u órganos que actúen con celeridad y eficiencia.
9. La existencia real de un procedimiento ágil.(42)
10. La vigencia de la norma de puerto seguro y regulación de transferencia de datos transfronteras.
11. Dentro de las excepciones a la prohibición de tratamiento de datos no deberá contemplarse: i. El consentimiento del titular que se presta para la existencia de contratos de adhesión. iii. Datos sean

(42) Que no parta de que el ciudadano es quien se da cuenta de la lesión, quien ha de ofrecer "prueba de cargo", hacer referencia de los funcionarios públicos o de los particulares que han realizado el procesamiento, así como una descripción del "hecho u omisión" que motiva la acción.

de carácter económico, financiero, bancario o comercial. iii. Listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento. iv. Datos necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, v. Datos que provengan de fuentes públicas.

12. En caso de establecerse como excepción a la prohibición el interés público, la norma debe contener cómo se define éste.
13. La existencia de un tribunal ágil y expedito.

Deben las normas de Protección de Datos Personas físicas y jurídicas?

Este trabajo inscribe sus propuestas dentro de los vértices democracia, autodeterminación informativa y desarrollo. Hemos expuesto que cada uno de esos vértices deben apuntar a la tutela y protección de la persona humana quien es el fin, concibiendo los otros elementos e intereses como medios.

Si hemos expuesto que la autodeterminación informativa como bien jurídico es la que torna necesaria la protección, será fácil concluir que tal bien jurídico no cobija a las personas jurídicas, puesto que dijimos que partimos con Ferrajoli de que los bienes jurídicos deben tener siempre como titular a las personas. Lo anterior no quiere decir que las personas jurídicas no deban ser objeto de tutela, sino que la discusión deberá abrirse, para determinar cuál es el bien jurídico a tutelar en esos casos. Así por ejemplo, podría decirse que se trata del derecho a la imagen comercial o al nombre. Lo que debe quedar claro es que los argumentos que fundamentan la tutela a las personas físicas no pueden apoyar –desde un punto de visto lógico jurídico- la tutela de las personas jurídicas. Sería conveniente una discusión que se ocupe de estos temas para evitar que el producto legislativo incluya normas dentro de un ámbito de protección que no es exactamente el que le corresponde o bajo una nebulosa teórica.

Algunos han dicho que "...la información sobre las personas jurídicas es tan relevante como la de las personas naturales y también merece ser resguardada. Esta tutela jurídica por ende permanece en el ámbito de las reglas generales del derecho, por lo que cualquier persona jurídica respecto de la cual se abuse de sus antecedentes propios o bien

éstos sean procesados en forma errada (datos obsoletos, caducos, inexactos), deberá recurrir a los procedimientos, acciones y recursos generales contemplados en nuestro ordenamiento jurídico. Estimamos que si bien en menor amplitud que las personas naturales, las personas jurídicas también gozan de un necesario derecho a la confidencialidad o reserva de los antecedentes que a ellas se refieren, por cuanto éstos las convierten en sujetos de derechos y en personas identificadas o identificables."(43)

CONCLUSION

Hemos visto que Latinoamérica se acerca más al modelo europeo de protección de datos que al Norteamericano que parte del principio de la privacidad. No obstante, falta mucho por recorrer en este camino.

Si la tendencia continuara así y América Latina opta por el modelo europeo que prevé las agencias de protección de datos, éstas podrían ser importantes para contrarrestar las presiones que por la demanda de seguridad, impone la vigilancia que se ha incrementado luego del desastre de setiembre de 2001. Los intereses políticos vigentes originados en esos eventos, tornan más difícil la unificación de los sistemas de protección.

Para que la normativa por hacer tienda verdaderamente a proteger los derechos de las personas, se hace necesario promover la discusión abierta que podría estar fundada sobre los vértices democracia, desarrollo y protección de datos personales.

Hemos aportado una síntesis de los elementos que debería contener tal discusión. Por otra parte, las agencias oficiales que ostentan alguna autoridad internacional deberán abrirse a la valoración de la protección de la persona humana frente el al tratamiento de datos personales si pretenden "medir" el desarrollo" como calidad de vida.

---

(43) JIJENA LEIVA, Renato Javier. *Luces y sombras de la ley chilena sobre protección de datos personales*. Flile://:/TEMO/htm2606.htm

BIBLIOGRAFÍA

BECK, Ulrich. *¿Qué es la Globalización? Falacias del globalismo*, respuestas a la globalización. Piados, Barcelona, 1998.

CAMPUZANO TOMÉ, Herminia. *Vida Privada y Datos Personales, su protección frente a la sociedad de la infomación*. Tecnos, Madrid, España, 2000.

CASSESE, Antonio. *Los Derechos Humanos en el mundo contemporáneo*. Ariel, Barcelona, España, 1991.

CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación informativa y Estado de Derecho en la Sociedad Tecnológica*. CONAMAJ, San José, Costa Rica, 1997.

CHIRINO SÁNCHEZ, Alfredo. *Ponencia sobre autodeterminación informativa en el IX Congreso Iberoamericano de Derecho e Informática "Justicia e Internet"* celebrado en San José, Costa Rica del 1 al 5 de abril del 2002.

DAVARA RODRÍGUEZ, Miguel Angel. *Manual de Derecho Informático. Aranzadi*. Madrid, l997.

FERRAJOLI, Luigi. *Derecho y razón. Teoría del garantismo penal*. Editorial Trotta, Madrid, 1995.

FERREIRA RUBIO, Delia Matilde. *El derecho a la intimidad*. Editorial Universidad, Buenos Aires, 1982.

GARRIDA DOMÍNGUEZ, Ana. *La protección de los datos personales en el Derecho Español*. Universidad Carlos III de Madrid, Dykinson, Madrid, 1999.

GUIBOURG, Ricardo A. y otros. *Manual de informática jurídica*. Astrea, Buenos Aires, 1996.

HERNÁNDEZ VALLE, Rubén. *El Régimen Jurídico de los Derechos Fundamentales en Costa Rica*. Editorial Juricentro, 2001, San José, Costa Rica.

Informe de PNUD 2002, *Profundizar la democracia en un mundo fragmentado*.

Instituto Misionero Hijas de San Pablo. *El Rostro Humano de la Cultura Digital*. Géminis Ltda., Bogotá, Colombia, 2000.

JIJENA LEIVA, Renato Javier. *Luces y sombras de la ley chilena sobre protección de datos personales*. Flile://C:/TEMO/htm2606.htm

Joseph Priestley, en MORI, Georgio. *La Revolución Industrial*, 1983, citado por, citado por Edgar Roy Ramírez B., ¿Será mejor todo tiempo futuro? En *Tras El Término Tecnología y Otros Ensayos*. Editorial Tecnológica de Costa Rica, Cartago, Costa Rica, 1995.

JOYANES AGUILAR, Luis. Cibersociedad. *Los retos sociales ante un nuevo mundo digital*. Mcgraw-Hill, España, 1997.

KNORR, Jolene Marie y otro. *La Protección del Consumidor* en *El Comercio Electrónico*. Investigaciones Jurídicas S.A., San José, Costa Rica, 2001.

LLAMAZARES CALZADILLA, María Cruz. *Las libertades de expresión e información como garantía del pluralismo democrático*. Departamento de Derecho Público y Filosofía del Derecho, Universidad Carlos III De Madrid, Civitas, Madrid, España, 1999.

MOYA, Eugenio. *Crítica de la Razón Tecnocientífica*. Biblioteca Nueva, S,L, Madrid, 1998.

PALAZZI, Pablo A. L*a transmisión internacional de datos personales y la protección de la privacidad*. Ad Hoc, Buenos Aires, febrero de 2002.

PIERINI, Alicia y LORENCES, Valentín. *Derecho de acceso a la información. Por una democracia con efectivo control ciudadano, Acción de Amparo*. Editorial Universidad, Buenos Aires, 1999.

RAMÍREZ B., Edgar Roy. ¿Será mejor todo tiempo futuro? en *Tras El Término Tecnología y Otros Ensayos*. Editorial Tecnológica de Costa Rica, Cartago, Costa Rica, 1995.

RIVAS, Alejandro Javier. Riesgos legales en Internet. Especial referencia a la protección de datos personales, en *Derecho de Internet. Contratación electrónica y firma digital*. Aranzadi, España, 2000.

RODRÍGUEZ RUIZ, Blanca. *El secreto de las comunicaciones, tecnología e intimidad*. McGraw Hill, Madrid, 1997.

SAXE FERNÁNDEZ, Eduardo. *Militarización de la crisis mundial: costos de la hegemonía, colapsos mundiales y pensamiento oficial*, en Documentos de estudio, número 15, ERI, UNA, Nueva Época, 2002.