CELARE
EUROLAT
Revista de Relaciones Eurolatinoamericanas
Nº 83 - Año 17 - Agosto 2011

LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA Y AMÉRICA LATINA

UPV UNIVERSIDAD PEDRO DE VALDIVIA

CELARE - Centro Latinoamericano para las Relaciones con Europa
Centro Académico asociado a la
UNIVERSIDAD PEDRO DE VALDIVIA, CHILE

ÍNDICE

La protección de datos, Un derecho humano del Siglo XXI

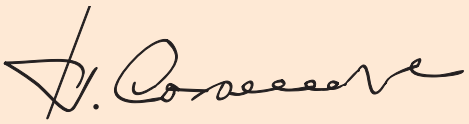
Héctor Casanueva

Director Ejecutivo de CELARE

La protección de datos es hoy una inevitable preocupación ciudadana, de la que es preciso que las autoridades se hagan cargo, en un contexto de exponencial crecimiento de la demografía de la red Internet y, por lo tanto, de la permeabilidad y la accesibilidad a la información personal. La protección a este ámbito de la vida privada de las personas, emana de los principales instrumentos internacionales de derechos humanos. Sin embargo, los avances en las TI y sus implicaciones han dado origen a un derecho distinto, para proteger la intimidad y la privacidad, pues el uso cada vez más extendido de la informática facilita la acumulación de grandes cantidades de información personal, no solamente su identidad, sino la creación de perfiles del comportamiento, enfermedades, dónde y qué compran, situación laboral, socio-económica, entre otras. Por tanto, la autodeterminación informativa es el derecho que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaba y utiliza sus datos.

La Unión Europea ha llevado a cabo un largo proceso para llegar a una normativa que regule la protección de datos en la red, se ve reflejado extensamente en las innumerables reuniones y acuerdos entre los países desde varias décadas atrás. En América Latina es una temática que se aborda también y que cada día cobra mayor fuerza. La próxima Cumbre ALC-UE a realizarse en Chile en 2013 debería abordar en alguna de sus temáticas la cooperación en esta materia, muy necesaria para ambas regiones.

En esta edición de la Revista EUROLAT, hemos querido dar a conocer, mediante la colaboración de especialistas de diferentes países y el trabajo del equipo de comunicaciones de CELARE, cómo se desarrolla este tema en los países miembros y en las instituciones de la Unión Europea, así como los avances que se van produciendo al respecto también en América Latina, que en muchos casos tienen como referente a la Europa comunitaria. Contribuimos con ello a poner de manifiesto la necesidad de la oportuna y permanente actualización en la normativa reguladora de esta materia, indispensable para un normal desarrollo del mercado, del trabajo, de las redes sociales, de la relación del ciudadano con el Estado, y en definitiva, de la democracia.



Democracia, constitución y protección de datos personales

*Por Raúl Arrieta

Abogado de Gutierrez & Brodsky en Derecho Público y Derecho y Tecnología. Chile

El desarrollo de las Tecnologías de la Información y Comunicación y la aparición de Internet, en particular, como importante canal de distribución de bienes y servicios ha cambiado a fondo a) las economías, los mercados y las estructuras industriales; b) los productos, los servicios y sus flujos; c) la segmentación de los consumidores, sus valores, su conducta; y d) los mercados de empleo y mano de obra. En definitiva, se ha ido produciendo en forma paulatina, pero con una velocidad abismante un cambio en la sociedad, en la forma de vida y en la política.

Causa de ello sin duda representa el hecho que el desarrollo que han experimentados las tecnologías de la información y comunicación en los últimos años hayan hecho viables cuestiones que parecían imposibles de realizar y, que consecuentemente formaban sólo parte de lo posible. Sin embargo, es necesario tener presente que por el hecho de que una determinada cosa la permita a la tecnología no necesariamente es deseable que ella se arraigue dentro de nuestra democracia. Adicionalmente, resulta relevante considerar que la tecnología confiere poder económico y político, y éste puede ejercerse para bien o para mal, así la tecnología nunca será socialmente neutra, ya que produce repercusiones sociales, obligando al Estado a intervenir. Es por ello que estimamos que cualquier análisis que se haga respecto a la irrupción de estas tecnologías y de Internet en la vida cotidiana de las personas, necesariamente nos obliga a considerar que éstas han de situarse al servicio de las personas y nunca a la inversa.

En la época en que vivimos las personas dejan huellas electrónicas, rastros de su identidad, comportamiento y preferencias en las bases de datos de los servicios que utilizan. Desde el momento en que se levantan van dejando trazas del quehacer diario. Así, al utilizar el teléfono, al circular por las autopistas urbanas, al pagar con una tarjeta de crédito, al registrarse en el ingreso a la oficina, al navegar por Internet, al comprar, etc. De este modo, a medida que las tecnologías se hacen más presentes en el quehacer diario, más huellas van quedando almacenadas, o lo que es igual, más rastros de las personas es posible encontrar. Junto a ello, hay muchas bases de datos y empresas que utilizan dicha información, sea capturándola, organizándola, vendiéndola y en general utilizándola.

Lo anterior, más allá de constituir una situación cotidiana que el desarrollo de las tecnologías de la información y comunicación permite, y que en principio podríamos acordar resulta axiológicamente neutro, requiere ser analizada al alero de la indispensable defensa de los derechos fundamentales, de manera de argüir si dicha clase de actividades puede llegar a menoscabarlos.

En esta perspectiva es posible sostener que el desarrollo de las tecnologías de la información y comunicación van configurando una serie de cambios en lo que guarda relación con la forma en que las personas se relacionan con el entorno y consecuentemente con la forma en que las mismas vinculan con la igualdad, libertad y dignidad, todos axiomas constitucionales que sirven o sirvieron de base al desarrollo constitucional contemporáneo y por supuesto de nuestra Democracia. Al respecto, no es vano recordar que el Anteproyecto Constitucional y sus Fundamentos nos ilustra justamente respecto a estos valores en el constitucionalismo nacional, al señalar que la constitución al disponer en su artículo 1º que "los hombres nacen libres e iguales en dignidad", ha querido consagrar esta norma no sólo inspirado en los preceptos de la Declaración Universal de los Derechos Humanos, sino especialmente en la tradición libertaria de Chile, respetuosa de la persona humana como ser dotado de inteligencia y voluntad libre por su creador. El respeto a la dignidad del hombre es, pues, el principio fundamental que inspira la nueva constitución.

Ahora bien, estimamos que el análisis de esos cambios resulta relevante tenerlos en consideración ya que han de incitarnos a considerar que el contexto y argumentos que se tuvieron a la vista a la hora que el poder constituyente definiera el contenido de nuestra Carta Fundamental ya no sean necesariamente los mismos, sin que ello cuestiones la vigencia o validez de la misma, pero sí que haga necesario y del más alto interés reflexionar en torno a las consecuencias que estos cambios han producido en el sistema de garantías como elemento sustancial de nuestra democracia, de manera de determinar si la Constitución se basta tal como está para que no haya merma en el amparo de los derechos fundamentales o si bien resulta necesario promover ciertos ajustes constitucionales como consecuencia del impacto de la tecnología en nuestra sociedad.

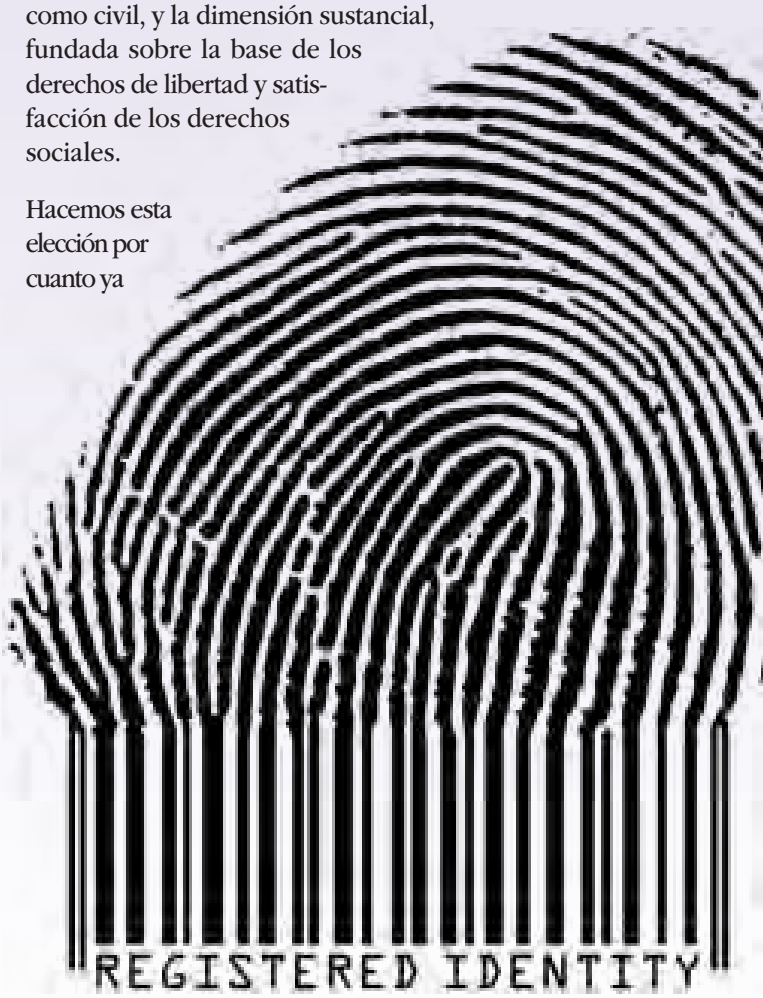
Lo anterior es especialmente relevante por dos razones. La primera, porque la constitución existe porque el sujeto titular del poder constituyente, que es el mismo pueblo soberano, la ha querido, tomando determinadas decisiones e imprimiendo por consecuencia, a esa misma constitución, determinados caracteres. Esas decisiones, a su vez, aparecen transcritas en la constitución, en el plano normativo, a través de grandes principios, que en general se refieren a los derechos de los ciudadanos en el plano civil, político y también social. El conjunto de estas normas, en fin, se concibe, a partir de la constitución alemana de Weimar de 1919 –y en el concreto desarrollo de las experiencia de las constituciones democráticas del siglo XX-, como un verdadero y auténtico núcleo fundamental de la constitución, derivado directamente del poder constituyente, de manera que representa el aspecto más esencial y en definitiva irrenunciable de cada constitución. Así, la constitución se dota de un contenido político que está directamente relacionado con la voluntad constituyente del pueblo soberano y que es un contenido democrático. La segunda, porque el significado político más importante de la democracia es la capacidad que poseen sus instituciones para proteger los derechos y libertades de los ciudadanos y, consecuentemente, de hacerse cargo de las mutaciones que ocurren en la Sociedad en aras de asegurar la vigencia de los mismos.

De este modo consideramos que no es ni debiera ser baladí la forma en que se enfrentan los ajustes necesarios de implementar en el país para ajustar el marco normativo a los cambios y exigencias impuestas por el advenimiento de la Sociedad de la Información y Comunicación, ya que por una parte ha de exigirse que las adecuaciones sean consistentes con la idiosincrasia y tradición constitucional; por otra, que siempre propenden a asegurar la máxima efectividad de los principios y valores constitucionalmente establecidos; y, finalmente, que se observen las exigencias de la regulación de los derechos fundamentales ".

En nuestra opinión, la vulneración de cualquiera de los aspectos señalados precedentemente nos debiera llevar a concluir que se está actuando de espalda a la constitución, o lo que es lo mismo, de espalda a los ciudadanos.

En este trabajo intentamos esbozar qué es lo que ocurre con la irrupción de las tecnologías de la información y comunicación, y especialmente Internet, en los derechos fundamentales –al alero del derecho nacional- como consecuencia del tratamiento de datos personales, y que es necesario hacer para garantizar que los derechos fundamentales se encuentren a buen resguardo y no menoscabados por este tipo de actividades. Para ello, nos abocaremos a analizar la problemática asociada al trinomio Democracia, Derechos Fundamentales y Protección de Datos Personales, para lo cual adheriremos al paradigma de democracia constitucional que nos propone Ferrajoli, en cuya virtud se le concibe a ésta como un sistema jurídico articulado sobre dos dimensiones: la dimensión formal, fundada en el ejercicio de los derechos de autonomía, tanto política como civil, y la dimensión sustancial, fundada sobre la base de los derechos de libertad y satisfacción de los derechos sociales.

Hacemos esta elección por cuanto ya



adentrados en el siglo XXI no nos parece tolerable el aceptar concepciones meramente procedimentales de la Democracia. Estimamos que un Estado no puede, o más bien no debe, ser considerado democrático por el sólo hecho de que en él las decisiones sean adoptadas por la regla de las mayorías, porque hayan elecciones periódicas, porque los ciudadanos puedan elegir y ser elegidos, porque exista una separación de los poderes, entre otras condiciones que caracterizan formalmente a la democracia. La democracia es mucho más que ello y sin duda el Estado está llamado a llenarla de contenido y a posibilitar que en ésta sus habitantes se desarrollen plenamente, para contribuir a materializar efectivamente el mandato constitucional en cuya virtud el Estado debe crear las condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su mayor realización espiritual y material posible, con pleno respecto a los derechos y garantías que la Constitución establece . De esta forma resulta necesario considerar que el Estado es un promotor del bienestar común de la sociedad toda, para lo cual debe colocar todo su andamiaje al servicio de las personas de manera de lograr los fines constitucionales declarados en dicho artículo. Para que ello sea posible, resulta indispensable que el Estado a través de sus órganos desarrolle sus funciones propias con estricta sujeción a lo dispuesto en la Constitución y las leyes, toda vez que por ser ellas la forma en que se materializa el debate democrático a través de las autoridades de elección popular, han de entenderse que son las manifestaciones de la soberanía y consecuentemente se trata de las reglas que un Estado democrático se da para guiar justamente la vida de los nacionales.

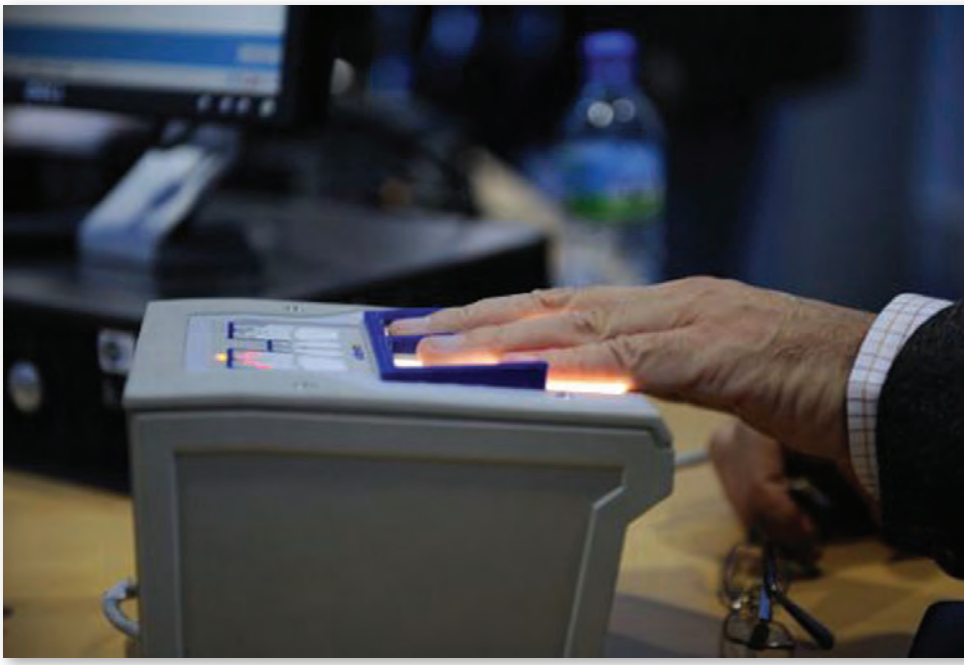
Es nuestro parecer que la democracia necesariamente tiene que ver con la forma en que los propios Estados se hacen cargo de satisfacer los derechos fundamentales que han quedado plasmados en las propias constituciones como valores jurídico morales que infunden la voluntad más elemental y primaria de los pueblos. Así, las constituciones no representan sólo el perfeccionamiento del Estado de derecho a través de la extensión del principio de legalidad a todos los poderes, incluso al legislativo. Constituyen también un programa político para el futuro: la imposición a todos los poderes de imperativos negativos y positivos como fuente para su legitimación, pero además –y diría sobre todo- para su deslegitimación. Constituyen, por así decirlo, utopías de derecho positivo que, a pesar de no ser realizables perfectamente, establecen de todos modos, en cuanto derecho sobre el derecho, las perspectivas de transformación del derecho mismo en dirección de la igualdad en los derechos fundamentales.

Así, la democracia supone la existencia de un binomio entre lo formal y lo sustancial. Formal porque está caracterizada por los llamados "universales de procedimiento" con el empleo de los cuales se pueden tomar decisiones de diferente contenido y sustancial porque se refiere predominantemente a ciertos contenidos a su vez inspirados en ideales característicos del pensamiento democrático. Según una vieja fórmula que considera a la democracia como gobierno del pueblo para el pueblo, la democracia formal es más que nada un gobierno del pueblo, la democracia sustancial es más que nada un gobierno para el pueblo.

Ahora bien, lo que resulta especialmente relevante a nuestro entender en la conceptualización de la democracia según este binomio, es el hecho de que la sustantividad de ésta viene dada especialmente por el hecho de que es ella la que condiciona la sustancia o significado de las decisiones que se adoptan según las reglas de procedimiento, vinculándolas, so pena de invalidez, al respeto de los derechos fundamentales y de los demás principios axiológicos establecidos en la constitución.

De esa manera, los derechos fundamentales se configuran como otros tantos vínculos sustanciales impuestos a la democracia política: vínculos negativos, generados por los derechos de libertad que ninguna mayoría puede violar; vínculos positivos, generados por los derechos sociales que ninguna mayoría puede dejar de satisfacer. De este modo la democracia comienza a llenarse de contenido, de sustancia, para

determinar su presencia y, por consiguiente, el accionar democrático obligará a que la regla de las mayorías tenga un doble límite impuesto, por una parte, por aquellas cosas que no se pueden decidir que, en palabras de Ferrajoli, importan la esfera de lo indecidible, para denominar al conjunto de principios que, en democracia, están sustraídos de la voluntad de las mayorías y, por la otra, aquellas respecto a las cuales les resulta obligatorio decidir. De este modo, por mucho que como consecuencia del deseo o la contingencia que un país viva en un momento determinado y se cuente con la mayoría necesaria para adoptar decisiones que vayan contra la sustancia de la constitución, no será posible que dichas decisiones se materialicen, de manera de mantener la democracia a buen recaudo y evitar que la dictadura de las mayorías se convierta en la principal amenaza del propio sistema democrático, de lo contrario una de sus principales virtudes terminaría convirtiéndose en el principal riesgo de la misma.



Ahora bien, el hecho de condicionar la democracia a que ella misma se haga cargo de cuestiones sustanciales que se encuentran reflejadas en las propias constituciones, como una suerte de programa ilustrado, supone necesariamente que el Derecho juega un rol que va mucho más allá de la simple legalidad de las actuaciones de los poderes públicos, ya que sujeta a todo el derecho al cumplimiento de ciertas exigencias morales que se condensan en los derechos fundamentales. De este modo, no resulta posible que los órganos del Estado se alejen, en el cumplimiento de sus mandatos constitucionales, de los lineamientos y/o directrices que la propia constitución infunde a todo el ordenamiento jurídico y al quehacer nacional, dando paso a la configuración, según el paradigma contractualista, al "Estado instrumento" para fines no suyos. Sin las garantías de los derechos fundamentales –desde el derecho a la vida a los derechos de libertad y a los derechos sociales- los fines externos o, si se quiere, los valores y, por así decir, la razón social de estos artificios que son el Estado y toda otra institución política.

Así, son los mismos modelos axiológicos del derecho positivo, y ya no sólo sus contenidos contingentes –su deber ser, y no sólo su ser- los que se encuentran incorporados al ordenamiento del Estado constitucional de derecho, como derecho sobre el derecho, en forma de vínculos y límites jurídicos a la producción jurídica. De aquí se desprende una innovación en la propia estructura de la legalidad, que es quizá la conquista más importante del derecho contemporáneo: la regulación jurídica del derecho positivo mismo, no sólo en cuanto a las formas de producción sino también por lo que se refiere a los contenidos producidos.

A partir de estas consideraciones el binomio Democracia y Derechos Fundamentales se arraiga con un vigor que a esta altura de la historia impide legítimamente concebir a una sin la presencia de la otra. Ello trae, igualmente, consigo que la amenaza o vulneración de los derechos fundamentales también arrastren el deterioro de la democracia.

Por otra parte hace algunos años ya se ha comenzado a oír hablar de la "contaminación de las libertades", término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías. En este caso particular la contaminación se produce como consecuencia de que las nuevas técnicas permiten utilizar y divulgar datos personales con excesiva facilidad, lo que convierte al ciudadano en un "hombre de vidrio" por el riesgo de que se construyan, con una sencillez abismante, perfiles de la personalidad a partir de los datos, lo que sin duda convierte su tratamiento en una pérdida del anonimato con el consecuente defecto jurídico constitucional que ello importa.

Una de las principales causas de esta ignominia, en nuestra opinión, es justamente la que se refiere al tratamiento de datos. Siendo ello así, es hora de completar el trinomio objeto de este estudio y analizar cómo y por qué la protección de datos se relaciona con la democracia y los derechos fundamentales.

El desarrollo tecnológico permite procesar grandes volúmenes de información prácticamente en tiempo real. Por su parte, la evolución de las telecomunicaciones también ha permitido que los resultados de ese procesamiento se comuniquen a cualquier lugar del mundo también en tiempo real. Ello, sumado al hecho de que en la época que estamos viviendo hay una necesidad desmesurada por el manejo de información, llegando a un punto en que el flujo y almacenamiento de ésta en muchos casos llega a realizarse sin tener claridad de la necesidad, pero sí sabiendo que en algún momento podría llegar a servir para algo. Sánchez Bravo nos sugiere que la información es el símbolo emblemático de la nueva era, y es ahí donde se halla el origen de múltiples conflictos.

Tal como la era industrial se basó en la producción a gran escala, la nueva época se funda en la comunicación y en la información a gran escala.

Parece consolidarse en los Estados modernos una situación en la que el uso múltiple e indiscriminado de datos personales se ve como una cuestión, no solamente necesaria, sino también como algo natural.

La prestación o suministro de cualquier servicio, tanto público como privado, lleva aparejada la imposición de suministrar toda una serie de datos que, en la mayoría de los casos, nada tiene que ver y son irrelevantes para la prestación del servicio de que se trate, sin embargo, a diario son requeridos y los ciudadanos los entregan sin siquiera cuestionarse el por qué de la solicitud.

Por otra parte suelen oírse voces que se levantan, en aras de la seguridad o del combate contra el terrorismo, las que señalan que el ciudadano que no tiene nada que esconder, no tiene nada que temer. Así, este ciudadano no tendría por qué estar preocupado de que el Estado recopilase toda la información posible que se refiriese a él. Sin embargo, Rodotà nos recuerda que el "hombre de vidrio" es una metáfora nazi, que refleja la idea de un Estado que puede adueñarse por entero de la vida de las personas, que frente a si no tiene ciudadanos sino súbditos. Las consecuencias de este planteamiento son dramáticas para las personas y destructivas para la democracia. En efecto, si una persona quiere preservar una esfera, aunque mínima de privacidad e intimidad, y desea que nadie conozca ciertas informaciones sobre sí mismo, se convierte, según el Estado, en "alguien que tiene algo que esconder" y, automáticamente, en sospechoso, en "enemigo del pueblo". Se trata de una lógica, típica de los regímenes totalitarios, y, por lo tanto, contraria a la democracia.

Así, queda en evidencia que los ciudadanos nos encontramos a diario sometidos a una constante entrega de datos personales, sin tener claridad para que son recolectados, cuando escasamente sabemos que están siendo recolectados; tampoco que es lo que se hará con dichos datos personales; no proyectamos las consecuencias que puede tener el tratamiento que se haga de los mismos; y como consecuencia de todo ello, ni siquiera sabemos dónde están nuestros datos.

Lo único que si podemos tener claro hasta este punto es el hecho de que se crean permanentemente, tanto en el mundo privado como en los organismos públicos, múltiples bases de datos que lo que hacen es almacenar información estructurada permitiendo relacionarla y consultarla fácilmente a través de procedimientos o rutinas de recuperación de dicha información. De este modo, por su intermedio se permite extraer las cualidades de una persona para así poder "perfilarla" y saber de antemano de ella. Así, se trata de información que pudiendo aparecer como inocua, irrelevante o incluso conveniente para quien ha de tomar una decisión, asoma indudablemente la amenaza de estigmatización de las personas por una situación coyuntural o bien por la calidad de la información de que se dispone en dichas bases de datos.

Ahora bien, parece bueno en este punto recordar que los estigmas permiten "categorizar" o "inferiorizar" a las personas y a los grupos a partir de sus atributos físicos, sociales o culturales. El estigma produce una identidad social basada en un descrédito proveniente de las diferentes categorías sociales, así como en supuestas fallas, defectos o desventajas. El estigma es un atributo profundamente desacreditador que estigmatiza a uno o puede confirmar la "normalidad" del otro.

Permitir y posibilitar la estigmatización de las personas sin duda se cierne sobre la democracia como una gran amenaza, toda vez que sus aspiraciones más profundas y auténticas se ven seriamente menoscabadas. Es por ello que estimamos resulta indispensable recordar que en un Estado democrático no puede existir justificación alguna que avale la afección ilegítima de los derechos fundamentales, razón por la cual los esfuerzos que se hagan por propender a la debida protección de los datos personales no han de tener límite.

Con la finalidad de dar respuesta a la problemática asociada a la contaminación de las libertades por el tratamiento de datos personales hace un par de décadas comenzó a surgir un nuevo derecho, el de la protección

de datos personales, conceptualizado como el amparo de los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales, con el fin de confeccionar información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad.

De esta forma, la protección de los datos personales deja de tener una correspondencia unívoca con el derecho a la vida privada y a la intimidad, para más bien pasar a configurarse como un derecho autónomo relacionado con la posibilidad de cada persona de tutelar la circulación de la información que le incumben. Así, la protección de datos se convierte en un elemento central de la forma en que el ciudadano vive y se relaciona en la Sociedad de la Información y Comunicación.

En tal sentido, el cambio de paradigma es sustantivo, sobre todo si se tiene en consideración el hecho de que en el derecho a la vida privada los mecanismos de tutela del mismo parten de la premisa de que la persona tiene derecho a excluir interferencias ajenas sobre su vida, así la tutela es estática y negativa. Sin embargo, en la protección de datos personales la cuestión es sustancialmente diferente, ya que su ejercicio se concreta en poderes de intervención, la tutela es dinámica y sigue a los datos durante su circulación. Adicionalmente, se confía no sólo a la iniciativa de las personas interesadas sino que requiere de la instalación de autoridades independientes que contribuyan a proteger a las personas, lo que implica una permanente y especifica responsabilidad pública.

Dicho ello, consideramos indispensable resaltar el hecho de que los derechos fundamentales deben crear y mantener las condiciones elementales para asegurar una vida en libertad y la dignidad humana. Ello sólo se consigue cuando la libertad de la vida en sociedad resulta garantizada en igual medida que la libertad individual. Ambas se encuentran inseparablemente unidas.

Así, estimamos que lo que resulta verdaderamente necesario en nuestro país es que surja la conciencia y convicción de parte de los responsables de asegurar la vigencia del Estado de Derecho de que la forma en que se tratan los datos personales representa una de las principales formas en que se vulneran actualmente los derechos fundamentales. De este modo, más que seguir esperando reformas normativas, es necesario comenzar a brindar la protección que las personas nos merecemos, porque lo que no es discutible es que la forma en que la información se trata puede afectar en contenido esencial de prácticamente todos los derechos garantizados en el catálogo constitucional.

**Raúl Arrieta Cortés, abogado, Magister (c) en Derecho Público y Diplomado en Derecho Administrativo: Derecho, Economía y Libre Competencia, ambos de la Universidad de Chile. Ejerce libremente la profesión y previamente fue asesor en temas de tecnologías de la información y comunicación para diferentes instituciones públicas y privadas, tanto nacionales como extranjeras y fue Jefe del Gabinete de la Subsecretaría de Telecomunicaciones, asi como, Jefe del Fondo de Desarrollo de las Telecomunicaciones. Es Consejero del Instituto Chileno de Derecho y Tecnologías.*

AGENDA DIGITAL: LAS NUEVAS NORMAS SOBRE TELECOMUNICACIONES BENEFICIAN A CIUDADANOS Y EMPRESAS DE TODA EUROPA

El 25 de mayo de 2011, los europeos disfrutaron de nuevos derechos y servicios en materia de teléfonos, móviles e Internet. Desde esa fecha se incorporaron a los ordenamientos jurídicos nacionales las nuevas normas de la UE en materia de telecomunicaciones para garantizar un sector de las telecomunicaciones más competitivo y mejores servicios a los clientes. Entre ellas se cuenta el derecho de los clientes a cambiar de operador de telecomunicaciones en un solo día sin cambiar de número de teléfono, el derecho a una mayor claridad sobre los servicios ofrecidos a los consumidores y una mejor protección de los datos personales en línea. Unos nuevos poderes de supervisión para la Comisión Europea y poderes reguladores para el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) facilitarán una mayor seguridad reglamentaria y ayudarán a los operadores a crecer en un mercado de las telecomunicaciones único y paneuropeo. La Comisión ha colaborado estrechamente con los Estados miembros a efectos de la rápida aplicación de esas normas de la UE y estudiará incoar procedimientos de infracción contra los Estados miembros que no las hayan incorporado a tiempo a su ordenamiento jurídico. La consolidación del mercado único de los servicios de telecomunicaciones es un objetivo crucial de la Agenda Digital para Europa (véase IP/10/581, MEMO/10/199 y MEMO/10/200).

Neelie Kroes, Vicepresidenta de la Comisión Europea responsable de la Agenda Digital, ha declarado lo siguiente: «Los ciudadanos y las empresas deben aprovechar plenamente las oportunidades que les brindan estas nuevas normas para conseguir unos servicios de telecomunicaciones más competitivos. Haré todo lo posible para ayudarles a hacerlo. Si estos derechos no se llevan a la práctica, tomaré las medidas necesarias para resolver esta situación frente a los Estados miembros y los operadores de telecomunicaciones».

Desde el 25 de mayo, las nuevas normas de la UE facilitan lo siguiente a los ciudadanos y las empresas:

Alto grado de protección a los consumidores y mayor capacidad de elección:

- Posibilidad de cambiar de operador de telefonía fija o móvil sin cambiar de número de teléfono en un solo día.
- Duración máxima de 24 meses de los nuevos contratos de los clientes y obligación de los operadores de ofrecer contratos de 12 meses, lo que permitirá a los clientes cambiar de operador más fácilmente si encuentran mejores condiciones.
- Información más clara sobre los servicios a los que se haya abonado el cliente. Los contratos celebrados con los consumidores deben informar sobre los niveles mínimos de calidad. En especial, los abonados a Internet deben recibir información sobre las técnicas de gestión del tráfico y su efecto en la calidad del servicio, así como sobre otras limitaciones (por ejemplo, límites a la anchura de banda, velocidad de conexión disponible o bloqueo o estrangulamiento del acceso a determinados servicios tales como el protocolo de transmisión de voz por Internet). Los contratos también deben informar de las indemnizaciones y reembolsos si no se alcanzan esos niveles mínimos (véase IP/11/486 y MEMO/11/319).

Mayor seguridad y privacidad en línea:

- Mayor protección contra las violaciones de los datos personales y el correo no deseado (spam),

notificaciones obligatorias de las violaciones de los datos personales.

- Mejor información y requisitos de consentimiento para guardar información o acceder a la misma en los aparatos de los usuarios, tales como los cookies no relacionados con el servicio al que se haya accedido (véase MEMO/11/320)

Una regulación más coherente en toda la UE

- Las autoridades reguladoras nacionales obtendrán una mayor independencia y podrán obligar a los operadores de telecomunicaciones con un peso significativo en el mercado a separar sus redes de telecomunicaciones de sus ramas de servicios para garantizar un acceso no discriminatorio para otros operadores, sin dividir necesariamente la propiedad y sin que exista la obligación de crear una empresa distinta.
- La Comisión, en cooperación con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), también ha recibido nuevas atribuciones de supervisión de las medidas correctoras en materia de competencia en los mercados de telecomunicaciones (el llamado «procedimiento del artículo 7»). En la práctica, si la Comisión considerara que un proyecto de medida correctora en materia de competencia notificada por una autoridad reguladora nacional crearía un obstáculo al mercado único de servicios de telecomunicaciones, puede proceder a una evaluación detallada y, previa consulta al ORECE, emitir una recomendación a la autoridad reguladora nacional a efectos de la modificación o retirada de la medida correctora prevista. Las autoridades reguladores nacionales deben tener en cuenta esas recomendaciones en la mayor medida posible (véase MEMO/11/321).

Otro elemento nuevo de esta normativa es el mejor acceso a los servicios de urgencia, incluido el 112, el número de llamada de urgencia único europeo.

La Recomendación de la Comisión por la que se indica a las autoridades reguladoras nacionales cómo regular el acceso competitivo de terceros a las redes de fibra ultrarrápidas, también conocidas por el nombre de redes de «acceso de nueva generación» o NGA (véase MEMO/10/424), se presentó recientemente basándose en los nuevos elementos de las normas actualizadas en materia de telecomunicaciones.

La Comisión está vigilando estrechamente la aplicación de las nuevas normas sobre telecomunicaciones por parte de los Estados miembros y recurrirá a todas sus atribuciones, aumentadas recientemente por el Tratado de Lisboa, para garantizar la incorporación plena y oportuna de las normas actualizadas sobre telecomunicaciones a los ordenamientos jurídicos nacionales. Para ayudar a los Estados miembros a aplicar las nuevas normas sobre las telecomunicaciones, la Comisión ha elaborado directrices sobre varios temas, tales como los cookies y el servicio universal.

Antecedentes

El Parlamento Europeo y el Consejo adoptaron oficialmente las normas de la UE revisadas en materia de redes y servicios de telecomunicaciones a finales de 2009 (MEMO/09/491). El Parlamento y el Consejo acordaron que las normas debían incorporarse a los ordenamientos jurídicos nacionales de los 27 Estados miembros a más tardar el 25 de mayo de 2011.

Las dos Directivas que entraron en vigor el 25 de mayo de 2011, la Directiva para la mejora de la legislación y la Directiva sobre los derechos de los ciudadanos, modificaron cinco Directivas vigentes distintas de la UE (la Directiva Marco, la Directiva de acceso, la Directiva de autorización, la Directiva de servicio universal y la Directiva sobre privacidad electrónica). También se ha adoptado un nuevo Reglamento por el que se crea el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), cuya sede se estableció oficialmente en Riga en mayo de 2010 (IP/10/641).

Página web de la Agenda Digital:

http://ec.europa.eu/information_society/digital-agenda/index_en.htm

Página web de Neelie Kroes: http://ec.europa.eu/commission_2010-2014/kroes/

Twitter de Neelie Kroes: http://twitter.com/neelie-kroeseu

La Protección de los Datos Personales en México

La inclusión del derecho fundamental en el marco jurídico mexicano

*Por Ángel José Trinidad Zaldívar

Abogado de la UNAM, especialidad en Finanzas Públicas y Maestría en Administración y Gobierno. México

En el año 2001, en pleno proceso de transición democrática, cuando la efervescencia política demandaba centrar la atención en temas complejos como la reforma del Estado con todas sus variantes: la política (¿nuevo régimen?); la económica (¿rompimiento del modelo neoliberal?), la social (¿nuevos esquemas de desarrollo?); se incorporó en el debate, aunque tímidamente y con escepticismo, el tema de los datos personales. Fue un diputado del Partido de la Revolución Democrática, quien presentó la primera iniciativa de Ley Federal de Protección de Datos Personales, el 6 de septiembre del 2001 . A pesar de que al día siguiente se turnó a la Comisión de Gobernación, nunca se emitió dictamen alguno. Un año después, un senador del Partido Revolucionario Institucional, presentó otra iniciativa que tampoco prosperó.

Dado que el derecho a la protección de los datos personales exigía atención y espacio propio, se le incluyó limitadamente en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) , que de sus 64 artículos, le dedicó apenas siete y algunas referencias o fracciones dispersas en otros.

No obstante que el tema de los datos personales ha estado presente en las agendas internacionales y ha sido ampliamente discutido desde hace cinco décadas, en México tuvieron que pasar nueve años -2001 al 2010-, nueve iniciativas de ley con sus respectivas mesas de análisis, foros y seminarios, así como tres reformas constitucionales, para que se aprobara la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

Las reformas constitucionales que le dieron cuerpo y consistencia al derecho a la protección de los datos personales ocurrieron en 2007 con modificaciones al artículo 6°, y en 2008 y 2009, con cambios a los artículos 73° y 16°, respectivamente. En la primera, del artículo 6°, se establecieron como principios y bases, que la información que se refiere a la vida privada y los datos personales estaría protegida en los términos y con las excepciones que fijen las leyes; así como que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendría acceso gratuito a sus datos personales o a su rectificación.

La segunda reforma, al artículo 73, facultó al Congreso para legislar en materia de protección de datos personales en posesión de particulares. Finalmente, la reforma al artículo 16 dio estructura y sustento constitucional al derecho a la protección de los datos personales, al establecer que toda persona tiene derecho a la protección de éstos, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

El logro de contar con una regulación específica en materia de datos personales implicó un proceso legislativo complejo del que destacan dos aspectos. El primero hace notar la resistencia y oposición de múltiples y encontrados actores e intereses a su reglamentación durante tanto tiempo, lo que revela

que dichos datos tienen un valor que no se había reconocido plenamente. El segundo aspecto refiere a la apatía de la ciudadanía que no exigió con firmeza, que sus datos personales se regularan a la brevedad, pues a diferencia de otros países, particularmente los europeos, existe poca consciencia entre los mexicanos sobre la importancia que sus datos tienen, los cuáles entregan a la menor provocación, sin reflexionar que al hacerlo son materialmente diseccionado por un sinnúmero de instituciones y empresas que extraen información, despojando a las personas en cierto sentido de su identidad.

La concepción de la protección de los datos personales en México y la tarea del IFAI como órgano garante.

El derecho a la protección de los datos personales, en sus primeros momentos, buscaba que el Estado se abstuviera de entrometerse en la vida personal de sus gobernados, es decir, tenía un sentido de limitación al poder público para proteger la esfera de intimidad de éstos últimos. En la actualidad, se ha dado un giro importante a esta idea, las personas pasan de ser receptores pasivos de un derecho consistente en la no intromisión del Estado en su vida privada (es decir, un sentido negativo), a ser actores que ejercen su derecho de control sobre su información, con la potestad de autodeterminación informativa, que significa el derecho a decidir a quién se le entregará un dato y qué puede hacer esa persona o institución con el mismo, lo que se traduce también en acciones de la autoridad (un sentido positivo) de establecer normas y mecanismos para proteger la vida privada y los datos personales.

Como se manifestó por el máximo tribunal español en la sentencia 254/1993, en la que se determinó que "no es posible aceptar que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión" , la regulación actual prevé que el Estado debe proveer lo necesario para hacer efectivo el derecho a la protección de los datos personales y contar con instituciones para ello. En el caso mexicano, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) es el encargado de garantizar este derecho.

En este sentido, el IFAI se encuentra ante el enorme reto de hacer efectivo este derecho con todo lo que implica: la difusión de su conocimiento entre la sociedad mexicana para fomentar su ejercicio y conciencia del cuidado de los datos, la promoción de su vigencia plena para garantizar la seguridad de los mismos, resolver los conflictos entre partes que se presenten, vigilar el cumplimiento de la norma, así como, construir un compromiso de corresponsabilidad con los sectores obligados, a fin de lograr altos niveles de acatamiento de la Ley.

Aún cuando México llega tarde al debate de la protección de los datos personales, el tema es de importancia mayúscula porque tiene implicaciones en diversos campos de la vida de las personas, particularmente en el ejercicio de la libertad, por un doble aspecto.

Por un lado, tal y como lo expusieron los legisladores en el dictamen de la LFPDPPP "gracias a algoritmos matemáticos y fórmulas aplicadas, dicha información [nuestros datos personales] se utiliza para predecir, con asombrosa exactitud, las decisiones que vamos a tomar. Es por ello importante establecer controles y límites al manejo indiscriminado de la información personal que generamos, ya que de lo contrario, nuestras conductas pueden ser manipuladas aún sin percatarnos de ello, coartando y vulnerando nuestras libertades". En este caso perderíamos nuestra libertad sin siquiera percibirlo. Con sutileza, malicia y tecnología, alguna institución o empresa puede inducirnos o empujarnos a decidir algo respecto de lo que no estamos convencidos. En cierto sentido leerán nuestro pensamiento, con los riesgos que esto conlleva. Puede sonar a ciencia ficción, pero es una realidad. El Tribunal Federal Alemán alertó al respecto al emitir una sentencia sobre la Ley del Censo en la que dispuso que "la proliferación de centros de datos ha permitido, gracias a los avances tecnológicos, producir una imagen total y pormenorizada de la persona respectiva –un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose el ciudadano en un hombre de cristal". Y como es sabido, el cristal es frágil. Ciudadanos frágiles hacen sociedades débiles, debilidad que es aprovechada por el gobierno para coartar la libertad.

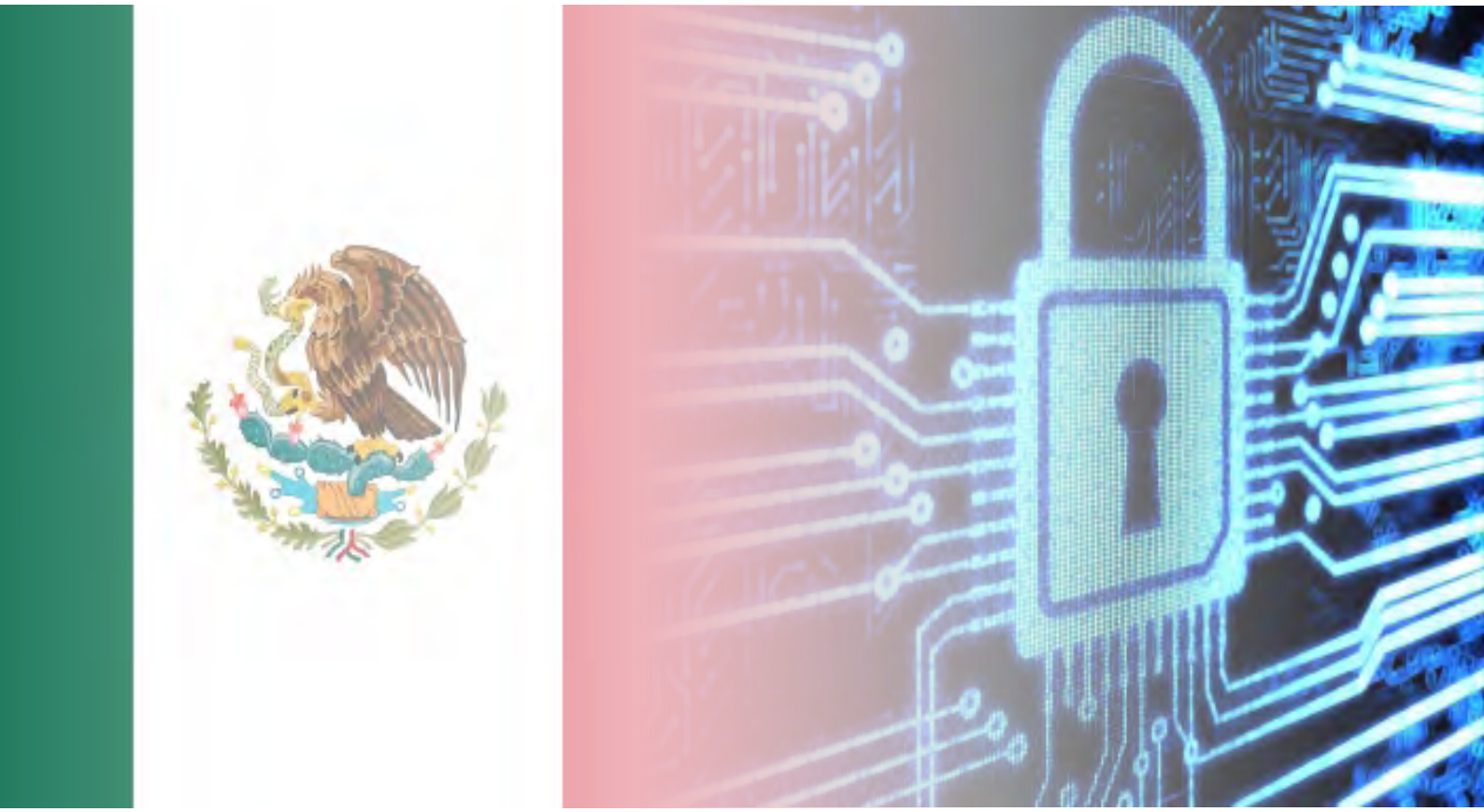
Por otra parte, el segundo mecanismo en el que un mal manejo de datos personales incide en nuestra libertad tiene que ver con la incertidumbre que genera el hecho de saber que ciertos datos pueden circular sin restricción alguna y, en consecuencia, los puede tener cualquier persona. En este sentido, "[aquél] que no pueda percibir con seguridad suficiente qué informaciones relativas a su persona son conocidas en determinado sectores de su entorno social y no pueda saber en consecuencia qué se sabe de él, puede coartar substancialmente su libertad de planificar o decidir. Por ejemplo, quien sepa de antemano que su participación en una re-

unión o iniciativa ciudadana va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo, renunciará presumiblemente a lo que supone un ejercicio de sus derechos fundamentales", es decir de su libertad de asociación. Mientras que en el primer caso –creación de perfiles de personalidad- nuestra disminución de libertad es pasiva o inconsciente, en este segundo caso la disminución es activa o consciente puesto que somos nosotros mismos los que limitamos o saboteamos nuestra libertad.

La LFPDPPP entrará en vigor al inicio de 2012. Ante este desafío, el IFAI tiene como tareas inmediatas: la emisión de los instrumentos normativos necesarios para asegurar su protección, así como, la implementación de procedimientos para el ejercicio de los derechos ARCO.

Cabe recordar que el derecho a la protección de los datos personales, que en México, en el año 2001, aparecía como una nimiedad frente a otros temas, en la actualidad adquiere una posición central en el debate nacional. Un sistema democrático no sólo no puede coartar libertades, sino que, por el contrario, tiene que protegerlas. Así, al considerar la necesidad de garantizar que la esfera más cercana y sensible al ciudadano, la de su información personal, sea resguardada de intromisiones que atenten contra lo más valioso de la persona humana, que es su dignidad y su libertad; la labor del IFAI, como órgano garante de este derecho, resultará crucial para la efectiva protección y ejercicio que se alcance del mismo en los próximos años. La responsabilidad asignada es grande, pero los resultados de la vigencia plena del derecho serán los de contar con una sociedad más democrática y con mayores garantías para sus ciudadanos.

**Ángel José Trinidad Zaldívar es Abogado de la UNAM, especialidad en Finanzas Públicas y Maestría en Administración y Gobierno. Durante cinco años fue Secretario Ejecutivo del IFAI (cargo que obtuvo a través de un concurso) y actualmente es Comisionado del mismo instituto. Entre otras actividades ha sido Coordinador de Enlace Interinstitucional de la Presidencia de la República, colaborador del Lic. Luis Donaldo Colosio, Candidato a la Presidencia. Academia: Profesor de Teoría General del Estado; Publicaciones: "La Transparencia y el Acceso a la Información como Política Pública y su Impacto en la Sociedad y el Gobierno"; "Descentralización, una Asignatura Pendiente", y "Breviario para la Reflexión", entre otros. Articulista del Periódico Milenio-Puebla*



URUGUAY: PROTECCIÓN DE DATOS PERSONALES

*Dr. Felipe Rotondo

Presidente del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, Uruguay

1. Marco normativo:

Ley 18.331 de 11-VIII-2008 y decreto 414/009: reconoce la protección como derecho humano, fundamental.

2. Ámbitos subjetivo, objetivo y territorial.

A. Abarca toda información, numérica, alfabética, gráfica, acústica, etc.

   Atañe a datos personales en fichas, Cd, discos duros, etc., organizados; excluye bases de personas físicas en actividades personales o domésticas.

B. Responsable de la base, propietario o quien decide sobre uso del tratamiento: persona física o jurídica, privada o pública.

C. Titular de datos: toda persona física determinada o determinable; la protección se extiende a la persona jurídica en cuanto corresponda.

   Hay normas propias de personas físicas, como la vista en 2.A o el registro de sus datos comerciales (por 5 años prorrogables por una sola vez).

D. Las normas se aplican si el tratamiento se hace por responsable establecido en el país o usa medios en él situados.

3. Principios.

A. Respeto al orden jurídico, derechos humanos y moralidad pública; registro de bases.

B. Veracidad de datos, obtenidos lealmente.

C. Finalidad específica, coherencia en tratamiento de datos, a eliminar si no son pertinentes.

D. Consentimiento informado previo, documentado de modo sencillo, gratuito; para comunicación entre bases, se exige, además, interés legítimo de emisor y destinatario. El interesado debe poder saber fin de la base, responsable, etc.; su silencio en 10 días hábiles, implica rechazo.

   Se exceptúa del consentimiento datos de fuentes públicas, los necesarios para cumplir deberes legales y listados con ciertos datos .

E. Seguridad: condiciones técnicas que aseguren confidencialidad y ejercicio de derechos; si se viola, debe comunicarse a interesados.

F. Reserva de datos: uso para el fin de su recolección en operaciones del giro del responsable, sin difusión. El secreto profesional rige a quien trabaje para aquel, en toda relación jurídica.

G. Responsabilidad hecha valer ante la administración o ante el Juez.

4. Derechos del titular a:

A. Ser informado debidamente y antes de la recolección sobre fin, destinatarios, responsable, obligación o no de responder, derechos, etc.

B. Acceso gratuito a toda la información que le concierne, sin formalidades, en principio cada 6 meses. Debe dársela clara, inteligible en 5 días hábiles, por el medio que indique.

C. La rectificación, actualización, inclusión, supresión sin cargo, en 5 días hábiles; en su caso informarse razones de negativa.

D. Dar su consentimiento para comunicación o cesión de datos; excepciones estrictas, en base a ley.

5. Datos sensibles, de origen racial, étnico, preferencia política, creencia religiosa, afiliación sindical, salud, vida sexual.

Su tratamiento exige consentimiento escrito; no hay obligación de darlos y existe prohibición de principio de bases en la materia. Su recolección cabe en base a ley; el uso requiere proceso de disociación, así para estadísticas.

6. Unidad Reguladora y de Control de Datos Personales.

A. Institucionalidad.

Órgano estatal, desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información-Presidencia de la República, con atribuciones legales propias y autonomía técnica. En sus tareas los miembros no reciben órdenes ni instrucciones.

B. Autoridades: a) Consejo Ejecutivo de 3 miembros, b) Consejo Consultivo de 5 miembros.

C. Competencias: *Asesorar; recomendar políticas en tratamiento, seguridad, etc. de datos. *Dictar normas. *Registrar bases y códigos de práctica profesional. *Autorizar transferencias internacionales. *Controlar observancia de normas. *Sancionar a responsables o encargados de tratamiento.

7. Acción jurisdiccional de habeas data.

A. Legitimación y objeto: titular al que se niegue acceso, rectificación, inclusión o supresión de datos en 5 días hábiles o no se le justifique negativa.

B. Proceso sumario: audiencia pública en 3 días, en la que se produce prueba, alegatos y sentencia, ésta prorrogable por breve plazo, excepcionalmente hasta 3 días. La sentencia fija conducta a cumplir en plazo de hasta 15 días corridos; la apelación no suspende el amparo y el tribunal superior tiene 4 días para decidir.

8. Aspectos a destacar:

A. El país transita el proceso de adecuación a estándares de recibo a nivel internacional; el Grupo del art. 29 de la Directiva 95/46/CE informó favorablemente al respecto el 12-X-2010.

B. La Unidad tuvo la iniciativa de tramitar ante el Consejo de Europa la adhesión al Convenio 108 sobre protección de personas respecto al trato automatizado de datos personales y a su Protocolo sobre autoridades de control y flujos transfronterizos de datos.

**El Doctor Felipe Rotondo es Integrante y Presidente del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, Uruguay; Profesor de Derecho Constitucional y Administrativo*

Resolución de Madrid

31 Conferencia Internacional de Protección de Datos

Madrid, Noviembre de 2009

Estándares Internacionales sobre Protección de Datos Personales y Privacidad

Los responsables de Protección de Datos de 83 países de todo el mundo acordaron, por unanimidad en Madrid, en Noviembre de 2009, un conjunto de estándares internacionales para proteger la privacidad de las personas y el manejo que de sus datos personales hacen las empresas y organismos públicos. El documento fue aprobado al término de la 31 Conferencia Internacional de Protección de Datos y Privacidad, que reunió a más de mil expertos.

LA 31 CONFERENCIA:

Sin dejar de lado la influencia de las nuevas tecnologías, uno de los temas capitales sobre los que giró la conferencia fue la educación de los menores, un reto estratégico en el mundo digital hacia el que evolucionamos a grandes pasos. La protección de datos como elemento estratégico en el ámbito empresarial y las transferencias internacionales de datos en un mundo globalizado fueron otros de los ejes de la conferencia. Fueron también objeto de discusión y análisis, nuevos modelos publicitarios y nuevas técnicas comerciales, y su incidencia en el ámbito de la protección de datos.

El binomio **seguridad - privacidad** fue otras de las cuestiones que los expertos reunidos en Madrid estudiaron a fondo, especialmente, en relación a aquellos sistemas que plantean mayor controversia como la proliferación de dispositivos de video- vigilancia, o los que utilizan a modo de soporte el propio cuerpo humano, como la biometría, y cuyo uso se extiende en terrenos cada vez más cotidianos y diversos.

LA RESOLUCIÓN DE MADRID

La Resolución tiene un doble objetivo: por un lado, lograr el reconocimiento de la protección de datos y de la privacidad como derechos fundamentales, con independencia de la nacionalidad o residencia de las personas; por otro, constatar las dificultades que generan, tanto para el ciudadano como para las empresas, las diferencias persistentes entre los marcos jurídicos de los diferentes países, en especial debido al hecho de que muchos Estados no han aprobado todavía leyes adecuadas en la materia.

Las autoridades de protección de datos están convencidas de que el reconocimiento de estos derechos pasa por la adopción de un **instrumento legislativo, universal y vinculante, que consagre el respeto a la privacidad a nivel mundial.**

Es por ello que fue elaborada una propuesta conjunta, encargada a la Agencia Española de Protección de Datos, transformada en la **Resolución de Madrid**, para que sirva como base para la elaboración de un futuro **Convenio internacional**, y que entretanto se emplee como **instrumento de cooperación y comprensión entre los pueblos**.

DECISIÓN DE LA 31 CONFERENCIA

La Conferencia resuelve:

1. Acoge con satisfacción la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter Personal. La Propuesta Conjunta demuestra la viabilidad de tales estándares, como un nuevo paso hacia la elaboración, en el momento oportuno, de un instrumento internacional vinculante.
2. Afirma que la Propuesta Conjunta ofrece un conjunto de principios, derechos, obligaciones y procedimientos que cualquier sistema jurídico de protección de datos y privacidad debe esforzarse por alcanzar. De este modo, el tratamiento de datos personales en el sector público y privado se llevaría a cabo, a través de un enfoque más uniforme a nivel internacional:
   a. de manera leal, lícita, y proporcionada en relación con finalidades determinadas, explícitas y legítimas.
   b. sobre la base de políticas transparentes, informando adecuadamente a los interesados y sin ninguna discriminación arbitraria en su contra.
   c. garantizando la exactitud, la confidencialidad y la seguridad de los datos, así como la legitimidad del tratamiento, y los derechos de los afectados a acceder, rectificar y cancelar los datos, así como a oponerse a un determinado tratamiento.
   d. aplicando el principio de responsabilidad, incluyendo la responsabilidad por daños, incluso si las operaciones de tratamiento se llevan a cabo por prestadores de servicios que actúen por cuenta del responsable.
   e. ofreciendo garantías más adecuadas cuando los datos son sensibles.
   f. garantizando que los datos personales transferidos internacionalmente se benefician del nivel de protección previsto en el mencionado conjunto de estándares.
   g. sometiendo el tratamiento a la vigilancia de autoridades de supervisión, independientes e imparciales, con poderes y recursos adecuados, y sometidas a un deber de cooperación entre sí.
   h. en un marco nuevo y moderno de medidas proactivas, orientadas en particular a prevenir y detectar infracciones y basadas en la designación de oficiales de privacidad, así como en auditorias eficaces y en evaluaciones de impacto de privacidad.

3. Instar a las Autoridades de Protección de Datos y Privacidad acreditadas ante la Conferencia Internacional a dar la máxima difusión a la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter Personal.

4. Encomendar a las Autoridades organizadoras de la 31ª y 32ª Conferencias Internacionales la coordinación de un Grupo de Contacto, integrado por las Autoridades de Protección de Datos y Privacidad que así lo deseen, que se encargará de:

   a. la promoción y difusión de Propuesta Conjunta entre entidades privadas, expertos y organismos públicos nacionales e internacionales como base para un futuro trabajo para la elaboración de un Convenio universal vinculante, y en particular entre las instituciones y organizaciones mencionadas en la Declaración de Montreux; y

   b. explorar e informar sobre otras formas en que la propuesta conjunta podría utilizarse como base para el desarrollo de la comprensión y la cooperación internacionales sobre protección de datos y la privacidad, particularmente en el contexto de permitir las transferencias internacionales de datos personales, que tendrán lugar de un modo que proteja los derechos y libertades de los individuos.

5. Solicitar al Grupo de Contacto:

   a. coordinar su labor con el Grupo director sobre la representación en reuniones de organizaciones internacionales,

   b. informar de cualquier avance relevante a la 32ª Conferencia Internacional, para garantizar una atención continua al tema de la presente resolución.

TEXTO DE LA PROPUESTA CONJUNTA APROBADA POR LA RESOLUCIÓN DE MADRID

Principio de lealtad y legalidad

1. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos. 2. En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados.

Principio de finalidad

1. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable.

2. La persona responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.

Principio de proporcionalidad

1. El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas en el apartado anterior. 2. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.

Principio de calidad

1. La persona responsable deberá asegurar en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados. 2. La persona responsable deberá limitar el período de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos.

Principio de Transparencia

1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.

2. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

3. Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.

4. Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.

5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos

Principio de Responsabilidad

La persona responsable deberá: a. adoptar las medidas necesarias para cumplir con los principios y obligaciones estable-

cidos en el presente Documento y en la legislación nacional aplicable, y b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23.

DERECHOS DEL INTERESADO

Derecho de Acceso

1. El interesado tendrá derecho a recabar de la persona responsable, cuando así lo solicite, información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos.
2. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo.
3. La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo.

Derecho de Rectificación y cancelación

1. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o cancelación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.
2. Cuando proceda, la persona responsable rectificará o cancelará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.
3. La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable o, en su caso, por las relaciones contractuales entre la persona responsable y el interesado.

Derecho de oposición

1. El interesado podrá oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal.
2. No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable.
3. Cualquier interesado podrá oponerse, igualmente, a aquellas decisiones que conlleven efectos jurídicos basadas únicamente en un tratamiento automatizado de datos de carácter personal, excepto cuando la decisión hubiese sido expresamente solicitada por el interesado o sea precisa para el establecimiento, mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el propio interesado. En este último caso, el interesado debe tener la posibilidad de hacer valer su punto de vista, a fin de defender su derecho o interés.

Ejercicio de estos derechos

1. Los derechos previstos en los apartados 16 a 18 del presente Documento podrán ser ejercidos: a. Directamente por el interesado, que deberá acreditar adecuadamente su identidad ante la persona responsable. b. Por medio de representante, que deberá acreditar adecuadamente tal condición ante la persona responsable.
2. La persona responsable deberá implementar procedimientos que permitan a los interesados ejercer los derechos previstos en los apartados 16 a 18 del presente documento de forma sencilla, ágil y eficaz, y que no conlleven demoras o costes indebidos, ni ingreso alguno para la persona responsable.
3. Cuando la persona responsable aprecie que, de acuerdo con la legislación nacional aplicable, no procede el ejercicio de los derechos previstos en la presente Parte, informará cumplidamente al interesado de los motivos que concurran en su apreciación.

PROPONENTES DE LA RESOLUCIÓN SOBRE ESTÁNDARES INTERNACIONALES DE PRIVACIDAD

Agencia Española de Protección de Datos
Comisario Federal de Protección de Datos y la transparencia (Suiza)
Supervisor Europeo de Protección de Datos
Comisión Nacional de la Informática y de las Libertades (Francia)
Comisario de Protección de Datos de Irlanda
Oficina del Comisario de Privacidad de Canadá
Oficina para la Protección de los Datos Personales (República Checa)
Comisario Federal para la Protección de Datos (Alemania)
Garante para la Protección de Datos Personales (Italia)
Autoridad Holandesa de Protección de Datos
Comisario de Privacidad de Nueva Zelanda
Oficina del Comisario de Información (Reino Unido)

Coproponentes:

Agencia de Protección de Datos de Andorra
Agencia Catalana de Protección de Datos
Agencia de Protección de Datos de la Comunidad de Madrid
Agencia Vasca de Protección de Datos
Oficina del Supervisor de Protección de Datos la Isla de Man
Inspección de Protección de Datos de Estonia
Inspección Estatal de Protección de Datos (Lituania)
Comisario para la Protección de Datos de Berlín (Alemania)
Comisario de Protección de Datos de Schleswig-Holstein (Alemania)
Director Nacional de Protección de Datos Personales (Argentina)
Comisario de Protección de Datos (Malta)
Comisión de la Informática y las Libertades (Burkina-Faso)
Comisario de Protección de Datos Personales (Chipre)
Defensor de la Protección de Datos (Finlandia)
Comisario de Información (Eslovenia
Autoridad Griega de Protección de Datos

Nacimiento de la normativa actual, un largo camino de encuentro entre los países de Europa

El largo proceso que ha realizado la Unión Europea respecto de una legislación que regule la Protección de Datos en la red, se ve reflejada extensamente en las innumerables reuniones y acuerdos entre los países desde varias décadas atrás. Un importante avance representó el artículo 1 del Convenio firmado el 14 de diciembre de 1960 en París y que entró en vigor el 30 de septiembre de 1961, de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y que tuvo por objetivo promover políticas dirigidas a conseguir la mayor expansión de la economía, el empleo y una progresión del nivel de vida en los países miembros, manteniendo su estabilidad financiera y contribuyendo al desarrollo de la economía mundial. Además de aportar a una sana expansión económica entre los países miembros, así como en los países no miembros, en vías de desarrollo económico. Y, por último, contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, conforme con las obligaciones internacionales.

En este sentido la recomendación del consejo relativa a las directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales de fecha 23 de septiembre de 1980, afirmó que EL CONSEJO, considerando los artículos 1(c) y 5(b) del Convenio sobre la Organización para la Cooperación y el Desarrollo Económicos del 14 de diciembre de 1860, reconoció que, aunque las leyes y políticas nacionales pueden diferir, los países miembros tienen un interés común en proteger la privacidad y las libertades individuales, así como en reconciliar los valores fundamentales pero contradictorios como la privacidad y el libre flujo de información. El Consejo en esta ocasión recomendó 4 ideas poderosas: Que los Países Miembros tengan en cuenta en su legislación interna los principios relativos a la protección de la privacidad y las libertades individuales establecidos en las Directrices contenidas en el Anexo a esta Recomendación y que forma parte del mismo; Que los Países Miembros se esfuercen por eliminar o evitar que aparezcan, en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales; Que los Países Miembros colaboren en la implantación de las Directrices establecidas en el Anexo; y que los Estados Miembros convengan cuanto antes en los procedimientos específicos de consulta y cooperación para la aplicación de esas Directrices.

Memoria explicativa

Cabe señalar que uno de los rasgos de los países miembros de la OCDE en la pasada década ha sido la elaboración de leyes para la protección de la privacidad. Estas leyes han mostrado una tendencia a asumir diferentes formas según los países, y en muchos de ellos aún se están elaborando. La disparidad de la legislación puede crear obstáculos al libre flujo de información entre países.

Dichos flujos se han incrementado de gran manera en los últimos años y están abocados a seguir aumentando debido a la introducción de nueva tecnología informática y de la comunicación. La OCDE, que lleva años con una actitud activa en este campo, decidió ocuparse del problema de separarse de la legislación propia de cada país y en 1976 encargó a un Grupo de Expertos que elaborara Directrices sobre las normas básicas que han de regir el flujo transfronterizo y la protección de los datos personales y la privacidad, para así facilitar la armonización de la legislación nacional. El grupo ya ha terminado el trabajo.

Las Directrices son amplias y reflejan el debate y el trabajo legislativo que se ha estado haciendo durante varios años en los países miembros. El Grupo de Expertos que preparó las Directrices ha considerado fundamental el emitir una Memoria Explicativa que acompañe al trabajo. Su objeto es explicar y elaborar las Directrices y los problemas básicos de protección de la privacidad y las libertades individuales. Llama la atención sobre temas clave que han surgido en las discusiones de las Directrices y explica las razones que llevaron a la elección de soluciones concretas.

La Primera Parte de la Memoria da una información básica general sobre el área de interés tal y como la conciben los países miembros. Explica la necesidad de la actuación internacional y resume el trabajo realizado hasta el momento por la OCDE y algunos otros organismos internacionales. Concluye con una lista de los principales problemas con los que el Grupo de Expertos se encontró durante el trabajo.

La Segunda Parte se divide en dos secciones. La primera contiene comentarios sobre ciertos rasgos generales de las Directrices y la segunda comentarios detallados sobre apartados concretos.

Esta Memoria es un documento informativo, preparado para explicar y describir en general el trabajo del Grupo de Expertos. Queda subordinada a las Directrices y no puede variar el significado de las Directrices, pero se facilita para ayudar a una mejor interpretación y aplicación de las mismas.

(Para mayores antecedentes sobre Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, acudir a: http://www.oecd.org/dataoecd/16/51/15590267.pdf)

TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES

De igual forma en el Convenio Nº 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, los Estados Partes,

miembros del Consejo de Europa, considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales y considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados. Reconoce la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos. Convino esta normativa, entre otras cosas, garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Para mayores antecedentes sobre el Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, acudir a: http://www.apd.cat/media/246.pdf

UN MUNDO SIN FRONTERAS

Asimismo en la 31º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, realizada en Madrid en Noviembre de 2009, se acordó una Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales. La Conferencia consideró que el derecho a la protección de datos y a la privacidad es un derecho fundamental de las personas, con independencia de su nacionalidad o residencia. Que con el crecimiento de la sociedad de la información, el derecho a la protección de datos y a la privacidad es una condición indispensable en una sociedad democrática y liberal para garantizar el respeto de los derechos humanos, así como la libre circulación de información en una economía de mercado. El reconocimiento de estos derechos pasa por la adopción de un instrumento legislativo universal y vinculante, que haga uso, consagre y complemente los principios comunes de protección de datos y de respeto a la privacidad enunciados en los diferentes instrumentos existentes, además de reforzar la cooperación internacional entre autoridades de protección de datos. El desarrollo de reglas internacionales que garanticen, de un modo uniforme, el respeto a la protección de datos y a la privacidad, resulta prioritario. La Conferencia mandata la creación de un Grupo de Trabajo, bajo coordinación de la Autoridad organizadora de la 31ª Conferencia Internacional y con la participación de las Autoridades de protección de datos interesadas en ello, con el objetivo de elaborar una Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal

Para mayores antecedentes sobre la 31º Conferencia Internacional de autoridades de protección de datos y privacidad. Hacia estándares internacionales sobre

privacidad, resolución 108º del Consejo de Europa, acudir a: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

PROTECCIÓN DE LAS LIBERTADES Y DERECHOS

Según expresa la Directiva 95/46/CE del Parlamento Europeo y del Consejo, con fecha 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de Datos Personales y a la Libre Circulación de estos datos, expresó en sus disposiciones generales que los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. De esta forma, los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre ellos por motivos relacionados con la protección garantizada en virtud del apartado 1, entre otras consideraciones generales.

Para mayores antecedentes sobre la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, acudir a: http://www.cert.fnmt.es/legsoporte/Directiva%2095_46_CE%20Datos%20CaracterPersonal.pdf

GRUPO DE TRABAJO

El Grupo de Trabajo del Artículo 29 (GT 29) fue creado por la Directiva 95/46/CE, y tiene carácter de órgano consultivo independiente, integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997.

Cabe destacar que el GT 29 se reúne en plenarios con una periodicidad bimensual y se organiza en diversos subgrupos de trabajo para analizar todas aquellas cuestiones que inciden, o pueden llegar a afectar, a la protección de datos personales. El GT 29 emite sus observaciones a través de Decisiones, Dictámenes, Documentos de Trabajo, Informes o Recomendaciones. El GT 29 aprueba un informe anual con las novedades de cada Estado miembro en materia de protección de datos.

ESTÁNDARES INTERNACIONALES

La "Propuesta Conjunta de Estándares Internacionales de Protección de Datos y Privacidad" es la apuesta de las autoridades de supervisión para proteger la privacidad en un mundo sin fronteras, en el que reforzar el carácter universal de estos derechos se hace imprescindible.

El documento tiene un doble objetivo: por un lado, lograr el reconocimiento de la protección de datos y de la privacidad como derechos fundamentales, con independencia de la nacionalidad o residencia de las personas; por otro, constatar las dificultades que generan, tanto para el ciudadano como para las empresas, las diferencias persistentes entre los marcos jurídicos de los diferentes países, en especial debido al hecho de que muchos Estados no han aprobado todavía leyes adecuadas en la materia.

Las autoridades de protección de datos están convencidas de que el reconocimiento de estos derechos pasa por la adopción de un instrumento legislativo, universal y vinculante, que consagre el respeto a la privacidad a nivel mundial. Es por ello que se elaboró esta propuesta conjunta, con la esperanza y el deseo de que sirva como base para los trabajos de elaboración de un futuro Convenio internacional, y que entretanto se emplee como instrumento de cooperación y comprensión entre los pueblos.

Toda la información sobre este Grupo de Trabajo del Artículo 29 puede ser consultada en https://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php

La discusión legislativa en Chile sobre el tratamiento de los datos personales: un vistazo a los últimos años

*Por Danielle Zaror Miralles

Asesora Ministerio de Economía, Fomento y Turismo. Chile

1. Consideraciones Preliminares

La incorporación de Chile a la Organización para la Cooperación y el Desarrollo Económico (OCDE) reveló un diagnóstico que puso de manifiesto la necesidad de incluir en nuestra legislación, con relativa urgencia, algunos principios en materia de protección de datos, muchos de los cuales se encuentran ausentes de nuestra regulación o recogidos de manera parcial o imprecisa.

Desde el año 1999, año de publicación de la Ley N° 19.628 sobre Protección de la Vida Privada, han sido alrededor de 60 las mociones parlamentarias y mensajes presidenciales, los que han pretendido regular materias tales como el tratamiento de los datos personales; la recogida, uso y divulgación de la información financiera y predictores de riesgo; la regulación de la videovigilancia; la incorporación de mecanismos que permitan salvaguardar la protección de la privacidad en Internet; el spam, el control del marketing directo; entre muchas otras materias. Sin embargo, pese a la fertilidad de ideas y buenas intenciones, no ha existido en todos estos años una voluntad política desde el poder ejecutivo para promover decididamente actualizaciones e innovaciones en esta materia.

Quizás el proceso de incorporación a la OCDE ha sido el paso más concreto en este sentido que han dado las autoridades políticas desde el año 1999, año de la publicación de la Ley Nº 19.628 sobre Protección a la vida Privada. En efecto, desde que comenzó el proceso de ingreso de nuestro país, los temas vinculados a la protección de la vida privada y datos personales han retomado un interesante impulso desde la perspectiva académica y en menor medida (o de manera fluctuante) en la agenda legislativa chilena.

2. Diagnóstico Chileno

Al listar aquellas materias respecto de las cuales Chile debía mejorar estándares para acceder al grupo de las mejores prácticas de países desarrollados, se evidenció que, si bien Chile fue pionero en América Latina en regular esta materia, habían ciertos aspectos de esa regulación que resultaban insuficientes a la luz de las modernas realidades de los países integrantes de la OCDE, se hacía necesario entonces determinar cuál es el estándar de protección adecuada al que debía atenderse luego de este diagnóstico. Entre los principales aspectos donde era necesario avanzar se identificaba como requerimiento de primera necesidad "contar con los mecanismos y estructuras judiciales y/o administrativas que aseguren esos derechos que van a ser debidamente amparados" ; para ello es imprescindible la creación de una autoridad de control independiente o autónoma que permitiera de manera razonable a los ciudadanos acceder a la protección de sus derechos cuando fueran estos conculcados. La creación de esta autoridad trae como consecuencias:

a) La creación de un procedimiento de reclamo del titular de los datos ante el responsable de la base de datos.

b) La creación de un procedimiento administrativo, en caso que el anterior no diera debida satisfacción a la ciudadanía afectada.

c) La instauración de un catalogo de sanciones en caso de infracciones a la ley, entre otros aspectos de naturaleza orgánica.

Pero la actualización no era sólo adjetiva sino también sustantiva puesto que exigía reconocer y reforzar algunos derechos que no estaban debidamente recogidos en la legislación vigente.

Adicionalmente las condiciones de incorporación hacían necesaria que en la adecuación se consideraran estándares para la transferencia internacional, segura, de datos personales.

Este esfuerzo obviamente era una invitación para completar y ajustar todos esos aspectos que si bien no eran parte de las condiciones esenciales de acceso a la OCDE (si exigibles a mediano plazo), permitían aprovechar esta oportunidad para hacer una reforma completa, esto es, una evolución que permitiera regular de manera moderna y al más alto estándar aspectos tales como el uso de los datos de las personas por organismos públicos y privados, de la información comercial de las personas, la transferencia transfronteriza, el envío de spam, entre otros temas.

Sin embargo, la regulación sobre el uso de la información financiera ha tendido históricamente a distraer el debate principal sobre la protección de datos, concentrando la discusión entre los generadores de la información, los distribuidores y entre algunas autoridades acerca de la conveniencia de consolidar o no información patrimonial o positiva con información morosa o negativa.

Como hemos indicado, un porcentaje no despreciable de las decenas de iniciativas parlamentarias buscan regular, de manera antagónica en algunos casos, el tratamiento de información financiera, pero lo cierto es que ninguna iniciativa aborda los aspectos previos, marcos o fundamentales que son necesarios para comenzar cualquier discusión acerca de la protección y tratamiento lícito de los datos personales.

3. Esfuerzos Legislativos desde el año 2008 a la fecha

En este punto analizaremos los proyectos de ley que desde el año 2008 han sido enviados desde el poder ejecutivo para su tramitación legislativa.

I. Proyecto de Ley que modifica la Ley N 19.628 sobre Protección a la Vida Privada y la Ley N 20.285 sobre Acceso a la Información Pública.

Este mensaje presidencial fue el primer paso concreto del proceso de incorporación de Chile a la OCDE en materia de protección de datos personales.

Entre los principales aspectos a destacar de este proyecto de ley podemos mencionar los que siguen:

a) Reconocimiento explícito de derechos: En la regulación nacional no existe una declaración del legislador que permita entender que cada persona es dueña de sus datos personales, por lo tanto, dicha parte de la propuesta busca consagrar el derecho de las personas de controlar aquellos datos que le conciernen a través del reconocimiento del derecho de acceso, rectificación, cancelación y oposición al tratamiento indebido de ellos.

b) Se amplía el margen de sujetos protegidos. Este proyecto de ley extiende su protección a las personas jurídicas. Sin embargo, no compartimos esta iniciativa por cuanto dichos entes no poseen vida privada, que es la garantía constitucional en virtud de la cual se construye, en Chile, la protección de los datos personales. Distinto es el caso de la extensión de la regulación relativa a información financiera sobre dichas personas, por cuanto ahí lo que importa es la reputación de la entidad, cuestión que se encuentra prote-

gida por una garantía distinta y sí aplicable a ellas como lo es el derecho a la honra.

c) Establecimiento de una autoridad de control. Encargo definido para el recientemente creado Consejo Para la Transparencia, creado por la ley N° 20.285. Dentro de las funciones más importantes se le entrega la mantención de un Registro Único Nacional de las Bases de Datos; la facultad de inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley; se le confiere una potestad normativa, de ahí que se le faculte para dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimidad de un tratamiento de datos; se le faculta para conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos; ejercer el control y adoptar las autorizaciones que procedan para las transferencias internacionales de datos, entre otras funciones de menor entidad.

d) Fortalecimiento de derechos de información. Se busca fortalecer el derecho de los titulares de datos a conocer la finalidad con la que están siendo recogidos sus datos y quiénes son los destinatarios de ellos. Asimismo su derecho a oponerse a dicha recolección o a revocar en caso que se haya otorgado, entre otros.

e) Autorización debe ser expresa. Se pone énfasis en la forma como debe ser prestado el consentimiento del titular para efectuar tratamiento de datos personales, el cual debe efectuarse expresamente y por escrito. Se consagra además un sistema de presunciones de consentimiento, esto es, aún cuando no se requiera la autorización del titular, deberá informarse a éste de la existencia del tratamiento y de su derecho a oponerse. Se prescinde del consentimiento, mas no del conocimiento del titular.

f) Se regula el flujo transfronterizo de datos. Se establece que debe ser la autoridad de control quien autorice un intercambio internacional de datos respecto de aquellos países que no cumplan con un nivel de protección adecuado.

g) Se refuerza el deber de rectificación y corrección de datos. Con la legislación vigente el titular de datos personales tiene que probar al responsable de una base de datos que los datos que posee son erróneos, inexactos, equívocos o incompletos. Con la propuesta, se invierte la carga de la prueba debiendo siempre el responsable de la base de datos modificarlos, a menos que él pruebe que dichos datos son correctos. Además, se establece que si dichos datos hubieren sido comunicados a terceros, el responsable de la base de datos les deberá informar su corrección o eliminación, estando estos también obligados a rectificar o eliminar los datos en los términos informados.

h) Se regulan infracciones y sanciones. Se crea un catálogo pormenorizado de infracciones, distinguiendo entre leves, graves y gravísimas, con sus respectivas sanciones, consistentes en multas o, en el peor escenario, la cancelación del registro. Se establece un procedimiento sancionatorio, que puede iniciarse de oficio o por denuncia. Tal procedimiento garantiza la bilateralidad de la audiencia y el derecho a defensa del acusado o denunciado. Será la autoridad de control quien conozca de este proceso de reclamación y aplique en definitiva las sanciones. En contra de la resolución que imponga la sanción, se podrá reponer ante el mismo Consejo y en contra de la resolución que se pronuncie sobre esta última, podrá recurrirse de ilegalidad ante la Corte de Apelaciones, en los mismos términos que se regula en el artículo 28 de la Ley Nº 20.285 sobre Acceso a la Información Pública.

II. Proyecto de Ley que Introduce una Indicación Sustitutiva a los Proyectos de Ley que Modifican la Ley N° 19.628 Sobre Protección De La Vida Privada (Boletines N° 5309-03, 5356-07 y 6298-05).

Este proyecto de ley, conocido coloquialmente como "Proyecto sobre Deuda Consolidada", desplazó de la discusión política y legislativa del proyecto analizado en el punto anterior, no porque regule de mejor manera dichas materias, sino porque regula aspectos que concentran, hasta aquí, toda la atención de las iniciativas parlamentarias, (ya sea porque su actual tratamiento se considera que vulnera la vida privada de las personas, ya sea porque distorsiona algunos mecanismos para que el mercado financiero funcione de una manera más adecuada), pues como hemos indicado, su contenido apunta a regular el tratamiento de la información financiera y comercial de las personas, materias mucho más comprensibles por la mayoría de la ciudadanía que aquellas vinculadas a la autodeterminación informativa.

La información financiera en Chile está regulada desde el año 1928 en el Decreto Supremo Nº 950 del Ministerio de Hacienda y obliga a ciertos actores del mercado financiero a reportar la información morosa de los títulos de crédito de los deudores a una entidad denominada "Cámara de Comercio de Santiago". La ventaja de este sistema es que si bien centraliza el destinatario final de esta información, la norma no regula el costo ni la forma como los burós o distribuidores de información tratan dichos datos.

No existen tampoco mecanismos que obliguen a estos entes responsables a contemplar procedimientos para el resguardo de los derechos de los titulares de esos datos, ni estándares de seguridad, calidad y veracidad de los datos conocidos por el público cuyos datos son tratados. Hasta este punto podemos afirmar que todo el sistema está construido sobre conductas de autorregulación de estos actores.

Este mensaje fue presentado a tramitación legislativa como condición de avance del proyecto anterior en 2009. Entre los principales aspectos de esta iniciativa podemos destacar:

a) El reforzamiento de los derechos de los titulares de información financiera, sean estos personas naturales o jurídicas, para un adecuado funcionamiento del mercado del crédito, ya sean en instituciones bancarias o de otro tipo;

b) La ampliación de la información relativa a obligaciones económicas disponible en el mercado financiero, para que además de los datos sobre deudas morosas que hoy existe también se registre el buen comportamiento de pago de las personas, esto es lo que se conoce como deuda positiva;

c) Se introducen mecanismos de control de calidad y veracidad de los datos; y

d) Se crea una instancia administrativa para regular, fiscalizar y sancionar a los agentes y ordenar el mercado de la información comercial.

Alguna doctrina nacional discrepa de la promoción de estos cambios señalando que "no es posible detectar una tendencia clara que permita establecer estándares internacionales replicables, sobre todo cuando se quiere impulsar cambios por la vía compulsiva". Estas últimas opiniones estiman que este sistema es eficiente y que no necesita modificaciones.

III. Agenda Legislativa al 2010.

A la fecha ambos proyectos se encuentran en suspenso. Si bien ambos fueron presentados a tramitación legislativa, uno frenó el avance del otro y pero el último no concitó el acuerdo necesario entre las fuerzas políticas representadas en el parlamento por lo que se consideró apropiado suspender (también) su tramitación hasta que no se presentaran reformas para promover su aprobación.

Lo cierto es que la regulación de los datos personales en Chile sigue siendo un tema importante, presente en la agenda pública y parlamentaria, requerida por nuestra participación cada vez más activa en el concierto internacional, y quizás más importante aún, sentida por la ciudadanía. Sin embargo, hasta la fecha, las autoridades políticas no se han manifestado por ninguna de las alternativas presentadas en este trabajo, pero tampoco han dado indicios de proponer modificaciones o propuestas nuevas.

Quizás un impulso para retomar estos temas venga desde el propio parlamento, donde una comisión de senadores, especialmente sensibles al tema (todos promotores de distintas mociones ligadas a la protección de datos personales) se encuentran preparando una propuesta nueva y total que será presentada en los próximos meses al Presidente de la República.

**Danielle Zaror Miralles, abogada Universidad de Concepción, Magister en Derecho Económico Universidad de Chile, Diplomada en Regulación de Mercado Eléctrico y Telecomunicaciones; Asesora Ministerio de Economía, Fomento y Turismo.*

Protección de datos en el mundo

Fuente: Instituto Federal de Acceso a la Información Pública, según presentación de Lina Ornelas, Directora General de Clasificación y Datos Personales IFAI, México.

¿Qué es un dato personal?

Toda información concerniente a una persona física, identificada o identificable. Esta definición se retoma del ámbito internacional.

¿Cómo surge este nuevo derecho?

Del derecho a la intimidad (noción tradicional "a ser dejado solo"), y por el uso vertiginoso de la tecnología (que representa una amenaza a la privacidad por la acumulación de grandes cantidades de información, su transmisión fuera de las fronteras en minutos, así como la formación de perfiles del comportamiento de las personas –quienes son, qué enfermedades tienen, dónde y qué compran, etc.).

¿En qué consiste el derecho a la autodeterminación informativa?

Es el derecho que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaba y utiliza sus datos personales.

¿En qué consiste el derecho a la protección de datos personales?

Es un derecho fundamental (nuevo) que busca la protección de la persona en relación con el tratamiento de su información.

¿Cuáles son sus orígenes?

Los principales instrumentos internacionales de derechos humanos reconocen al derecho a la vida privada. Sin embargo, los avances en las TI y sus implicaciones para la vida de las personas dieron origen a un derecho distinto, relacionado con la protección de los datos personales

Las tres fases de creación fueron: La Resolución 509 de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos, a finales de los 70's; Leyes nacionales de Alemania Francia, Dinamarca, Austria, Luxemburgo; la Resolución del Parlamento Europeo sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática (1979); y en los 80's surge un catálogo de derechos de los ciudadanos para hacer efectiva la protección de los datos personales que se positiviza en diversos instrumentos normativos

¿Cuáles son los principales instrumentos en Europa?

El Convenio 108 del Consejo de Europa sobre protección de datos personales (1985); la Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos; la Carta de Derechos Fundamentales de la Unión Europea (2000); y Reconoce el derecho a la protección de datos como un derecho fundamental y autónomo, distinto al derecho a la intimidad y la privacidad de las personas

¿Cuáles son los principales instrumentos a nivel internacional?

OCDE "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales" (1980), que define conceptos fundamentales (e.g. datos personales, afectado), aplica a los sectores público y privado, establece principios aplicables al tratamiento de datos personales, garantiza el libre flujo sujeto al respeto a los principios de la directriz.

La Resolución 45/95 de la Asamblea de la ONU que contiene una lista básica de principios en materia de protección de datos personales y las Directrices para la armonización de la protección de datos personales de Iberoamérica (2007)

¿Y en el Continente Americano?

Canadá tiene leyes de protección de datos personales a nivel federal y provincial; Estados Unidos tiene regulaciones sectoriales "privacy act" (safe harbour), pero no reconoce el derecho como tal; En América Latina sólo Argentina y Chile tienen legislación específica en la materia; México tiene una regulación parcial sólo para ficheros públicos

COMPUTACIÓN EN NUBE PARA EUROPA

AGENDA DIGITAL: LA COMISIÓN RECABA OPINIONES SOBRE CÓMO SACAR MEJOR PROVECHO DE LA COMPUTACIÓN EN NUBE PARA EUROPA

La Comisión Europea se encuentra recabando opiniones de ciudadanos, empresas, administraciones públicas y otras partes interesadas sobre cómo sacar el máximo provecho de la «computación en nube». La computación en nube permite a empresas, administraciones públicas y personas que utilizan redes como Internet tener acceso a sus datos y programas desde ordenadores ubicados en otro lugar. Puede ayudar a las empresas –en particular a las PYME– a disminuir de forma drástica los costes de las tecnologías de la información, a los gobiernos a proporcionar servicios a precios más bajos y a ahorrar energía mediante un uso más eficaz de los equipos informáticos. La computación en nube ya está ampliamente extendida, por ejemplo en los servicios de correo electrónico a través de la web. La tendencia se está afianzando y se prevé que en 2014 los servicios en nube hayan generado beneficios de aproximadamente 35000 millones de euros en Europa. La promoción de las condiciones óptimas para que los ciudadanos y las empresas saquen el mayor provecho posible de este avance técnico constituye una de las acciones previstas en la Agenda Digital para Europa (véase IP/10/581, MEMO/10/199 y MEMO/10/200). Las respuestas contribuirán a la preparación de una estrategia europea de computación en nube que la Comisión presentará en 2012.

Neelie Kroes, Vicepresidenta de la Comisión Europea responsable de la Agenda Digital, ha declarado: «Estoy muy ilusionada con los beneficios que ofrece la computación en nube en materia de recorte de costes, mejora de los servicios y creación de nuevas oportunidades comerciales. Vamos a necesitar una estrategia de computación en nube bien definida para obtener el mayor provecho posible de su potencial. La información que estamos solicitando a las partes interesadas es importante para hacerlo bien».

La computación en nube tiene muchas posibilidades de convertirse en una de las principales industrias emergentes de servicios y ofrece grandes oportunidades para las empresas de telecomunicaciones y tecnología en Europa. Las empresas clientes y las administraciones públicas pueden beneficiarse de los precios bajos y los servicios punteros si utilizan la computación en nube en vez de instalar y mantener programas y equipos informáticos propios.

La Comisión insta a las partes interesadas, en especial a los fabricantes y a los usuarios de redes en nube, a relatar su experiencia, sus necesidades, sus expectativas y sus perspectivas sobre el uso y suministro de servicios de computación en nube. El cuestionario se propone obtener información sobre las siguientes cuestiones, entre otras:

- protección de datos y asuntos de responsabilidad, particularmente en contextos transfronterizos;
- otras barreras legales y técnicas que puedan ralentizar el desarrollo de la computación en nube en Europa;
- soluciones de normalización e interoperabilidad;
- contratación de servicios en nube, en particular para las PYME;
- formas de promoción de la investigación e innovación sobre computación en nube.

Los resultados contribuirán a la confección de una estrategia europea de computación en nube que la Comisión presentará en 2012. Dicha estrategia se propone clarificar las condiciones legales para la incorporación de la computación en nube en Europa, estimular el desarrollo de una industria y un mercado en nube europeos que sean competitivos y facilitar el desarrollo de servicios innovadores de computación en nube para ciudadanos y empresas.

Si desea acceder a la consulta pública, visite: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=cloudcomputing&lang=en

Sitio web de la Agenda Digital: http://ec.europa.eu/information_society/digital-agenda/index_en.htm

Sitio web de Neelie Kroes: http://ec.europa.eu/commission_2010-2014/kroes/

Twitter de Neelie Kroes: http://twitter.com/neeliekroeseu

EL MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE

Avances y desafíos pendientes en su configuración jurídica

*Por Andrea Paola Ruiz Rosas

Jefa de la Unidad de Normativa y Regulación del Consejo para la Transparencia. Chile

I. Ideas preliminares

Antes de abordar el tema de este artículo resulta forzoso sentar las bases de lo que debemos entender o, más bien, lo que debemos exigir al Ordenamiento Jurídico, para estimar que estamos ante un marco regulatorio propiamente tal. No es lo mismo hablar de un conjunto de normas (marco normativo) que de un conjunto de instituciones que conjugadas debidamente otorgan protección a un derecho fundamental en el contexto de un Estado Democrático de Derecho (marco regulatorio).

A nuestro entender, un marco regulatorio está conformado por varios elementos, que evidentemente exigen un marco normativo sólido, pero que, además, requieren de una serie de condiciones para fructificar en la orientación que se persigue. Así, no será suficiente con que exista una norma legal, incluso constitucional, que reconozca y regule el ejercicio del derecho, sino que es esencial que su titular tenga conciencia de su calidad de tal y del alcance de ese derecho y los sujetos obligados del alcance de las exigencias legales; y, por sobre todo, que ante un desconocimiento el Ordenamiento Jurídico reconduzca la conducta y reaccione mediante herramientas sancionatorias e indemnizatorias adecuadas (órgano competente, sanciones e indemnización). Serán, por lo tanto, tres los verbos rectores que buscaremos conjugar al describir el marco regulatorio en esta materia: normar, ordenar y encaminar.

Al conjugar los referidos verbos rectores los que van de la mano con las exigencias contempladas por la Unión Europea para que un país garantice un nivel de protección adecuado y se autoricen transferencias de datos desde un estado miembro hasta su territorio con la protección de los datos personales que otorga el Ordenamiento Jurídico en Chile se debe tener en especial consideración que esta protección tiene la categoría de derecho fundamental y que se ve vulnerable y vulnerada por la evidente y cada vez más profunda interfaz que se produce entre los datos personales y las tecnologías de la información. No abundaremos en problemáticas concretas, que escapan a la finalidad de estas líneas, pero sí recalcaremos que estas interconexiones ponen en evidencia las falencias normativas de nuestro país y hacen cada vez más necesario un marco regulatorio adecuado y ajustado a las exigencias internacionales.

II. Normar: dictar una normativa que de sustento legal al derecho fundamental a la protección de datos de carácter personal

Chile desde el 28 de agosto de 1999 cuenta con una normativa general relativa a la protección de los datos de carácter personal que se funda, principalmente, en el artículo 19 N°4 de la Constitución Política de la República, el que asegura a todas las personas el derecho a la vida privada y a la honra de la persona y su

familia. La referida norma es la Ley N°19.628, que como se puede apreciar en su texto tiene dos títulos: "Sobre protección a la vida privada" y "Protección de datos de carácter personal.

Más allá de este dato anecdótico, la ley comienza definiendo su ámbito de aplicación al disponer que rige todo "tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares", siendo indiferente que el tratamiento sea automatizado o manual o que la base de datos este restringida a ser utilizada en un ámbito privado o doméstico.

Con un rol evidentemente pedagógico, la ley continúa definiendo una serie de conceptos de gran trascendencia en esta materia. Interesa destacar la definición datos personales y de su titular; la de datos sensibles, las de fuentes accesibles al público, la de tratamiento de datos, la de responsable del registro o banco de datos, entre otras. Por su intermedio, es dable concluir que sólo pueden ser titulares del derecho las personas naturales y no las jurídicas, que da igual si el banco está automatizado o contempla un tratamiento manual, que la figura del responsable no alcanza a referirse al encargado que efectúa tratamientos por su cuenta, que las fuentes accesibles al público por esa sola circunstancia conllevan una protección restringida, etc.

A pesar de ser presentada como una ley protectora de los datos de carácter personal, el primer derecho que consagra es el derecho de toda persona (el responsable del registro o banco de datos) a efectuar tratamiento de datos personales, bajo tres requisitos: a) siempre que lo haga de manera concordante con esta ley; b) para finalidades permitidas por el ordenamiento jurídico y c) en todo caso, respetando el pleno ejercicio de los derechos fundamentales de los titulares de los datos y las facultades que esta ley les reconoce.

Por su parte y respecto de los titulares del derecho a la protección de datos personales la ley recoge una serie de derechos, entre ellos: el derecho de acceso, que consiste en acceder gratuitamente a información sobre sus datos, la procedencia o destinatario, el propósito del almacenamiento, etc.; el derecho de modificación; el derecho de eliminación o cancelación definitiva del dato personal en el registro respectivo; el derecho de bloqueo, que es la supresión temporal del dato personal; derecho a conocer la comunicación de datos; derecho de oposición y derecho a indemnización. Todos estos derechos están reconocidos de forma expresa, pero algunos de ellos son graduados o limitados en su ejercicio a casos o situaciones particulares. Asimismo, la ley aborda en forma particularizada la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, consignando las modificaciones introducidas por la Ley N°19.812, que fortalecen los derechos de los titulares de dichos datos y restringen su comunicación.

En cuanto al sujeto responsable, la ley distingue entre sujetos privados y sujetos públicos, estableciendo respecto de estos últimos una especial regulación. En concreto, autoriza el tratamiento de datos personales por parte de un organismo público, sin el consentimiento del titular, respecto de las materias de su competencia y con sujeción a las reglas establecidas en la ley. La doble exigencia de que el tratamiento se encuentre dentro de las materias de su competencia y que se efectúe de acuerdo a la ley, pareciere innecesaria y más bien una redundancia del legislador, teniendo en consideración que por exigencias constitucionales un órgano público sólo puede actuar válidamente dentro de la esfera de su competencia y en la forma que prescriba la ley (artículo 7), puesto que si se extralimitara su actuación adolecería del vicio de nulidad. Por consiguiente, en la medida que el organismo público cumpla con el mandato constitucional, podrá efectuar el tratamiento de datos personales sin autorización por parte de su titular.

Una real peculiaridad en la ley viene dada por la obligación de registro que pesa sobre los organismos públicos que son responsables de bancos de datos. Para dar cumplimiento a esta exigencia legal el Servicio de Registro Civil e Identificación debe llevar un registro de los bancos de datos personales a cargo de organismos públicos, el que tendrá carácter público y en el que constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende. El organismo público responsable del banco de datos proporcionará esos antecedentes al mencionado servicio cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados dentro de los quince días desde que se produzca el evento.

Asimismo y buscando configurar, de manera preliminar, un órgano de control respecto del tratamiento de bancos de datos en poder del sector público, la Ley de transparencia de la función pública y de acceso a la información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, encomendó

al Consejo para la Transparencia la facultad de velar por el adecuado cumplimiento de la Ley N°19.628 por parte de los órganos de la Administración del Estado, aun cuando omitió señalar el alcance preciso de dicha potestad.

A pesar del gran avance que significó en el año 1999 la entrada en vigencia de la Ley N°19.628 en Chile, en el curso de su implementación, la referida norma legal presentó una serie de deficiencias, que resultan aún más patentes si se tiene en cuenta el vertiginoso desarrollo tecnológico que se ha experimentado en el curso de estos últimos 10 años y las exigencias internacionales en la materia.

Destacan dentro de las principales críticas formuladas las siguientes : la ausencia de normas que hagan efectivo el principio de finalidad en el tratamiento de datos personales y el deber de información de tratamiento; la consagración de diversos conceptos que generan problemas interpretativos y que facilitan el desconocimiento de derechos, como, por ejemplo, el de fuente accesible al público; la falta de claridad respecto de quién es el responsable del tratamiento de los datos, en relación al encargado; la inexistencia de un registro de bases de datos en poder del sector privado y la falta de sanciones ante el incumplimiento del registro por parte de los órganos públicos; la ausencia de sanciones efectivas por infracciones a la normativa legal; la inutilidad del recurso de habeas data, siendo más conveniente interponer un recurso de protección cuando existe un desconocimiento de este derecho que utilizar la acción consagrada en la ley, la falta de una regulación adecuada para el tratamiento de datos personales en poder del sector público; la ausencia absoluta de normas que regulen las transferencias internacionales de datos personales; la inexistencia de una autoridad de control, entre muchas otras.

Parte de estos problemas están siendo discutidos en el Congreso Nacional, a través del conocimiento de iniciativas parlamentarias o del gobierno orientadas a adecuar la normativa nacional en materia de protección de datos a los estándares internacionales, en especial, a los de "protección adecuada" de la Unión Europea. Destaca dentro de los diversos proyectos de ley el presentado por el ejecutivo el año 2008 que se hace cargo de algunas de las deficiencias planteadas, fortaleciendo el marco normativo sustancial y proponiendo que el Consejo para la Transparencia sea el futuro órgano de control. A pesar de estos esfuerzos puntuales, sigue siendo un tema pendiente que exige un acuerdo transversal a nivel nacional, previa sensibilización de cada uno de los actores.

III. Ordenar: conseguir que la norma se haga realidad mediante su conocimiento y aplicación por los titulares de derechos y sujetos obligados

No obstante, el éxito de los esfuerzo normativos descritos supra es insuficiente para definir la concurrencia de un marco regulatorio en materia de protección de datos, debido a que la adecuada protección "se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento…". Sin embargo, las normas de protección de datos sólo contribuyen a la protección de las personas físicas si efectivamente se cumplen en la práctica. Por ello, es necesario considerar no sólo el contenido de las normas aplicables a los datos personales, sino también el sistema utilizado para asegurar la eficacia de dichas normas". Lo que deja sentado la precariedad del contenido del marco normativo y la relevancia de los dos elementos que pasamos a revisar: ordenar y encaminar.

De esta forma, el segundo factor determinante para reconocer la existencia de un marco regulatorio en protección de datos personales consiste en ordenar el ejercicio del derecho y las correlativas obligaciones que pesan sobre los sujetos responsables, es decir, colocar las cosas en el lugar que les corresponde, mediante una disposición legal adecuada (la Ley N°19.628 principalmente) y un órgano especialmente facultado al efecto.

Para ello constituirá una primera necesidad que exista conocimiento del derecho fundamental, que los titulares del derecho tengan conciencia que sus datos son proyección de su persona y que deben ejercer una tutela responsable respecto de los mismos, y que para el caso de existir una amenaza, perturbación o privación respecto de alguno de los derechos que consagra la normativa vigente tengan certidumbre de que su ejercicio estará amparado por el Ordenamiento Jurídico y será tutelado por un órgano competente. Esta intuición primaria del derecho a la protección de los datos de carácter personal es casi inexistente en nuestro país, pues a pesar de carecer de encuestas que corroboren esta conclusión, basta pensar en el número de veces en el día que entregamos nuestro RUT a todo aquel que lo solicita para las más variadas e, incluso, desconocidas finalidades y en la pasividad de los afectados.

Por otra parte, ordenar desde el punto de vista regulatorio tiene un segundo alcance para el sujeto obligado que consiste en la sumisión a la norma y su correspondiente aplicación. Con ello queremos significar que los sujetos responsables deben entender que la norma los obliga y,

en principio, darle cumplimiento espontáneo, dejando sólo para los desconocimientos más flagrantes la acción o amparo legal. Tal como existe un desconocimiento por parte de los titulares del derecho, también existe una rebeldía tácitamente aceptada por parte de los responsables de los bancos de datos, los que necesariamente conocen sus obligaciones, pero ante la falta de incentivos y de sanciones prefieren asumir el riesgo (con su eventual y consecutivo costo) y efectuar tratamientos al margen de la ley. Así ocurre, por ejemplo, con los órganos públicos que conocen la obligación de registro, pero que no la cumplen ante la falta de un órgano que les haga exigible el deber y de sanciones asociadas al incumplimiento.

Resulta forzoso reconocer, entonces, que para que el verbo "ordenar" del marco regulatorio se concretice no es suficiente que exista una norma legal que reconozca el derecho y que imponga las correlativas obligaciones, sino que a ello debe sumarse la existencia de un órgano independiente que sea promotor de la protección de datos ante la ciudadanía y fiscalizador de ésta por parte de los que efectúen tratamientos, es decir, una auténtica autoridad de control. Todas estas ideas, de una u otra forma, han sido catalogadas por la Unión Europea dentro de los objetivos de un sistema de protección de datos bajo el concepto de "nivel satisfactorio de cumplimiento de las normas".

IV. Encaminar: dirigir la normativa y el orden a garantizar efectivamente el derecho a través de una estructura organizacional independiente y sanciones adecuadas

El último elemento que conceptualizamos como conformador del marco regulatorio era el encaminamiento, queriendo significar con ello la necesidad que el marco normativo (el normar) y el ordenamiento de derechos y deberes relativos a la protección de datos (el ordenar) cuenten con una herramienta eficiente y eficaz que vuelva a encauzar o enderezar cualquier desconocimiento a la normativa vigente en la materia.

Las restricciones que las normas legales y los tribunales de justicia presentan respecto de la protección de datos personales en este encaminamiento son claras, no tienen la cercanía, las primeras, ni el tiempo, ni especialización, los segundos, para resolver con la celeridad que se requiere los casos de desconocimiento de este derecho fundamental. De ahí que la exigencia de una autoridad de control llamada a velar por el adecuado cumplimiento de las disposiciones relativas a la protección de datos, con atribuciones sancionatorias, es una pieza fundamental del aparataje jurídico. Será el marco normativo el que otorgue los recursos sancionatorios, pero es básico que esta autoridad tenga atribuciones para aplicar la norma con la contundencia que el conocimiento especializado le pueda proveer, a fin de orientar las conductas a la protección del derecho encomendada.

En este sentido, la normativa europea, ha puesto de relieve la importancia de ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos y la de ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las referidas normas , mediante la estructuración de un sistema de supervisión externa que adopte la forma de autoridad independiente.

V. Idea final: Los temas pendientes del marco regulatorio

Las ideas preliminares que expusimos al comienzo de este artículo tenían un propósito específico: poner en evidencia que en nuestro país hablar de marco regulatorio de la protección de datos personales es todavía un proyecto en construcción, puesto que de los tres verbos rectores que exigíamos conjugar, tal vez y con algunas deficiencias, sólo logramos evidenciar el ámbito normativo, dejando a gran distancia el de dar orden a los diversos actores (titulares del derecho, responsables del registro y encargados del tratamiento) y el de encaminar su ejercicio, a través de un órgano independiente y sanciones adecuadas.

El desarrollo institucional del marco regulatorio, del que dimos cuenta en estas líneas, representa una gran tarea pendiente para el país, la que deberá tener como primer objetivo insertar en nuestro ADN jurídico nacional este derecho fundamental a la protección de datos personales.

**Andrea Ruiz Rosas, abogada especialista en Derecho Público y Administrativo de la Universidad de Chile; Doctora © en Derecho Administrativo de la Universidad Complutense de Madrid y Magíster en Derecho Público de la Universidad de Chile; Jefa de la Unidad de Normativa y Regulación del Consejo para la Transparencia.*

El despliegue de este proyecto aborda su segunda fase

LA AUTORIDAD DE PROTECCIÓN DE DATOS DE FRANCIA AUTORIZA LA UTILIZACIÓN DE HISTORIALES CLÍNICOS ELECTRÓNICOS

Los historiales clínicos electrónicos son registros informatizados de cada beneficiario del seguro médico y permiten a los profesionales e instituciones sanitarias compartir información del paciente, la cual es necesaria para la coordinación de la asistencia, siempre y cuando haya un consentimiento previo.

La historia clínica electrónica fue creada por la Ley de 13 de agosto de 2004 de Seguros Médicos, con el objetivo de mejorar la coordinación y la calidad de la asistencia sanitaria. La primera fase de este proyecto se inició en el 2006 y ahora comienza su segunda fase, para la cual es indispensable la definición de un marco de trabajo regulatorio que defina el contenido de la historia clínica y las condiciones de acceso.

Una vez que se haya actualizado el software necesario y se hayan proporcionado las herramientas imprescindibles para su utilización, los sistemas de información serán capaces de comunicar con la historia clínica electrónica, lo que ahorrará a los profesionales sanitarios la necesidad de recopilar nuevamente la información de sus pacientes. Aquellos que aún no tengan actualizado el software podrán acceder a la historia clínica electrónica a través de un sitio web.

Cualquier beneficiario de un seguro médico que disponga de una tarjeta personal de salud (denominada Tarjeta Vital en Francia) podrá crear su propia historia clínica electrónica en una oficina sanitaria o en la recepción de una institución sanitaria y, de esta forma, acceder a ella directamente a través de un ordenador.

La inquietud por la seguridad en internet supera a otras cuestiones como el terrorismo o las estafas online

EL 35% DE LOS CIUDADANOS TEME QUE EL GOBIERNO DE ESTADOS UNIDOS TENGA ACCESO A SUS ACTIVIDADES EN INTERNET

La privacidad y el control de las actividades a través de Internet se han convertido en una de las cuatro cuestiones que más preocupan a los ciudadanos, con un 35% de la población preocupada por la posibilidad de que el Gobierno pueda acceder a sus datos.

Un estudio de la compañía Opera Software ha investigado el grado de inquietud de la población en cuestión de seguridad informática con motivo de la celebración del "Día de la protección de datos". El estudio, realizado por la empresa YouGov, ha encuestado a más de 3.000 personas en Estados Unidos, Japón y Rusia (1.000 en cada país). La muestra seleccionada es representativa de los adultos mayores de 18 años en los tres países.

El 35% de los encuestados en los Estados Unidos han situado como su principal preocupación en Internet que el gobierno tenga acceso a sus actividades. En el caso de Japón, la principal preocupación para un 33% es la seguridad en las compras online. En Estados Unidos y Rusia los usuarios no están tan preocupados en este sentido. El 5 y el 6 por ciento, respectivamente, comparten la preocupación con los japoneses.

El 38% de los participantes rusos han destacado las redes sociales como su máxima preocupación de seguridad en la red. Los encuestados han destacado la gran accesibilidad a sus actividades en este tipo de páginas. En el caso de Estados Unidos, con un 15%, y Japón, con un 10%, los usuarios han situado las redes sociales como su segunda preocupación en cuanto a seguridad en Internet.

Entre tanta preocupación también hay sitio para los usuarios que están tranquilos sobre sus actividades en Internet. Entre el 13 y el 19 por ciento de los encuestados en cada país no está preocupado porque otras personas puedan conocer sus actividades online.

Los programas antivirus son la medida preferida para proteger la privacidad en línea. En Rusia el 90% utiliza estos programas, mientras que en Estados Unidos el número baja al 79% y en Japón al 68%. A pesar de su preocupación por la violación de privacidad online y la utilización de antivirus, menos del 61% de los encuestados en los Estados Unidos utilizan contraseñas seguras, y en Japón la cifra baja hasta menos de un tercio.

La utilización de software y sitios web que no recogen información es una práctica muy poco desarrollada. Solamente el 9,15% de los encuestados en cada país acceden de forma habitual a estos portales. El grado de preocupación de los usuarios respecto a su privacidad parece no corresponderse con las medidas de prevención que utilizan.

"Es interesante notar las diferencias entre lo que la gente dice que les preocupa en la seguridad en Internet y lo

que realmente hacen para protegerse", ha explicado el oficial de desarrollo de Opera, Bautizan Krogh. "Nosotros a menudo vemos que esto es la naturaleza humana. Tememos los accidentes de tráfico, pero no usamos un cinturón de seguridad o el casco. Se teme la bancarrota, pero sigue gastando. Esto se parece muchísimo al comportamiento sobre la seguridad en Internet".

Cuando se les consultó a los usuarios con qué dispositivo se sienten más seguros para acceder a Internet, los tres países prefirieron usar un ordenador en vez de un teléfono móvil, sobre todo en Rusia, con un 62%. Esta tendencia fue más fuerte entre los hombres. Entre el 22 y el 31 por ciento de los encuestados en cada país no tiene preferencias por ningún dispositivo.

En total, un 54% de los encuestados en los Estados Unidos y un 46% en Rusia cree que la responsabilidad de garantizar la seguridad online de las personas y su privacidad se encuentra en los propios usuarios. En Japón, el 47% de los encuestados han señalado que es responsabilidad de las webs de las empresas. Para el 25% de los encuestados en Estados Unidos es responsabilidad del gobierno.

La cuestión de la privacidad en Internet ocupa el cuarto lugar entre las preocupaciones de los ciudadanos. Entre el 22 y el 29 por ciento de todos los encuestados consideran la defensa de sus datos y actividades en Internet como su mayor preocupación. Los datos confirman un aumento de la atención de las poblaciones en materia de privacidad online.

Las personas están más preocupadas por su privacidad en línea que por los ataques terroristas, por arruinarse o por ser atacados en su casa. La privacidad en la red continúa ganando protagonismo y su aparición en la lista de inquietudes en la población es significativa.

FACEBOOK CEDE DATOS DE CONTACTO A TERCEROS

Aunque el usuario es, por supuesto, el que da permiso para que la conocida red social ceda a los programadores sus datos de contacto, los afectados pueden olvidar algo básico: que, en muchas ocasiones, dicha información incluye el número de teléfono y la dirección que el usuario especificó en su perfil cuando lo abrió.

A partir de ahora, bajarse un juego o cualquier otra aplicación de Facebook viene precedido de la siguiente advertencia/pregunta: "El (nombre de la aplicación) requiere su permiso para efectuar las siguientes acciones: acceder a su información básica y acceder a su información de contacto".

Por esta razón, una posible medida para evitar las consecuencias de la decisión de Facebook es modificar el perfil, quitando todos aquellos datos de contacto que pueden ser cedidos a terceros, según la nueva normativa de la compañía.

La nueva medida supone un nuevo desafío por parte de Facebook a las agencias que vigilan la privacidad de los datos de sus más de 500 millones de usuarios. En octubre del año pasado, la compañía estadounidense admitió fallos de seguridad en su red, tras hacer público The Wall Street Journal que varias de sus aplicaciones habían estado transmitiendo a otras empresas un número único que identifica a cada usuario de la web, y a partir del cual se podían obtener algunos de sus datos personales.

No era el primer escándalo de Facebook en cuanto a la gestión de la privacidad de sus miembros. Tan sólo tres meses antes, en julio del pasado año, un experto en seguridad recopiló información de más de 100 millones de usuarios. La empresa se defendió con la excusa de que los datos ya eran accesibles antes y, veladamente, culpó a los propios afectados por no haber cerrado sus perfiles. En mayo de 2010, Mark Zuckerberg, el fundador de Facebook, ya había reconocido que la compañía había cometido "un montón de errores" en este sentido.

Mediante un comic y un sitio web con juegos

LA AUTORIDAD DE PROTECCIÓN DE DATOS SUIZA LANZA UNA CAMPAÑA PARA PROTEGER SUS DATOS EN LA RED

La campaña, denominada Netla, no pone el foco en los peligros existentes en Internet, sino en que los jóvenes piensen cómo hacen uso de la red y cómo comparten sus experiencias, bien o mal.

Hanspeter Thür, Comisionado de Protección de Datos de Suiza, afirmó en la presentación de esta campaña que los jóvenes y los adolescentes deben tomar conciencia que subir una imagen a una red social podría, por ejemplo, tener consecuencias cuando busquen un trabajo posteriormente.

Un comic y un sitio web con dos juegos ayudarán a los jóvenes a reconsiderar su comportamiento online. Consejos para los padres y material de aprendizaje se encuentran también disponibles en este sitio web.

Ante la octava edición del Día Internacional de Internet segura

CONSEJOS PARA NAVEGAR EN LA RED DE UNA FORMA SEGURA

Con motivo de la octava edición del Día Internacional de la Internet segura, la compañía de seguridad Trend Micro ha publicado una guía de consejos prácticos "para

que los usuarios logren una experiencia 'online' segura cuando utilicen Internet".

"Dada la evolución que está experimentando el cibercrimen, los usuarios con fines malintencionados están realizando continuos avances con el objetivo de encontrar nuevos y mejores métodos y alternativas para infectar sistemas y aplicaciones, ya sean éstos equipos personales, smartphones, redes sociales, etc.", explica la compañía.

Por este motivo, instan a los usuarios a seguir consejos relacionados, por ejemplo, con el 'e-mail', como no abrir correos electrónicos procedentes de desconocidos o verificar la autenticidad de los mensajes (algo que recomiendan hacer con herramientas dedicadas a ese fin).

Además, también recomiendan no seguir enlaces no verificados, tanto en correos como en páginas web. "Esto es particularmente peligroso en los sitios de redes sociales, donde es más probable que el usuario baje la guardia", explican desde Trend Micro.

Otros consejos son detener la descarga de archivos que procedan de fuentes poco seguras y, en general, no descargar nunca archivos de páginas dudosas. En este sentido, recomiendan analizar los archivos antes de descargarlos y leer los acuerdos de licencia.

En cuanto a los dispositivos móviles, Trend Micro recomienda no acceder "nunca" a páginas financieras "u otros sitios que requieran información confidencial" desde teléfonos 'inteligentes', dado que esto "facilita el acceso a los cibercriminales para robar no sólo dinero, sino información sobre identificación personal". Además, hay que "prestar atención a los detalles", dado que, al variar el tamaño y la capacidad de estos dispositivos, algunos buscadores pueden ocultar las direcciones URL al completo, lo que puede ser utilizado para ataques de 'phising'.

Estos dispositivos, recuerdan, tienen integradas funciones de seguridad que los usuarios deben aprovechar. Las aplicaciones, advierten, también son utilizadas en algunos ataques, por lo que los usuarios deben ser selectivos a la hora de descargarlas e instalarlas.

Por último, en lo referente al 'software', recomiendan a los usuarios no utilizar 'software' sin licencia y descargar las actualizaciones del mismo de forma regular.

El paquete consta de once medidas

LA UE PRESENTA PROPUESTAS PARA AUMENTAR LA SEGURIDAD EN LA RED PARA LOS MENORES

La Comisión Europea ha presentado una batería de propuestas destinadas a mejorar la protección de los derechos de los menores en la UE y, sobre todo, para promover una justicia más adaptada a sus necesidades y reforzar la seguridad en Internet con el objetivo de combatir la pornografía infantil y el acoso en la red.

La vicepresidenta de la Comisión y responsable de Justicia, Viviane Reding, ha justificado las nuevas propuestas porque "los derechos de los menores son derechos fundamentales", tal y como deja claro la Carta Europea de los Derechos Humanos, jurídicamente vinculante tras la entrada en vigor del Tratado de Lisboa, que insta a los veintisiete a promover los derechos del menor.

"La Unión y sus 27 Estados miembros deben velar por la protección de sus derechos y garantizar que el interés superior del menor guíe su acción. Necesitamos, especialmente, una justicia mejor adaptada a los menores que garantice la toma en consideración de sus derechos cada vez que tengan que recurrir al sistema judicial, ya sea como víctimas o sospechosos, cuando sus padres se divorcien y cuando no se entiendan sobre las modalidades de su custodia", ha recalcado en un comunicado.

El Ejecutivo comunitario ha presentado un paquete de once medidas que pondrá en marcha en los próximos años para reforzar la protección de los derechos del menor, garantizar una protección especial de los menores discapacitados y víctimas de la exclusión social, proteger a los menores víctimas de la criminalidad, introduciendo garantías para los menores sospechosos y para reforzar la seguridad en Internet contra la pornografía infantil o la manipulación psicológica. Igualmente, pondrá en marcha el portal Europa para concienciarles de sus derechos.

La Comisión, que se ha comprometido a garantizar que las políticas comunitarias respeten el interés supremo del menor, publicó el primer informe anual de los Derechos Fundamentales en el que se valorarán los progresos realizados hasta ahora para cumplir los derechos del menor.

Congregó a miembros de distintos ámbitos de actividad relacionados con la privacidad

LA APEP ORGANIZÓ EL I CONGRESO NACIONAL DE PRIVACIDAD

Entre los participantes figuraron los Directores de las diferentes Autoridades de Control de España, así como la Asesora del Supervisor Europeo de Protección de Datos, y también otros ponentes nacionales e internacionales de especial relevancia.

Entre los temas que se trataron destacaron los referentes a los retos para la protección de datos personales, la

posible reforma de la Directiva 95/46, la protección de datos y su relación con los medios de comunicación, el Esquema Nacional de Seguridad, el acceso a los expedientes administrativos, la publicación de datos en Boletines Oficiales, el cloud computing y la reciente reforma del régimen sancionador de la LOPD.

Incumplimiento

PAÍSES DE LA UE DONDE SE VULNERA LA PRIVACIDAD EN INTERNET

En concreto, el 7% de los usuarios de Internet en España denuncia abusos contra su privacidad, un porcentaje que es casi el doble que el registrado de media en la Unión Europea (4%).

Junto a España, Bulgaria es el país con el porcentaje más elevado, también con un 7%, seguido por Italia y los Países Bajos con un 6%. Por el contrario, en la República Checa, Chipre, Eslovenia, Finlandia y Suecia sólo reportaron delitos contra la privacidad el 1% de los internautas.

España también se sitúa por encima de la media comunitaria en los casos de personas que han perdido dinero por delitos de "phising" (suplantación de la identidad en Internet), "pharming" (redireccionar al usuario a páginas falsas) o por pagos erróneos con la tarjeta de crédito. En este caso, el 4% de los usuarios de Internet en España aseguran que han perdido dinero con este tipo de ataques informáticos, mientras que la media de la UE se sitúa en el 3%. Los países con los porcentajes más elevados son Letonia (8%), Reino Unido (7%), Malta (5%) y Austria (5%).

Además, el 33% de los internautas españoles afirma que sus equipos han sufrido el ataque de virus, frente al 31% de la media comunitaria. No obstante, el porcentaje español es muy inferior al de otros países como Bulgaria (58%), Malta (50%), Eslovaquia (47%) o Hungría (46%).

A pesar de situarse por encima de la media en todos los tipos de ataques informáticos, los internautas españoles se sitúan al mismo nivel que el resto de países comunitarios en el uso de programas de seguridad informática o antivirus, con un 84% del total. Los usuarios más precavidos son, con diferencia, los de los Países Bajos, con un 96% de los internautas que utilizan este tipo de programas defensivos; seguidos por los de Luxemburgo, Malta y Finlandia, con el 91%.

Por último, España se sitúa por debajo de la media europea en el caso de incidencias relacionadas con el acceso de menores a páginas web inapropiadas o para adultos, con un 3% del total frente al 5% de la UE. No obstante, también está por debajo de la media en el porcentaje de usuarios que utilizan programas de control parental, con un 13%, un punto menos que el resto de la Unión.

Para enseñarles a preservar su privacidad en las redes sociales

LA AGENCIA VASCA DE PROTECCIÓN DE DATOS ELABORA UNA GUÍA AUDIOVISUAL DIRIGIDA A LOS JÓVENES

Para ello, en esta guía audiovisual se recogen una serie de recomendaciones para que los usuarios de redes sociales como Twiter, Tuenti o Facebook, en especial los más jóvenes, no cuelguen en sus perfiles datos privados o que podrían comprometerles en el futuro por ejemplo, a la hora de buscar un empleo.

Así, en las tutorías se recomienda que no se permita la descarga de las fotos personales, así como que no se pongan números de teléfono a disposición de otros usuarios, entre otros consejos.

Está especialmente dirigido a los jóvenes porque, según su Director, son a los que "más les gusta exhibir sus habilidades", así como sus "últimas juergas".

Ha explicado que este comportamiento no es achacable sólo a esta generación, sino que las precedentes también alardeaban de las mismas cosas, con la diferencia de que no podían plasmarlo en Internet, donde "todo deja huella".

No obstante, ha reconocido que los más jóvenes son cada vez más conscientes de que deben preservar su privacidad, al tiempo que ha considerado que la sociedad debería también adaptarse a estas nuevas tecnologías.

"Si cuando uno está buscando trabajo sale en la entrevista una foto suya en una juerga (colgada previamente en una red social) se debería pensar que es una persona normal", ha considerado.

En busca de una base común: protección de datos en las relaciones trasatlánticas (EEUU/ Unión Europea)

Hallar el equilibrio adecuado entre la lucha contra el terrorismo y la protección de la intimidad de los ciudadanos se ha convertido en el principal caballo de batalla en la negociación de acuerdos transatlánticos entre la Unión Europea y Estados Unidos. Eric Holder, fiscal general de EE.UU., cree que es posible encontrar la solución a través del diálogo. "Compartimos vuestra preocupación por la protección de la intimidad y las libertades civiles", señaló Holder en el PE.

Eric Holder recibió una calurosa bienvenida por parte de los eurodiputados en su visita al Parlamento Europeo el martes 20 de septiembre de 2010. Los aplausos recibidos tras su discurso dieron clara muestra del deseo que existe por llegar a un entendimiento definitivo en materia de protección de datos. Holder habló de una política de "mano tendida", palabras que el europarlamentario socialista español Juan López Aguilar supo apreciar como "un gesto de buena voluntad".

Cabe recordar que la protección de los datos personales ha sido en los últimos años motivo de desacuerdos entre la Unión Europea y Estados Unidos, especialmente cuando el PE mostró su negativa a la transferencia de datos bancarios a Estados Unidos en el conocido como informe SWIFT. Ahora parece más cercana la posibilidad de un acuerdo sobre esta materia, así como sobre el intercambio de información de los datos de vuelo de los pasajeros. En ambos casos la Eurocámara dispondrá del derecho de veto.

"Ninguna de las partes obtendrá todo lo que pide, pero al final de lo que se trata es de proteger a nuestros ciudadanos" apuntó Holder. El titular del departamento estadounidense de Justicia se refirió a este encuentro como "un intercambio franco de opiniones entre amigos" y confió en que las negociaciones den fruto lo antes posible.

Cabe recordar que los ministros de asuntos Exteriores de la Unión Europea pusieron fin definitivamente al acuerdo provisional de transferencia de datos bancarios con Estados Unidos a través de la red SWIFT, tras el rechazo expresado por la Eurocámara el 11 de febrero de 2010. Para los eurodiputados, el acuerdo no ofrecía garantías suficientes en cuanto a protección de los datos de los ciudadanos europeos. Este artículo repasa las claves de este asunto, fundamental tanto para el PE como para los ciudadanos.

Ocho de cada diez transacciones financieras que se realizan en 208 países del mundo pasan a través de la empresa SWIFT. Tras los atentados contra las Torres Gemelas en Nueva York, Estados Unidos recurrió a SWIFT para rastrear transacciones bancarias, sobre la base de un programa de su departamento de Estado para el seguimiento de la financiación del terrorismo.

A lo largo de 2009, SWIFT estableció en Suiza un centro específico de almacenamiento de sus datos europeos; hasta ese momento, todo se concentraba en un servidor estadounidense. El cambio hizo necesaria la negociación de un nuevo acuerdo entre la Comisión y el Consejo, por un lado, y Estados Unidos, por otro.

Claves de la negociación

Tres son los puntos clave que pueden desbloquear definitivamente la negociación. El primero y principal son las diferencias de orden jurídico a ambos lados del Atlántico, aunque Holder prefiere optar por "no atascarnos en términos técnicos y tener presente nuestro verdadero objetivo: la protección de nuestros ciudadanos".

El segundo aspecto responde al esfuerzo que la administración de Obama ha emprendido por redirigir su política en lo que a derechos fundamentales se refiere.

El compromiso de cerrar Guantánamo, la ruptura con algunas de las técnicas más polémicas empleadas por el anterior gobierno y el reconocimiento de los errores cometidos en el pasado hacen que ahora Estados Unidos reme en la misma dirección que la Unión Europea.

Por último, EE.UU. pretende conceder al debate entre ambas partes un enfoque más pragmático y menos "académico". "Deberíamos centrarnos en lo que ocurrió y no en lo que hipotéticamente podría ocurrir", opinó Holder, quien también dijo no tener constancia de que "bajo los acuerdos entre la UE y Estados Unidos se haya socavado la protección de datos".

Opiniones discordantes

En cambio, la eurodiputada liberal rumana Renate Weber rebatió uno de los comentarios de Holder recordando que "la protección de datos se basa fundamentalmente en evitar problemas hipotéticos".

Podría decirse que los eurodiputados coinciden en el objetivo, pero no en las formas. Así, el popular alemán Manfred Weber aseguró que "queremos seguridad jurídica para los ciudadanos europeos que crucen el Atlántico", mientras que la española del grupo parlamentario socialista Carmen Romero consideró que "la intimidad en Estados Unidos parece una especie de derecho condicionado".

Eric Holder también mantuvo un encuentro con la Vicepresidenta de la Comisión y responsable de Justicia, Derechos fundamentales y Ciudadanía, Viviane Reding, y con Cecilia Malmström, comisaria de Asuntos de Interior.

La negociación que está ocurriendo hoy

El futuro de la protección de datos en la cooperación policial y judicial entre la UE y Estados Unidos pasa por un acuerdo que está siendo negociado en estos momentos. El lunes 25 de octubre, eurodiputados, expertos y representantes de la Comisión, el Consejo y el gobierno estadounidense debatieron cómo debe ser este acuerdo marco. Para Jan Philipp Albrecht, ponente sobre el tema en el PE, "es muy importante contar con estándares comunes", porque "cada vez se intercambian más datos".

La audiencia especial, organizada por la comisión parlamentaria de Libertades Civiles, estuvo dividida en tres sesiones de debate en la que se trataron temas como el fortalecimiento del diálogo sobre protección de datos, los valores comunes a ambas orillas del Atlántico, posibles obstáculos constitucionales y cómo afrontar conjuntamente el impacto que podría suponer el nuevo acuerdo marco.

Se habla de acuerdo marco porque el objetivo es establecer estándares comunes básicos a los que debería ajustarse cualquier debate o negociación sobre intercambio de datos. Por el momento, el punto que ha suscitado mayores diferencias es si el acuerdo debe ser de carácter retroactivo (como pide la Unión Europea) o no (como defiende Estados Unidos).

Hasta el momento, la Comisión Europea ha presentado al Consejo un proyecto de mandato. El acuerdo final precisará del visto bueno del Parlamento Europeo, que tendrá capacidad para vetarlo si no lo considera satisfactorio.

ÚLTIMAS PUBLICACIONES

CELARE-Centro Latinoamericano para las Relaciones con Europa

Fue fundado en 1993 para promover los vínculos entre la Unión Europea y América Latina y el Caribe (UE/ALC). Es una corporación de derecho privado, pluralista y sin fines de lucro, con sede en Santiago de Chile, que ejecuta sus programas en las subregiones y países latinoamericanos, así como en los estados miembros europeos.

Sus objetivos son cooperar al fortalecimiento de los vínculos históricos, políticos, culturales y económicos entre la UE y ALC. Promover la reflexión sobre el proceso de asociación entre ambas regiones, destinado a construir un proyecto estratégico común. Aportar a la dinámica de cooperación e intercambio, principalmente entre parlamentos, gobiernos, entidades académicas, medios de comunicación y la sociedad civil organizada de ambas regiones. Promover y apoyar los procesos de integración de América Latina, aprovechando la experiencia y la cooperación de la Unión Europea. Acompañar a los organismos públicos y privados e instituciones académicas y sociales de ambas regiones, en sus programas y proyectos de cooperación al desarrollo.

Presidente: Gonzalo Arenas Valverde. **Director Ejecutivo:** Héctor Casanueva Ojeda. www.celare.org

PUBLICACIONES Y SERVICIOS DE INFORMACIÓN CELARE SOBRE RELACIONES EUROLATINOAMERICANAS

LIBROS MÁS RECIENTES

- La Unión Europea, América Latina y el Caribe:10 años de Asociación Estratégica (2009)
- Migraciones y Codesarrollo en la Relación entre la UE y ALC (2009)
- V Cumbre América Latina y el Caribe - Unión Europea, Lima 2008: Evaluación, desafíos y propuestas (2008)
- Hacia una América Latina Solidaria (2007)
- Migraciones: Experiencias en América Latina y la Unión Europea (2006)
- Las relaciones eurolatinoamericanas: de la Cumbre de Viena a la Cumbre de Lima (2006)
- El diálogo social en los Acuerdos Unión Europea / América Latina: Situación en el sector rural en Chile y México (2006)
- De Guadalajara a Viena: Hacia una Cumbre Nueva (2005)
- Juntos en un Solo Mundo. XVII Conferencia Interparlamentaria UE / AL. Lima 2005 (2005)
- III Cumbre ALC/UE - México 2004
- Proyecciones de los Consensos de Guadalajara (2005)
- El Diseño de la Asociación Estratégica Birregional (2005)
- Aportes a la III Cumbre Unión Europea / América Latina y el Caribe. Guadalajara 2004 (2004)
- XVI Conferencia Interparlamentaria Unión Europea - América Latina. Bruselas 2003 (2003)
- La Asociación Estratégica Chile - Unión Europea (2003)
- II Cumbre Unión Europea - América Latina y el Caribe. Reflexiones y Proyecciones tras Madrid 2002 (2002)
- II Cumbre América Latina y el Caribe - Unión Europea en un Mundo Global. Aportes para una Carta de Navegación Común (2002)
- Unión Europea y América Latina frente a los Desafíos de la Globalización (2001)
- La Sociedad Civil del Mercosur y Chile en la Asociación con la Unión Europea (2000)

- **SERIE DOCUMENTACIÓN DE BASE DE LAS RELACIONES UNIÓN EUROPEA / AMÉRICA LATINA Y EL CARIBE**

  Años 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010.

- **Revista EUROLAT: Revista temática periódica publicada desde 1995.**

  Últimos números publicados:

  76: Las distintas caras de la migración
  77: Cohesión social, la clave del desarrollo
  78: Desarrollo sostenible en las relaciones ALC-UE
  79: Hacia una alianza energética ALC-UE
  80: 10 años de la Asociación Estratégica ALC-UE
  81: El Tratado de Lisboa y el Futuro de Europa
  82: Género y Desarrollo en las Relaciones UE-ALC

EUROLAT

Servicios Informativos EUROLAT:

Pauta informativa diaria y Semanario Eurolat de monitoreo sobre las Relaciones Unión Europea/América Latina y el Caribe, situación de la integración europea y latinoamericana

LLEGA DIARIAMENTE A SU CASILLA. SUSCRIPCIÓN GRATUITA. SOLICITARLA A: celareuealc@celare.org

Las publicaciones CELARE están disponibles en formato electrónico en el portal Web institucional

REVISTA EUROLAT: *Dirección y edición general:* Héctor Casanueva Ojeda
Redacción y documentación: Equipo Celare - *Diseño y diagramación:* Francisco Martínez.
Esta revista se ha realizado con ayuda financiera de la Unión Europea. El contenido de este documento es responsabilidad exclusiva de CELARE y en modo alguno debe considerarse que refleja la posición de la Unión Europea.

CELARE

UNIVERSIDAD PEDRO DE VALDIVIA

CELARE - Centro Latinoamericano para las Relaciones con Europa,
Apoquindo 5142, Las Condes, Santiago de Chile.
Tel. 562-8285840. Correo electrónico: celareuealc@celare.org
Portal Web: www.celare.org