HACIA UNA EFECTIVA PROTECCIÓN DE LOS DATOS EN IBEROAMÉRICA

Declaraciones de la iniciativa del Observatorio Iberoamericano de Protección de Datos

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

Atención al Vecino Av. Belgrano 673
0800 999 3722

@defensoriacaba
www.defensoria.org.ar

Alejandro Amor Defensor del Pueblo

PRESENTACIÓN

Daniel López Carballo
Director del Observatorio Iberoamericano de Protección de Datos / España

Si bien la mayor parte de las legislaciones iberoamericanas regulan el derecho de las personas a la protección sobre sus datos, en el marco del llamado habeas data, como garantía constitucional, cada vez son más los Estados que cuentan con normas específicas en materia de protección de datos, adecuando sus leyes, decretos y otra normativa para una mejor salvaguarda de este derecho fundamental, así como su tutela judicial efectiva.

La protección de la privacidad debe ser entendida como un derecho fundamental, tal y como reconoce Naciones Unidas en el marco de la protección de la libertad individual, la libertad de expresión, la intimidad y la dignidad personal. A mayor abundamiento, el Consejo de Europa lo define como un derecho humano fundamental, mismo sentido en que es tratado en la Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos, donde se define la privacidad como un derecho, afirmándose que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".

El habeas data nace como garantía constitucional del derecho contra la información abusiva, inexacta o perjudicial para las personas, íntimamente ligada al derecho a la protección de datos de carácter personal, permite el acceso a registros y ficheros de datos, públicos y privados, con la finalidad de adecuar, actualizar, rectificar, cancelar o mantener en reserva la información del ciudadano afectado.

En su Declaración de Principios, la propia Comisión Interamericana de Derechos Humanos establece en su principio tercero que "toda persona tiene derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificar y/o enmendarla".

En este contexto nace la acción del habeas data, como derecho de acceso y control sobre los datos de carácter personal de las personas, garantizando el derecho a la intimidad. La propia Convención Americana en sus artículos 13.2 y 11 protege el derecho a la privacidad, la honra y la reputación de las personas.

La acción del habeas data está recogida en la mayoría de Constituciones de los Estados iberoamericanos, sírvase como ejemplo el artículo 15 de la Constitución Política de Colombia: "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las

informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

La Constitución Política de la República del Ecuador de 2008, concretamente en su artículo 92, se establece:

> () toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

La Constitución del Estado Centroamericano de Honduras de 1982 recoge en su artículo 76 la garantía al derecho al honor, a la intimidad personal, familiar y a la propia imagen; y en el artículo 182, el derecho fundamental de acceso a la información pública y privada, así como la garantía constitucional de habeas data:

> El Estado reconoce la garantía de Hábeas Corpus o Exhibición Personal, y de Hábeas Data. En consecuencia en el Hábeas Corpus o Exhibición Personal, toda persona agraviada o cualquier otra en nombre de ésta tiene derecho a promoverla; y en el Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la manera siguiente: (…) 2. El Hábeas Data: Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla. Las acciones de Hábeas Corpus y Hábeas Data se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles o inhábiles, y libre de costas. Únicamente conocerá de la garantía del Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tendrá la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a

> los derechos del honor, intimidad personal o familiar y la propia imagen. Los titulares de los órganos jurisdiccionales no podrán desechar la acción de Hábeas Corpus o Exhibición Personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad y a la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones constitucionales, incurrirán en responsabilidad penal y administrativa. Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurrirán en el delito de detención ilegal.

En el caso de Perú, en su Constitución Política de 1993, se reconoce en su artículo 2 el derecho de toda persona a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional, así como a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. A mayor abundamiento el artículo 200 establece, dentro de las garantías constitucionales "el habeas data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o personal, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5º y 6º de la Constitución".

La Constitución Federal Brasileña del 5 de octubre de 1988 determina, en su artículo 5, que el habeas data constituye un instrumento de defensa de los derechos individuales y colectivos "para asegurar el conocimiento de informaciones relativas a la persona del impetrante, que obren en registros o bancos de datos de entidades del gobierno o de carácter público" y "para la rectificación de datos, cuando no se prefiera hacerlo por el proceso secreto, judicial o administrativo".

Por último, a modo de ejemplo, la Constitución de Paraguay de 1992 incorpora el habeas data, reconociendo que "toda persona puede acceder a la información que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente, la actualización, la rectificación o destrucción de aquellos si fuesen erróneos o afectaren ilegítimamente sus derechos".

Una protección que se completa con desarrollos normativos específicos tales como la Ley N. 18331 (11 de noviembre de 2008) de Protección de Datos Personales y Acción Habeas Data en Uruguay; la Ley peruana 29733 de Protección de Datos Personales; en Argentina la Ley 25326 de Protección de Datos del 2 noviembre de 2000, el Decreto 1558/2001 Reglamentación de la Ley de Protección de Datos y la Ley 1845 de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires; la Ley 787 de Protección de Datos Personales en Nicaragua; en México la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, junto con su normativa de desarrollo; la Ley Estatutaria 1581, de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales en Colombia; en Chile la Ley 19628 sobre Protección de Datos

de carácter personal; la Ley Orgánica 172-13 de Protección de Datos de Carácter Personal de la República Dominicana; o en el caso de Costa Rica, tanto la Ley 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales, como el Decreto Ejecutivo 37554-JP, del 30 de octubre de 2012, que reglamenta dicha norma.

Junto con las normas enumeradas, otros países como Honduras, Panamá, Chile o Brasil, se encuentran elaborando nuevas normas en materia de protección de datos, produciéndose importantes avances desde el punto de vista de protección de este derecho fundamental en la región.

Y es que, en un mundo globalizado, en el que la movilidad, no solo geográfica, sino también económica y profesional juega un papel tan relevante, el tratamiento de los flujos constantes de información han de someterse a los cánones internacionales y a la legislación propia de cada Estado, en aras de proteger la intimidad de sus ciudadanos, garantizando su privacidad y la protección de su información.

Una cuestión fundamental cuya relevancia ha sido puesta de manifiesto por la propia OEA, que en el 86º período ordinario de sesiones a través del Comité Jurídico Interamericano adoptaba por consenso el informe sobre "Protección de Datos Personales". En el mismo sentido, cabe reseñar los avances de la Red Iberoamericana de Protección de Datos, que busca crear un foro integrador que permita involucrar a diversos actores sociales, tanto del sector público como privado.

Iberoamérica avanza en la legislación de un derecho fundamental inherente a las personas, dando pasos hacia un marco jurídico común que cree un espacio de seguridad jurídica, tanto en el ámbito empresarial y las transacciones económicas y de servicios, como de la libre circulación de las personas y sus relaciones más allá de su espacio cotidiano, donde Internet juega un papel fundamental y los datos se propagan a gran velocidad por las redes sociales.

Es en este punto donde desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, mediante los aportes de los diferentes colaboradores y la puesta en común de conocimientos y experiencias, se plantean los retos a abordar para una protección efectiva de este derecho, de tanta relevancia y en ocasiones desconocido, abordando cuestiones como la necesidad de unificar criterios normativos, la protección de los menores, educación, delitos informáticos y la protección de los datos desde el punto de vista penal, interacciones con el comercio electrónico, los tratamientos Big Data, la adopción de medidas de seguridad y la generación de un Sello Iberoamericano que aporte la seguridad jurídica necesaria a personas, empresas e instituciones.

Las próximas páginas nacen del esfuerzo y experiencia de los diferentes colaboradores de la iniciativa, desde el compromiso y el convencimiento de que es posible avanzar en esta protección y de los beneficios que este avance puede conllevar para la región.

PRÓLOGO

CUANDO PROTEGEMOS DATOS PROTEGEMOS PERSONAS

Eduardo Peduto
Director del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires / Argentina

Más de una vez hemos sostenido que con el tema de protección de datos personales nos hallamos frente a un derecho novedoso. Y utilizamos este adjetivo en dos de sus acepciones: una de ellas, la más extendida, la que refiere a la cualidad de nuevo; la segunda, menos utilizada en el lenguaje coloquial, es el adjetivo aplicado a aquello que antes no fue visto ni oído y que causa, en consecuencia, extrañeza o admiración. No creemos equivocarnos al utilizar la voz "novedoso" en esta doble vertiente.

Vamos a intentar validar su uso en el último sentido. Si bien progresivamente se va extendiendo el conocimiento del tema de la protección de datos personales que en la jerga jurídica es conocido bajo el latinazgo de "hábeas data" y, en tal carácter, su divulgación es aún más restringida socialmente, lo cierto es que como derecho no ha adquirido la suficiente entidad o, al menos, la entidad que poseen algunos otros derechos vinculados a las personas.

También debemos convenir que el conocimiento alcanzado en la comunidad sobre este derecho se halla más vinculado a cuestiones crediticias, patrimoniales o comerciales que a otros campos de los datos personales. Y bajo este genérico "otros campos" estamos englobando a los denominados datos sensibles. Y en definitiva, ¿cuáles son los datos que responden a esta categoría? Todos aquellos que revelen o puedan revelar origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual. En la Ciudad Autónoma de Buenos Aires, de donde somos autoridad de protección, el legislador, de manera aguda y proyectiva, le ha hecho un aditamento a esta enumeración: "o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos".

Respecto a este último tópico debemos decir que –sin llegar a configurar un campo impreciso e infinito– son múltiples los terrenos o figuras que encuadran en esta definición. Van desde aquel que, buscando trabajo, queda fuera de la oferta por vivir en un barrio carenciado o en una villa miseria, hasta los padres que reciben un subsidio por la discapacidad de un hijo o los que, por su situación de necesidad extrema, integran la nómina de algún plan de reinclusión social.

En definitiva, todas aquellas personas que, por una razón o por otra, se encuentran estigmatizadas por un imaginario social construido sobre prejuicios y descalificaciones. Y en

esto nos vemos obligados a hacer mención de las herramientas utilizadas para incursionar en el terreno del daño al otro.

Es así que un campo en el que vemos frecuentemente la aparición de conductas que conllevan trato discriminatorio, humillante o descalificador es el del mundo cibernético. Aquello que de manera englobante (bajo la forma de mensajes a móviles, correos electrónicos, foros, chats de Internet o redes sociales como Facebook) se conoce como acoso cibernético o ciberacoso y que se plasma en el envío y difusión de cierta información agraviante para alguien, ocultándose tras el anonimato o la posibilidad de construir un perfil falso que Internet les confiere. Es lamentablemente conocido el caso de personas que sometidas a este acoso durante largo tiempo han sufrido depresiones agudas, llegado al suicidio o, en un estallido de violencia, han atacado de manera indiscriminada a quienes suponían como sus agresores dado que el anonimato le impedía acceder a la fuente de su sufrimiento.

Finalmente, haremos referencia a una de las formas específicas del acoso cibernético: el conocido bajo el nombre de "grooming". Consiste en un accionar preparatorio para la comisión de delitos de agresión sexual más graves aún. La utilización de las Tecnologías de Información y Comunicación (TIC) permite a un adulto, mediante la utilización de un perfil falso, acceder a un menor de edad y mediante engaños crear una conexión emocional, siempre con el objetivo de llevar adelante un abuso de tipo sexual.

Es así que llegamos al comienzo o –más que a él– al título de estas líneas: cuando protegemos datos protegemos personas. Esta es la esencia de nuestra acción tanto en la divulgación, capacitación, investigación o cuando receptamos denuncias sobre la vulneración de datos personales. Hacer hincapié, nunca suficiente nunca vasto, que cuando nos abocamos a la protección de datos personales estamos protegiendo personas. Estamos protegiendo su intimidad, su privacidad, su dignidad. Su ciudadanía, entendida ésta en el sentido amplio en que hoy es reconocida por el desarrollo de las ciencias sociales. En definitiva, estamos protegiendo su mayor atributo: su condición de ser humano.

Por ello que en este desafío que se nos presenta a diario, los esfuerzos mancomunados son clave para su solución. Así, apoyamos la publicación de las "Declaraciones de la Iniciativa del Observatorio Iberoamericano de Protección de Datos" y promovemos el trabajo en redes que, sin lugar a dudas, darán sus frutos.

AVANCE Y ARMONIZACIÓN EN LA PROTECCIÓN DE LOS DATOS

MSc. Mauricio Garro Guillén
Director Nacional de la Agencia de Protección de Datos de los Habitantes / Costa Rica

La Protección de Datos Personales se ha constituido en un verdadero paradigma de nuestro tiempo. La fórmula del derecho a la intimidad perpetrada en el ámbito del Derecho Continental desde la génesis de las instituciones jurídicas romanas, calibró a lo largo de los siglos los límites y alcances de esa esfera de espacio privativo o inexorable, donde la libertad individual no puede ser invadida por terceros incluyendo al propio Estado.

Reconocido como Derecho Fundamental a través de innumerables instrumentos internacionales, forma parte inequívoca de toda norma constitucional en el mundo occidental, y es una garantía necesaria para el desarrollo de todas las libertades atinentes al ser humano.

A partir de ello, el camino del desarrollo histórico nos confronta con la evolución de las tecnologías de la comunicación y la información, siendo que el denominado "Right to Privacy" recibe un tratamiento similar en el ámbito del Common Law, es a inicios de la década de los setenta, durante el siglo pasado, que en los Estados Unidos de América comienzan a diseñarse los primeros rasgos del sistema de Protección de Datos Personales (Privacy); y es allí, particularmente en el Estado de California, donde nace el principio del "Data Breach Notification" o Vulnerabilidad de la Seguridad obligando a todo responsable de base de datos a informar a cada titular de datos personales cuando los mismos se han visto comprometidos, o bien se presuma que hayan podido verse comprometidos. En el transcurso del tiempo y a inicios de los años ochenta se promulga en el ámbito europeo la Convención número 108 Para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, hasta la fecha, el único instrumento internacional de esa naturaleza que existe.

Los años 90 ven el florecimiento de las legislaciones europeas en materia de protección de Datos Personales y la proliferación de las autoridades reguladoras en el entorno. La explosión de las redes sociales, el Big Data y el Internet de las Cosas ha provocado la masificación descontrolada, si se quiere, de la recopilación y tratamiento de Datos Personales.

La escasez de controles de seguridad eficientes, el ritmo trepidante con el que evolucionan y se renuevan las tecnologías, y los entornos legales débiles e incluso facilistas, han puesto a prueba la capacidad de respuesta tanto por parte del sector gubernamental como del empresarial. La reciente anulación del convenio del "Safe Harbor" y subsecuente aparición del denominado "Privacy Shield", son muestra de intensas diferencias en materia de las garantías que se deben salvaguardar desde la perspectiva del Common Law versus el Derecho Continental.

Así, el primero ha tendido a concentrarse más en materias como la defensa al consumidor y los productos financieros; mientras el segundo, verbigracia de la concepción nativa del Estado de Bienestar, tiende a conceptualizar un marco de defensas mucho más extenso, al punto de concebir a la propia Protección de Datos Personales como un Derecho Fundamental.

Envuelta en este mar de luchas conceptuales se encuentra nuestra región, Latinoamérica cada vez va dando pasos más firmes en el desarrollo de legislaciones y creación de autoridades reguladoras de la Protección de Datos.

Sin embargo, y a pesar de los fuertes vínculos culturales que nos unen, no son pocas las diferencias de percepción y consecuente aproximación al tratamiento de temas como el que nos atiende. Es ahí donde debemos hacer un esfuerzo por armonizar los límites y alcances de la Protección de Datos, no solo a nivel conceptual, pero incluso desde la perspectiva de la actividad procesal con la cual, las diferentes autoridades reguladoras tienen la potestad de resolver las garantías previstas en cada legislación. Temas de vital importancia, como la Transferencia Transfronteriza de Datos, deben ser abordados desde una perspectiva común y de mutuo beneficio para todos los países de la América Latina.

Es ahí donde el trabajo del Observatorio Iberoamericano de Protección de Datos cobra especial relevancia, como puente de comunicación entre los países del área, y las Declaraciones que aquí se incluyen son un esfuerzo de incalculable valor en el trabajo de crear ese sentido de unidad en la dirección, que nos permitirá desarrollar verdaderos criterios regionales de rigor necesarios en el contexto de un mundo globalizado.

LA INICIATIVA DEL OBSERVATORIO IBEROAMERICANO DE PROTECCIÓN DE DATOS

El Observatorio es una iniciativa cuya principal finalidad es extender la cultura de la privacidad y protección de datos en los distintos países, favoreciendo el conocimiento de la legislación y jurisprudencia existente al respecto, los derechos y las acciones que les asisten a sus ciudadanos, tratando de promover un clima de seguridad jurídica en el tratamiento de los datos de carácter personal que contribuya al desarrollo de las ciencias jurídicas en Iberoamérica.

Los contenidos del Observatorio son fruto del aprendizaje y la práctica diaria de los juristas, abogados, catedráticos, jueces y fiscales que participan en esta iniciativa colaborativa remitiendo desinteresadamente sus artículos y participando en sus diferentes Declaraciones y eventos organizados en el seno de la iniciativa, con la intención de lograr un mayor conocimiento de esta rama del derecho, tan fundamental y en ocasiones desconocida, no solo en la comunidad jurídica internacional, sino entre la propia ciudadanía.

La iniciativa nace en enero de 2013 como un foro de encuentro donde poder compartir experiencias e ideas en el ámbito jurídico y operacional de la privacidad y la protección de datos, sobre las diferentes normativas iberoamericanas y su aplicación.

En su primer año, se presentan las primeras Declaraciones de la iniciativa en Lima, Barranquilla (presentada por el juez de Control Constitucional Alexander Díaz García, autor de la Ley colombiana de delitos informáticos), Buenos Aires (presentada por Eduardo Peduto, director del Centro de Protección de Datos de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires), Santiago de Chile (presentada por Pedro Huichalaf Roa, actual Subsecretario de Telecomunicaciones del Gobierno de Chile, en el Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile) y La Plata (presentada en la Universidad de La Plata).

Durante 2014 siguen sumándose colaboradores y ampliándose el número de países que participan. Se presenta la Declaración de Riobamba (presentada en la Universidad de Chimborazo en el transcurso de la inauguración del Curso de Formación y Especialización para Peritos Profesionales en Ecuador).

En julio de 2014 se presenta la Declaración de Ciudad de Panamá, hacia la unificación de criterios y garantías para la protección de la identidad digital y el derecho al olvido, en el Colegio Nacional de Abogados de Panamá por su Presidente. En agosto del mismo año, se presenta la Declaración de México D.F., hacia la implantación de garantías para la privacidad en los tratamientos de Big Data, en el transcurso de la Jornada académica de protección de datos personales en Internet, dentro de la bienvenida para los alumnos de la cuarta generación

de la Maestría en Derecho de las Tecnologías de la Información y Comunicación de INFOTEC, en la ciudad de México Distrito Federal.

Durante ese año comienza a funcionar la iniciativa "Semillero de privacidad" en el seno del Observatorio Iberoamericano de Protección de Datos, como forma de extender la cultura de protección de datos a los centros universitarios de Iberoamérica, uniéndose a la misma la Universidad Central de Venezuela.

En enero de 2015 diferentes colaboradores de la iniciativa son premiados por la Agencia Española de Protección de Datos por su trabajo de investigación sobre protección de datos y habeas data en Iberoamérica, aglutinando el Observatorio más de 25 premios nacionales de protección de datos en las diferentes ediciones de los prestigiosos Premios de la Agencia.

El pasado 15 de marzo de 2016 se presentó la novena Declaración en San José (Costa Rica) en el transcurso del II Privacy Data Protection Forum. En esta ocasión fue abordada la implantación de un Sello sobre el tratamiento de datos personales en Iberoamérica, corriendo su presentación a cargo de Daniel López Carballo (director del Observatorio Iberoamericano de Protección de Datos) y Mauricio París (coordinador de la iniciativa en Costa Rica).

La iniciativa pretende desarrollarse en tres líneas maestras: facilitar información en materia de protección de datos a los visitantes de la web, sobre las diferentes instituciones, legislaciones, jurisprudencia e informes relevantes en los diferentes países; desde la iniciativa se presenta una base de datos detallada sobre privacidad, protección de datos y habeas data, que se complemente con otra información de interés.

La segunda línea pretende fomentar la cultura de la privacidad y su conocimiento en las diferentes facetas que abarca, mediante la difusión de artículos de interés elaborados por los colaboradores de la iniciativa.

En tercer lugar, se han desarrollado acciones colaborativas, como son las Declaraciones, donde se avanza en la unificación de criterios y recomendaciones a los diferentes países, instituciones, empresas, organizaciones y personas para un correcto tratamiento de los datos.

Actualmente, la iniciativa cuenta con más de 110 colaboradores de reconocido prestigio (jueces, fiscales, catedráticos, ingenieros, abogados, entre otros) de veintidós nacionalidades, desarrollándose su actividad principal a través de la página web del Observatorio **(www.oiprodat.com)**.

DECLARACIÓN DE LIMA, HACIA LA UNIFICACIÓN DE CRITERIOS NORMATIVOS SOBRE PROTECCIÓN DE DATOS Y PRIVACIDAD EN IBEROAMÉRICA[1]

El Derecho Constitucional en Iberoamérica ampara y establece las garantías y mecanismos para la defensa y promoción de la protección de datos personales. Los Estados democráticos se basan en los principios de soberanía popular, representación ciudadana, independencia de poderes, protección y promoción de los derechos civiles y políticos, económicos, sociales y culturales.

El derecho de las personas sobre la protección de sus datos, íntimamente ligado al ámbito del derecho a la intimidad, al honor y a la propia imagen, se encuentra regulado en la mayor parte de las legislaciones iberoamericanas en el marco del llamado "habeas data", como garantía constitucional. Cada vez son más los Estados que cuentan con normas específicas en materia de protección de datos, adaptando el resto de leyes, decretos y otra normativa para una mejor salvaguarda de los derechos de las personas, así como su tutela judicial efectiva.

En un mundo globalizado, en el que la movilidad, no solo geográfica, si no también económica, profesional, bancaria, juega un papel tan importante, las transferencias internacionales de datos, físicamente o a través de la propia red, la implantación de las empresas en diferentes países, así como la propia movilidad de las personas, implican un flujo constante de información que debe someterse a los cánones internacionales y la legislación propia de cada Estado, en aras de proteger la intimidad de las personas, garantizando su privacidad y la protección de su información.

La protección de los datos de las personas es un derecho fundamental reconocido por las Naciones Unidas que protege la libertad individual, la libertad de expresión, la intimidad y la dignidad personal.

El Consejo de Europa define el derecho a la privacidad como un derecho humano fundamental; la propia Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la privacidad como un derecho: "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación", por lo que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

1. La Declaración de Lima, hacia la unificación de criterios normativos sobre protección de datos y privacidad en Iberoamérica, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, presentada en la ciudad de Lima (Perú), el 12 de abril de 2013, por el Catedrático José Reynaldo López Viera, en el transcurso de las Jornadas de Derecho Constitucional. En la elaboración de la Declaración intervinieron Emilio Suñé Llinas, José Reynaldo López Viera, Ines Tornabene, Óscar Costa Román, Marta Sánchez Valdeón, Andrés Blázquez García, Francisco Ramón González-Calero Manzanares, Romina Florencia Cabrera, Camilo Alfonso Escobar Mora, José María Fernández-Varela Villamor y Damián Armijo Álvarez, coordinados por Daniel López Carballo.

Este derecho debe cubrir todos los aspectos de la vida del individuo, así como el tratamiento de sus datos personales por organizaciones públicas y privadas. Solo mediante una correcta información y formación de las personas se pueden prevenir utilizaciones delictivas de su información y el daño que ello conlleva al individuo y su entorno.

Los ciudadanos tienen derecho a conocer la legalidad en la recopilación de sus datos, quedando estos habilitados para, en caso de haberse recabado de forma ilegal, solicitar la correspondiente sanción a los responsables, aumentando el nivel de transparencia en el acceso a la información, así como el tratamiento y personas o entidades que acceden o son cesionarios de la misma.

La diferentes Constituciones iberoamericanas reconocen dicho derecho fundamental, recogiendo que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. Cada vez son más los países iberoamericanos que cuentan con una legislación específica en materia de protección de datos, así como de medios legales y organizativos para proteger el derecho a la privacidad y al honor de los ciudadanos.

El marco regulatorio en Iberoamérica ha avanzado mucho en los últimos años, tanto a nivel nacional como interno en cada país. Pero este avance no se ha visto acompañado aún por un crecimiento de los organismos nacionales y locales que sean autoridad en materia de protección de datos personales. Y tampoco se ve aún un posicionamiento importante de la temática en las agendas políticas. El trabajo de las autoridades existentes, de los organismos no gubernamentales, de los académicos y de todos los interesados debe dirigirse y focalizarse a la concientización en materia de protección de los datos personales, del cuidado de la ciberseguridad y de un verdadero trabajo en red e interrelacionado donde se coordinen políticas y gestiones que den por resultado un verdadero trabajo internacional en una temática que ya no admite fronteras.

Se debe dotar a las instituciones y al propio ciudadano de mecanismos y acciones para la protección de la información, que garanticen tanto el control de la seguridad y la correcta obtención y tratamiento de los datos, como el ejercicio del derecho de acceso a la información, de rectificarla o corregirla, de cancelarla o requerir la supresión de la información y el oponerse a un determinado tratamiento de los datos por parte de las personas, garantizando el principio de autodeterminación informativa.

En un mundo globalizado donde la información es tratada en diferentes Estados por multitud de personas, las acciones deben ser comunes y la persecución de las irregularidades y vulneraciones de las garantías constitucionales debe contar con la acción conjunta de la comunidad iberoamericana y sus socios estratégicos.

Debe progresarse hacia un marco jurídico común que cree un espacio de seguridad jurídica tanto en el ámbito empresarial y de las transacciones económicas y de servicios, como de la libre circulación de las personas y sus relaciones más allá de su espacio cotidiano, donde Internet juega un papel fundamental y los datos se propagan a gran velocidad por las redes sociales.

Solo mediante la cimentación del ordenamiento jurídico sobre unos principios generales, dúctiles y transversales, disminuyendo la incertidumbre de los ciudadanos y aportando claridad en la interpretación y en la aplicación del derecho a la protección de los datos personales, tomando como base el derecho sustantivo y procesal preexistente en Iberoamérica, desde el más profundo respeto a las bases constitucionales, que son garantía de la libertad y estado de derecho.

El avance de las nuevas tecnologías y la creación de espacios supranacionales en el ámbito de Internet conllevan la aparición de nuevas figuras jurídicas, y favorecen el desarrollo personal de los ciudadanos y el acceso a la información. La utilización de las mismas en ámbitos como el educativo deben llevar implícita una formación de las personas en materia de privacidad, un mayor conocimiento de sus derechos y obligaciones y una mayor formación que conlleve una protección de su intimidad.

La correcta utilización de las redes sociales y los medios de comunicación debe garantizar la protección de aquellos más vulnerables, en la educación de dichos valores deben intervenir, no solo la propia familia, sino también instituciones educativas y la propia Administración. La prevención de abusos en materia de protección de datos y una correcta formación evitan la vulneración de los derechos fundamentales de la persona y la consecución de delitos.

Es necesaria una formación y capacitación en las tecnologías de la información y la comunicación en todos los sectores laborales, pero con especial importancia en el de la educación, ya que de esta forma se conseguirá una rápida adaptación y concienciación por parte de toda la sociedad a las nuevas herramientas que se han desarrollado en las últimas décadas, ya que es obligación de los educadores la transmisión de sus conocimientos.

La legislación debe adaptarse a los nuevos tiempos, regulando nuevas figuras delictivas que atentan contra la intimidad y la seguridad jurídica de las personas. Los Estados deben facilitar mecanismos, formales y materiales, para una correcta protección de los ciudadanos, más allá de sus fronteras o de las nacionalidades de los mismos.

La información y la divulgación de los derechos de las personas en materia de protección de datos debe ser una prioridad de las instituciones nacionales, desde la infancia hasta la madurez, educar en valores, tanto para protección de la propia intimidad, como la de los demás ciudadanos.

El derecho a la intimidad debe ser un compromiso de todos. La denuncia de situaciones de ilegalidad o vulneraciones de la privacidad, la adopción de medidas de seguridad, no solo en el ámbito empresarial, y la adaptación a la realidad, a los nuevos medios y canales de comunicación existentes, debe ser una prioridad legislativa y social.

Las legislaciones nacionales deben avanzar hacia la adopción de estándares comunes de seguridad, por lo que se debe seguir el camino normativo que conlleve a una legislación común, homogeneizada en la materia, mediante la instauración de instituciones nacionales, órganos de control específicos, con potestades de intervención inmediata, que deberán tener garantías de independencia e imparcialidad, que vigilen por el correcto funcionamiento de los mecanismos constitucionales y un sistema de sanciones común.

Los Estados deben establecer modelos de seguridad que faciliten las transferencias de datos en condiciones óptimas, salvaguardando los principios de integridad y confidencialidad de la información. La cooperación internacional, no solo desde Iberoamérica sino con otros Estados y la propia Unión Europea debe ser un pilar clave en la función legislativa y las acciones de los organismos encargados de supervisar el cumplimiento de la ley.

Solo mediante la adopción de estos criterios normativos comunes, basados en principios jurídicos claros y del compromiso decidido de los Estados, sus instituciones y de los propios ciudadanos, se podrá garantizar una correcta protección de la intimidad, el derecho al honor y la privacidad de las personas, así como la protección de sus datos personales

DECLARACIÓN DE BARRANQUILLA, HACIA LA UNIFICACIÓN DE INSTRUMENTOS PARA LA PROTECCIÓN DE LA PRIVACIDAD EN IBEROAMÉRICA[2]

Los avances de las tecnologías de la información y la comunicación han cambiado radicalmente nuestro día a día tanto a nivel personal como a nivel profesional. Son muchas las ventajas y utilidades que nos aportan, pero como toda herramienta usada por el ser humano, también es susceptible de ser utilizada con fines ilícitos de toda clase, delitos electrónicos que tienen su razón de ser a través de la red, así como cualquier tipo de delito informático, relacionado con la información y los datos.

Diariamente conocemos casos de amenazas a través de virus o programas informáticos dañinos (malware) que circulan libremente por Internet instalándose en nuestros dispositivos.

Unas veces tratan de provocar daños en los equipos y redes informáticas, otras veces tratan de robarnos información o espiarnos (Spyware). Estas mismas amenazas se reproducen por ataques dirigidos por humanos (hackers) que los realizan con idénticas finalidades. Las motivaciones y finalidades de estos actos delictivos pueden ser tantas como autores las lleven a cabo, puesto que en algunos casos será para obtener información para vender, plagiar o chantajear, y en otros casos será para satisfacer un mero ego "intelectual".

De la misma manera, los delitos tradicionales han encontrado en las nuevas tecnologías una vía de ampliar el número de actos delictivos o simplemente quedar amparados en un supuesto "anonimato". Las tradicionales estafas y suplantaciones de identidad han encontrado nuevas variables como el phishing. La obtención de material sexual de menores llegando incluso al acoso o abuso sexual (grooming) ha encontrado un terreno propicio, ya que a través del correo electrónico, mensajería instantánea o redes sociales se puede contactar con los mismos induciendo al error por medio de perfiles falsos y, lo que resulta más preocupante, sin que pueda llegar a percatarse un adulto. Tampoco hay que olvidar que estas tecnologías también facilitan el intercambio de material sexual de menores por parte de los pederastas. Pese a ser los mismos delitos, la cantidad de víctimas potenciales es peligrosamente mayor, por la facilidad en el acceso a las mismas y la posibilidad de mantenerse, el delincuente, en el anonimato.

2. La Declaración de Barranquilla, hacia la unificación de instrumentos para la protección de la privacidad en Iberoamérica, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en la ciudad de Barranquilla (Colombia) el 1 de junio de 2013, por Alexander Díaz García, en el transcurso del Congreso en Seguridad Informática y Telecomunicaciones. En la elaboración de la Declaración intervinieron Alexander García Díaz, Francisco Ramón González-Calero Manzanares, Marta Sánchez Valdeón, Andrés Blázquez García, Javier Villegas Flores, Romina Florencia Cabrera, Óscar Costa Román, Camilo Alfonso Escobar Mora, Carlos Vera Quintana, Iván Darío Marrugo Jiménez, Analía Aspis, Ines Tornabene y Edgar Tomas Quiñonez Ríos, coordinados por Daniel López Carballo.

Igualmente, otros tipos delictivos han comenzado a cometerse a través de las nuevas tecnologías. Amparados en un "falso anonimato" y una falsa creencia de "impunidad", comienzan a proliferar los delitos de calumnias, injurias o revelación de secretos en sistemas de mensajería instantánea, foros o redes sociales, con una difusión y repercusión mediática antes desconocida, al igual que la amenaza o chantaje de difusión de material sexual (sextortion) que previamente había sido compartido (sexting). Otra modalidad de nueva creación es el acoso entre menores utilizando estas tecnologías (ciberbullying), que lamentablemente en algunas ocasiones ha acabado de forma trágica con un fatal desenlace. También el denominado espionaje industrial y robo de carteras de clientes encuentran en estas tecnologías posibilidades antes desconocidas.

Otra particularidad de este tipo de delitos es su repercusión y perdurabilidad en el tiempo. Además de los sistemas de mensajería instantánea que permiten los envíos masivos, la difusión por estos medios es universal y, con la llegada de los buscadores la información es fácilmente localizable y puede permanecer accesible de por vida, sin posibilidad de control por parte del afectado.

También se multiplican los daños causados, puesto que se pueden multiplicar los afectados, no solo porque con un solo click se llegue a multitud de destinatarios, sino porque además los daños pueden paralizar a una empresa, organismo público, infraestructura o servicio crítico.

Todas estas situaciones se ven afectadas por un componente de internacionalidad que va ligado intrínsecamente a las nuevas tecnologías. Información, medios tecnológicos y actores pueden encontrarse en ubicaciones muy diferentes y verse afectados por legislaciones distintas, la información puede ser almacenada o reproducida desde cualquier parte del mundo.

A esta circunstancia podemos sumarle la aplicación extrajurisdiccional de las leyes. En efecto, las empresas que explotan las redes sociales establecen sus propias políticas de uso y de privacidad, que son aceptadas por los usuarios como una adhesión, sin posibilidad de modificarlas. Y una de las principales consecuencias de esta adhesión es la aceptación de la ley que se aplica en caso de controversias con, por ejemplo, los datos personales. Un usuario de cualquier parte del mundo si quiere litigar contra alguno de los principales buscadores o redes sociales debe enderezar su litigio en el país de origen de estas empresas, sin perjuicio que los efectos de la actividad se produzcan en su país o en otros países.

Más compleja aún resultará la prueba de estos delitos, las más que polémicas "evidencias electrónicas", aquellos datos que de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática.

Las legislaciones e instrumentos jurídicos de los Estados deberán atender a los principios de la International Organization on Computer Evidence, sobre la adquisición y el tratamiento de la

evidencia electrónica, garantizando su veracidad, integridad y correcto tratamiento de forma segura. Ante este panorama, las medidas de respuesta por parte de los poderes públicos deben ser tan novedosas e innovadoras como lo son estas tecnologías; la Administración, su funcionamiento, las normas y el Poder Judicial deben adaptarse a los nuevos tiempos.

Los ordenamientos jurídicos de los países iberoamericanos deben contemplar nuevos tipos penales y establecer mecanismos de defensa de los derechos de las personas sobre su propia información, garantizando el derecho al honor y la intimidad, articulando y dotando de medios a la instituciones, generando información accesible y concienciando a los ciudadanos sobre sus derechos y cómo denunciar conductas ilegales.

Igualmente, la tendencia internacional deberá de pasar por armonizar los conceptos relacionados con este tipo de delitos, pues, si bien en la mayoría de las legislaciones nacionales existe protección, aún hay grandes diferencias conceptuales, desde los países que crean un nuevo bien jurídico tutelado "De la Protección de la información y de los datos" (Colombia), pasando por aquellos que determinan como bien jurídico "la protección de los sistemas informáticos"(Venezuela), terminando por aquellos países europeos en los que no existe diferenciación entre "delitos electrónicos" y "delitos informáticos". La unificación de criterios normativos en los diferentes países, su tipificación y las penas parejas deben ser prioridad legislativa en el ámbito internacional.

La cooperación y coordinación entre Estados y organizaciones internacionales debe ser un pilar básico, las tecnologías no reconocen fronteras. Las organizaciones iberoamericanas e internacionales deben establecer puentes de colaboración entre Estados, instituciones, empresas y particulares. Solo un compromiso de los actores implicados y una homogenización de criterios, normas y consecuencias pueden erradicar las situaciones de ilegalidad y vulneración de derechos.

Se debe dotar de medios a las instituciones que ya existen y se deberá avanzar en cuerpos de seguridad ultra nacionales, entendida como unidad especializada cuyo objetivo sería la prevención y el combate de los delitos electrónicos e informáticos encargados de establecer estrategias y de diseñar mecanismos que contrarresten los efectos de las conductas delictivas surgidas del Internet, junto a una clara cooperación de las fuerzas de seguridad nacionales. La definición internacional clara del concepto de ciberdelito debe ser materia a abordar por los foros internacionales.

Los Estados deben avanzar en el fortalecimiento de las "redes de alerta temprana", reforzando la información temprana sobre amenazas, en tiempo real por los instituciones, empresas y los ciudadanos que utilizan estas tecnologías.

Las nuevas formas de transmisión de datos posibilitados a través de redes informáticas y electrónicas tales como los sistemas inalámbricos, dispositivos de geolocalización, sistemas de radiofrecuencia y sensores deberán ser temas prioritarios para el desarrollo de estudios e investigación a fin de conocer y prevenir las nuevas formas de procesamiento de datos.

Los Estados deben armonizar sus normativas, evitando la creación de "paraísos cibernéticos" a través de los cuales los ciberdelincuentes puedan actuar impunemente. Para ello, se deben clarificar las reglas sobre competencia judicial, legislación aplicable y reconocimiento, así como la ejecución de resoluciones judiciales o administrativas, en aras de evitar lagunas legales que puedan favorecer estas conductas delictivas, con independencia del lugar donde se cometan dichas conductas, protegiendo la intimidad y la información de las personas.

Se deben reforzar los mecanismos de auxilio judicial y colaboración administrativa, intercambio de información y reconocimiento y ejecución de sentencias, sentencias en el marco de la Convención (NU) de Nueva York de 1958 relativa al reconocimiento y ejecución de laudos y sentencias judiciales, y actos administrativos entre Estados y entre estos y sus empresas y ciudadanos, de manera que una decisión judicial o administrativa en otro Estado se acabe ejecutando, aunque el autor o "arma del delito" se encuentren ubicados en otro.

Particularmente se deben facilitar mecanismos inmediatos, sencillos y universales para la tutela de los derechos de los usuarios, de manera que se minimicen los daños que puedan provocar en las "víctimas" la expansión viral, incontrolada y universal que posibilita las nuevas tecnologías. Para ello han de articularse instrumentos de colaboración con los distintos agentes intervinientes, muy especialmente con los prestadores de servicios de comunicaciones electrónicas, prestadores de servicios de intermediación y proveedores de contenidos; reforzar los mecanismos de identificación de los usuarios de las TIC ante la posible comisión de ilícitos, siempre de manera proporcionada y adecuada a los distintos escenarios posibles, procurando evitar así que el anonimato sirva como amparo y paraguas para la comisión de este tipo de actos, y siempre garantizando la protección del derecho a la intimidad del usuario.

Los tipos penales y las infracciones administrativas deben ser claros, correspondiendo al Poder Legislativo de cada uno de los Estados el ser dinámicos ante unas amenazas en proceso de continuo cambio; con el objeto de evitar que unos hechos puedan quedar sin sanción por falta de cobertura legal, el derecho debe adaptarse a los tiempos actuales y ser dinámico.

Los Estados y organizaciones internacionales deberán tener en sus plantillas, personal suficientemente formado para combatir estas amenazas y asistir a las víctimas (jueces, fiscales, unidades especiales de policía informática, expertos en hacking ético y ciberseguridad, asistentes sociales, profesores, psicólogos), en la protección de la privacidad, de los datos y la información; se deben contar con medios humanos y tecnológicos, asignando eficientemente recursos a la protección de las personas.

Los poderes públicos en colaboración con la sociedad civil deben realizar campañas de concienciación sobre ciber-amenazas en diferentes ámbitos sectoriales. Solo mediante una formación de menores, padres o tutores, profesores y la ciudadanía en general se pueden prevenir situaciones de riesgo. La seguridad de la información y la privacidad, la protección de los datos debe empezar por uno mismo, educando a los menores en una sociedad tecnológica, en la que las relaciones encuentran un nuevo medio de desarrollo, las redes sociales e Internet.

Asimismo, se debe promover una alfabetización digital, con especial hincapié en la privacidad y la protección de datos entre los "inmigrantes digitales", ya que habiendo nacido en un mundo anterior a la era de las TIC se han visto obligados a introducirse en este ámbito. De esta forma, consideramos como un punto vital la formación a lo largo de la vida para reciclar los conocimientos y fortalecer diferentes conductas y actitudes que aseguren la máxima privacidad de los individuos.

Los Estados en colaboración conjunta deben llevar adelante políticas educativas y de prevención que tengan como finalidad la reducción de la brecha digital en materia de datos personales y protección de la privacidad, no solo en el uso de los computadores portátiles sino también en las nuevas tecnologías que involucren –directa o indirectamente– la posibilidad de tratamiento de datos.

Se debe concienciar a las empresas sobre buenas prácticas en la salida al mercado de sus productos. Las empresas deben procurar que sus productos o servicios cumplan unos estándares mínimos en seguridad y privacidad, dejando la posibilidad al consumidor de optar por la configuración que desea implantar, garantizando la seguridad de sus datos.

En este sentido, en relación a la responsabilidad que las empresas y organizaciones tienen sobre la información y datos personales que tratan, se deberá apostar por un modelo de privacidad empresarial y corporativo, incorporando responsables de privacidad a la toma de decisiones, elaborando informes de impacto y tomando las medidas técnicas y organizativas necesarias para garantizar la privacidad y derechos de las personas.

Los Estados iberoamericanos, las organizaciones internacionales y empresas, deben invertir en Programas de I+D+I, que doten de contenido económico el estudio e implantación de estas medidas. Se deben habilitar partidas presupuestarias tanto en las empresas como en los poderes públicos, así como establecer los correspondientes beneficios fiscales para las empresas que pongan en marcha estos programas.

La transnacionalidad y universalidad de estas tecnologías requieren la urgente armonización internacional del "derecho al olvido". De no ser así, numerosos casos pueden recibir una respuesta estimatoria de los juzgados y tribunales, o incluso una persecución por parte de los órganos de la Administración cuando no exista tipo penal y sí infracción administrativa, y quedar en papel mojado al encontrarse el causante del perjuicio o su infraestructura

tecnológica ubicados en un país que no sea sensible al derecho de toda persona a poder borrar la información que le sea desfavorable o que simplemente, no desee compartir cuando una ley no obligue a su publicación o mantenimiento.

Junto con la armonización e internacionalización de las normas de los Estados, se debe avanzar en la capacitación de las personas, empresas e instituciones, sobre la utilización correcta de las herramientas informáticas. En un mundo tecnológico e interconectado, la educación y formación desde la infancia constituyen un valor necesario para la prevención de conductas delictivas y la correcta privacidad de los usuarios.

La libertad de expresión en los nuevos medios de comunicación debe asegurar los derechos fundamentales de la persona a la intimidad, al honor, a su privacidad y a la protección de sus datos personales. Las normas jurídicas, equilibradas y sociales, deben proteger esos principios fundamentales recogidos en las diferentes Constituciones nacionales de los Estados iberoamericanos.

El hombre es un ser libre que goza de su libre albedrío en la sociedad democrática; tal como es concebida, se debe procurar que la tecnología contribuya a su desarrollo, y le permita gozar más de su vida personal, expresarse, crear y disfrutar del ocio, sin ser esclavo de ella. Se deben utilizar las herramientas informáticas y nuevos canales de comunicación para mejorar la calidad de vida y los avances científicos; no para ser dominado por las mismas. La seguridad de la información, la protección de la privacidad debe ser un compromiso de todos: los usuarios, las empresas e instituciones y los propios Estados y organizaciones internacionales.

Por ello, desde la iniciativa del Observatorio Iberoamericano de Protección de Datos se hace un llamado a la comunidad general y en particular a los diferentes Estados iberoamericanos a que se fortalezcan decididamente los mecanismos de protección en materia de datos personales y seguridad de la información, adoptando medidas urgentes para contrarrestar los efectos del fenómeno criminal internacional. Estas medidas deberán incluir, sin limitarse a ello, redes de alertas tempranas en materia de delitos transnacionales, armonización de reglas de tratamiento de datos personales, adopción de mecanismos eficaces en materia judicial y administrativa internacional, programas de sensibilización y adopción de currículos académicos en protección de datos, seguridad de la información y delitos informáticos, así como programas de formación en la materia como elemento de prevención de conductas ilícitas con la información personal.

DECLARACIÓN DE BUENOS AIRES, HACIA LA UNIFICACIÓN DE CRITERIOS EDUCATIVOS PARA LA PROTECCIÓN DE LA PRIVACIDAD EN IBEROAMÉRICA[3]

Cuando pensamos en educación, la mayoría de las personas generamos una o varias imágenes mentales de niños y de escuelas. Pero la educación trasciende esta imagen, ya que es un concepto mayor. Los seres humanos no dejamos nunca de educarnos a lo largo de toda nuestra vida, en un mundo que gira vertiginosamente y que ¿evoluciona? día a día. Asimismo, cabe recordar que la escuela siempre se hace eco de las inquietudes de la sociedad. Hoy en día una gran parte de estas inquietudes vienen dadas por conceptos como "redes sociales", "videoconferencias", "ciberespacio" y la comunidad educativa se esfuerza por adaptarse a las nuevas tendencias tratando de dar respuesta a los nuevos problemas que han surgido.

Las Tecnologías de la Información y la Comunicación (TIC) han venido a demostrarnos que existe una tendencia mundial a la incorporación del avance de las herramientas digitales en la vida de los habitantes de este planeta, en cada minuto y lugar de su existencia. Esto nos genera nuevas oportunidades, pero también nuevos riesgos.

Las TIC son la puerta de entrada que posibilita el acceso al conocimiento acumulado de toda la historia; nos ponen al alcance de la mano una infinita cantidad de información; achican distancias; y nos permiten conectarnos a nivel global como ninguna otra tecnología había logrado.

Sin embargo, también la actual sociedad del conocimiento revela, igualmente, la existencia de diversos riesgos asociados, a saber: la generación de nuevas diferencias sociales entre quienes tienen y no tienen acceso a las tecnologías; situaciones de exclusión digital; la existencia de una brecha digital entre los menores y sus padres y educadores; así como la posible vulneración de los derechos humanos, como es el derecho a la protección de los datos personales.

Educación y acceso

Muchas veces, la decisión de acceso a lo que usualmente denominamos "tecnologías de la información y la comunicación" depende de las posibilidades de cada familia, de cada establecimiento educativo, de cada sociedad, de cada nación. A veces, los impedimentos

3. La Declaración de Buenos Aires, hacia la unificación de criterios educativos para la protección de la privacidad en Iberoamérica, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en la Ciudad Autónoma de Buenos Aires (Argentina), el 11 de julio de 2013, por el Director del Centro de Protección de Datos, Eduardo Peduto, en la Defensoría del Pueblo de Buenos Aires. En la elaboración de la Declaración intervinieron Ines Tornabene, Ezequiel Passeron, Óscar Costa Román, Francisco Ramón González-Calero Manzanares, Noemi Brito Izquierdo, Javier Sempere Samaniego, Javier Villegas Flores, Romina Florencia Cabrera, Carlos Vera Quintana, Analía Aspis, Edgar Tomas Quiñonez Ríos, Matilde Martínez y Alexander Díaz García, coordinados por Daniel López Carballo.

vienen dados por intereses supranacionales o particulares de algunas naciones que impiden el acceso de otras a esta fuente de poder que implica el conocer o, al menos, el contar con la potencialidad de acceder al conocimiento.

Por lo tanto, cuando pensamos en unificación de criterios educativos, no tenemos que olvidar algunos conceptos:

- Que educar es hacerlo para todos: niños, adolescentes y adultos.
- Que educar posibilita que todos los ciudadanos puedan acceder y hacer uso de la información y el conocimiento accedido, lo que resulta clave para el propio ejercicio de sus derechos fundamentales.
- Que el simple acceso al conocimiento no significa educar.
- Que todos los países deben ser soberanos para poder acceder a las fuentes del conocimiento.
- Que el concepto de educación es un concepto dinámico, que evoluciona constantemente. Por eso, todos debemos adaptarnos a los cambios y contribuir en las etapas de transición.
- Que la educación permite que se haga un uso correcto de las tecnologías de la información respetando los derechos de los demás.
- Que el acto pedagógico es un proceso inclusivo que potencia el desarrollo de las naciones y de cada uno de sus ciudadanos.
- Que existen brechas educativas que la tecnología está capacitada para disminuir, teniendo especial consideración en no crear nuevas distancias educativas digitales.
- Que la educación requiere un proceso permanente de evaluación y aseguramiento de la calidad y de su impacto en la sociedad.

Es por tanto que no solo debemos reclamar el derecho a la educación para todos los habitantes de nuestro planeta, sino una educación inclusiva, intercultural, de calidad y accesible por todas y todos los ciudadanos, que dé las mismas oportunidades a todos los ciudadanos de forma independiente al sexo, la raza, religión, condición social o nacionalidad.

En esta línea de pensamiento, debemos aclarar que nos encontramos ante un “arma de doble filo” cuando hablamos de las TIC, ya que aquellos individuos que tienen acceso a ellas de forma crítica y con los conocimientos necesarios que les permitan sacar el máximo partido a estas herramientas, podrán desarrollar su formación de una manera mucho más amplia a través de páginas web, videos, intercambios de opiniones mediante foros, mucho más brillante que quien no se sepa desenvolver de forma correcta en estos ambientes o directamente no tenga acceso a ellos. De esta forma, podemos concluir diciendo que hoy en día una persona que viva en un país no desarrollado puede acceder a la misma formación que otra que viva en el primer mundo, pero para ello debe tener acceso a las TIC de forma juiciosa para poder valorar los contenidos a los que accede.

La privacidad como un derecho humano fundamental

Es necesario inculcar a los ciudadanos la idea de la privacidad como un derecho humano que puede hallarse en el ámbito internacional en la Declaración Universal de Derechos Humanos de 1948, la cual específicamente protege la privacidad territorial y de las comunicaciones.

El Artículo 12 establece: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Diversos tratados internacionales de derechos humanos reconocen expresamente la privacidad como un derecho. El Pacto Internacional de Derechos Civiles y Políticos (PIDCP), la Convención Internacional de las Naciones Unidas sobre la Protección de Todos los Trabajadores Migratorios y sus Familias, etc.

Otros tratados regionales están también empezando a ser utilizados para proteger la privacidad. El artículo 11 de la Convención Americana sobre Derechos Humanos estipula el derecho a la privacidad en términos similares a los de la Declaración Universal. En 1965, la Organización de Estados Americanos proclamó la Declaración Americana de los Derechos y Deberes del Hombre, la cual estableció la protección de varios derechos humanos, entre ellos el de privacidad. A su vez, la Corte Interamericana de Derechos Humanos ha empezado a ocuparse de problemas de privacidad en sus casos.

Resulta asimismo de especial interés tener en cuenta la posibilidad de que este derecho fundamental también se reconozca de forma específica en la Convención de los Derechos del Niño de 20 de noviembre de 1989, siendo, además, el tratado internacional con la más amplia ratificación de la historia y cuyo objeto principal estriba, precisamente, en garantizar la protección y el desarrollo de los niños.

Protección de los datos personales

Teniendo en cuenta, entonces, que cuando hablamos de educación no nos referimos solamente a nuestros niños y adolescentes, sino a cada ser humano en nuestro mundo, debemos pensar necesariamente en la posibilidad de unificar criterios en materia educativa con la finalidad de que exista un uso responsable de las tecnologías de la información, y con ello lograr el máximo respeto a la protección de los datos personales. Hoy nos encontramos en un contexto regional particular, que nos interpela, que nos pide respuestas y por ende trabajo, toda vez que surge una iniciativa tan particular como este Observatorio y que tiene inmediatamente tanta repercusión y participación en numerosos actores de distintos países. Por lo tanto, debemos olvidarnos de las tradicionales fronteras físicas y políticas para comenzar a pensar

en “ciberfronteras” y trabajar de forma conjunta en nuevas normativas que salvaguarden los derechos de todos los ciudadanos, tendiendo renovados puentes y alianzas internacionales de forma que puedan protegerse, en mejor y mayor medida, los derechos fundamentales de todos los ciudadanos, con independencia de su nacionalidad, localización y/o ubicación física. Y es que no se debe olvidar que Internet es global y requiere de respuestas jurídicas, en la mayor medida posible, coordinadas en todos los países.

Se debe apostar por una educación en la utilización de las tecnologías de la información que involucren el tratamiento de los datos personales, así como campañas de prevención para el fomento de la comprensión de prácticas de buen uso de las herramientas informáticas que impliquen directa o indirectamente la manipulación de datos personales.

En este ámbito, la formación y la educación en privacidad resultan vitales para garantizar otros tantos derechos fundamentales, como la libertad de la información, la libertad de expresión y, en definitiva, el derecho a la educación y a la libre conformación de nuestra personalidad, de nuestro desarrollo personal.

Iberoamérica

Como región, tenemos muchas cosas en común. España, Latinoamérica y el Caribe conformamos una región especial. Podemos pensar que no es un océano el que nos separa, sino el que nos une, como nos unió en la historia, como fue el que posibilitó que esta porción del planeta sea lo que es hoy. Nos une desde un concepto de igualdad, y no de colonia; desde un concepto de idiosincrasia compartida, y no de dominación; desde una perspectiva de hermandad, de sentirnos o habernos empezado a sentir miembros de una misma sociedad.

Una sociedad que crece. Y que quiere seguir haciéndolo, no a la sombra de los países más desarrollados del mundo, sino desde su propio lugar y desde su propia cultura.

En esta línea, debemos destacar que las TIC hacen casi desaparecer las barreras físicas entre los continentes, ya que posibilitan tanto el trabajo colaborativo y cooperativo como el aprendizaje cooperativo y colaborativo, lo cual abre un sinfín de posibilidades tanto para los docentes como para los alumnos, ya que potencia la creación de redes de aprendizaje.

Disminuir la brecha digital y generacional

Por eso, las iniciativas que deben ganar nuestra atención y apoyo son aquellas que tienen en cuenta a los principales actores de la escena educativa: alumnos, docentes y padres. De esta forma educamos a todos, no solo a los alumnos, sino que también articulamos la educación en materia de protección de datos personales entre los distintos actores y donde cada Estado es un componente fundamental e integrante del guión.

Una educación enciclopedista y estática, donde algunos brinden a otros, en la creencia que son los destinatarios del conocimiento a quienes hay que abastecer, no será la respuesta adecuada en el estado de la evolución tecnológica que atravesamos. Es necesario incorporar herramientas que permitan llegar a los alumnos en su medio, hablarles en su propio lenguaje, y así permitir recuperar y resignificar la función docente como fundamental en la tarea educativa desde un punto de vista paidocéntrico y que permita brindar a los padres soluciones para cuidar y proteger a sus hijos y a sí mismos. Esto se logra escuchando a los más jóvenes, los llamados "nativos digitales", quienes más conocen las tecnologías de la información y la comunicación, pero también dando herramientas a los adultos para que puedan acompañar a los niños e intervenir así en el mundo digital, aportando las capacidades críticas y reflexivas necesarias, tratando de eliminar la brecha digital existente entre los menores y su gran manejo de las tecnologías de la información, y los mayores, en muchas ocasiones, desconocedores de su uso. Y que está generando que la sociedad se divida en dos grandes grupos: el de los nativos digitales y el de los inmigrantes digitales, que evolucionan por diferentes caminos y muchas veces de forma discordante entre sí.

Como sostenía el pedagogo Paulo Freire, es esencial al método, que la praxis acompañe a la reflexión. La una sin la otra hace que pierdan sentido las dos.

Sería incorrecto pensar en la entrega de dispositivos informáticos como un ente aislado y autorreferencial. La alfabetización digital debe ser acompañada por una alfabetización integral, basada en la recuperación de la educación pública, para formar ciudadanos con pensamiento crítico capaces de debatir los modos y fines de uso de las nuevas tecnologías, creando sus propios contenidos y mejorando los ya existentes, y no ser simples receptores pasivos. Por eso celebramos que las políticas públicas del Estado entiendan este fenómeno, y junto con el esfuerzo por la disminución de la brecha digital, en términos de dispositivos, la acompañen con esfuerzos para disminuir la brecha a nivel cognitivo. Esto es, no solo entregar el aparato técnico, sino también brindar el "know how" para utilizar los mismos de forma correcta, ya que de poco sirve dar tablets, pc's o smartphones, si este "regalo" no va acompañado de la información y/o formación necesaria.

Las distintas instituciones de aprendizaje del sistema educativo deben convertirse en un ámbito que interpele al estudiante sobre el cómo, por qué, cuándo, dónde y para qué se utilizan las nuevas tecnologías. Es por esto que resulta central que el espíritu crítico atraviese el recorrido educativo de los ciudadanos, y que éstos, en su trayectoria académica, no se limiten a la simple operación de un dispositivo tecnológico sin ser capaces de tener una mirada crítica de la realidad que los envuelve.

La tarea educativa, reiteramos, no es algo dedicado en exclusividad a los alumnos niños y adolescentes. Por citar algún programa, hablaremos del "Lifelong Learning Programe" (programa de aprendizaje permanente) creado por la Unión Europea en 2007 y que trata de

que el aprendizaje no solo se dé en los primeros años de la vida. En el ámbito de la protección de la privacidad, todos somos alumnos, y todos podemos ser educadores.

Esta educación, con la ayuda y la implantación de todos los poderes y autoridades públicas, no solo debe posibilitar ese uso responsable de las tecnologías de la información, sino que también es primordial eliminar la ofensa y la vulneración a los derechos fundamentales mediante actividades que conocemos con el nombre de “grooming”, “sexting” o “ciberbulling”.

Es fundamental impulsar cambios en el rol del docente, de simple trasmisor de conocimientos, fuente primaria de información y controlador de todos los aspectos del aprendizaje, a facilitador del aprendizaje, colaborador, co-alumno, facilitador de más opciones en el aprendizaje de los niños, niñas y adolescentes. Es por tanto que el profesor debe abandonar la figura tradicional de eje transversal de la educación, para convertirse en un guía del conocimiento que ayude a sus alumnos a resolver los problemas educativos que les puedan surgir.

Los alumnos deben pasar de ser simples receptores pasivos de información, reproductores de conocimiento, a participantes activos en el proceso de aprendizaje y productores de conocimiento y aprendizaje en colaboración con otros. Esta visión es, además, la más coherente desde el enfoque debido del respeto a los derechos fundamentales de los niños que, no se debe olvidar, son titulares de múltiples derechos, como el derecho a informarse, a expresarse, a educarse, así como a desarrollar de forma libre su personalidad, entre otros.

No debemos olvidar a los ciudadanos como parte del proceso de disminución de la brecha digital. Las iniciativas de gobierno electrónico y acceso a la información pública podrán ostentar todos sus beneficios si los ciudadanos comunes poseen las capacidades y conocimientos suficientes para sacar el mayor provecho de las diferentes iniciativas gubernamentales que tienen como fin facilitar los servicios públicos, la transparencia de gobierno y la participación ciudadana.

Estado del arte

Contamos a nivel mundial e Iberoamericano con herramientas jurídicas suficientes, idóneas para proteger los derechos derivados de la intimidad y la privacidad, para el respeto del honor, la reputación y la honra. Cada país viene trabajando arduamente en seguir generando una normativa que permita un mayor resguardo. Los lazos de cooperación entre los países iberoamericanos seguirán creciendo, en busca de una normativa que se complemente y que permita alianzas regionales cada vez mayores. Y encontramos que existe una fuerte y plena coincidencia doctrinaria en los caminos imprescindibles que se deben seguir para lograr cada día una mayor protección.

Por eso, creemos que todos hemos encontrado, por nuestra experiencia y por la observación

de las experiencias de otras áreas del mundo, que la prevención y la concientización se erigen como las dos principales herramientas para el resguardo de la intimidad, la privacidad y los datos personales.

Además de que existe una tendencia generalizada a considerar que el docente tiene un rol fundamental en esta tarea de prevención y concientización, y que puede convertirse, naturalmente y con un esfuerzo mínimo, en un verdadero agente de protección de datos personales que puede articular la experiencia educativa, ya que en el día a día recibe la retroalimentación de sus alumnos, y se ve precisado muchas veces de interactuar con los padres, ya que todos deben trabajar en la misma línea para alcanzar el objetivo común: una educación transversal que dote al futuro alumno de las herramientas necesarias para poder desenvolverse en su vida diaria.

Y también observamos que, en muchos casos, existe una brecha tecnológica entre docentes y alumnos, de las mismas características que la que se señala entre padres e hijos. Hoy se habla de los nativos digitales, esos niños y jóvenes que han nacido en un mundo con una tecnología determinada, y con un dominio natural y espontáneo, al menos en aquellos niños y jóvenes que hayan nacido en regiones y hogares donde la tecnología se encuentra presente.

Un nativo digital no “piensa” la tecnología, la usa. No la ve como un objeto ni como un objetivo en sí mismo, sino como un medio, como una herramienta. Pero esto no es una cuestión de edades, ya que en las regiones u hogares donde esta tecnología no ha accedido aún, la brecha tecnológica existe también. No es un gen el que determina que un niño o un adolescente sea un “nativo digital”, sino un medio cultural determinado del cual se impregna desde incluso antes de su nacimiento.

Así, los docentes y adultos, en general, pueden percatarse a sí mismos como carentes de cierto conocimiento, donde pueden fácilmente verse desbordados o superados por los conocimientos de sus alumnos. Y estas situaciones de disparidad pueden dar origen a muchos malentendidos.

Allí es donde entendemos que la tarea de quienes nos dedicamos a la divulgación de la protección de datos personales se vuelve indispensable para arrojar un poco de luz en la confusión. El rol docente no se subvierte; el rol docente debe ser el mismo: ayudar a la articulación del conocimiento, ayudar al discernimiento sobre lo que es verdadero o no desde el punto de vista del conocimiento científico, ayudar a entender y a pensar. Enseñar a aprender, para alcanzar una meta final como es “aprender a aprender”.

Es cierto que en esta nueva era el conocimiento está al alcance de todo aquel que pueda acceder a determinadas herramientas tecnológicas, como lo es por ejemplo internet. Pero no menos cierto es que el rol del docente en el aula es indispensable para ayudar a los educandos a seguir articulando y aprender a pensar y a valorar la información.

Los Estados serán quienes –con carácter obligatorio por cumplir una actividad pública– deben acercar las herramientas de concientización y prevención a alumnos, docentes y padres. Y la principal consigna que se debe difundir, sea desde el Estado, la docencia o el hogar, es que la mejor forma de cuidar nuestros datos personales es haciéndonos responsables de ellos.

Es decir, reconocer nuestro derecho humano a la protección de la información personal y ejercerlo. Nosotros debemos decidir qué queremos hacer con nuestros datos personales, quién puede disponer de ellos y para qué. Ésta es una tarea educativa en la cual todos ocupamos el rol de docentes y, a su vez, todos debemos ocupar el rol de educandos, ya que la propia característica permanentemente creciente y dinámica de la tecnología nos obliga a pensar y a repensar conceptos que a diario van cambiando.

Es por todo ello, que se debe potenciar el aprendizaje permanente ya que tal y como se ha expuesto, hemos dejado de vivir en un mundo que sufre pequeños cambios cada unos cuantos siglos, para vivir en una sociedad con constantes cambios a los que nos debemos enfrentar y dar soluciones.

Convergencia digital

En la actualidad vivimos un fenómeno tecnológico sin precedente. Vivimos en la era de la convergencia. Hoy podemos encontrar conexión a Internet, ver TV, escuchar la radio, chatear, leer libros, etc., en nuestros dispositivos móviles. Esto provoca un cambio enorme para la protección de la información.
Para poner un ejemplo de cómo las mismas situaciones van variando, recordemos que antes se daba como consejo a los padres que la computadora del hogar estuviera en un lugar de paso, a la vista de todos; hoy ese consejo no puede ser suficiente, dado que con la existencia de dispositivos móviles como los teléfonos celulares y las tabletas, ese consejo quedó, como poco, exiguo e insuficiente. Entonces, todos debemos tomar conciencia de cómo cambian día a día las situaciones debido a la evolución tecnológica. Este proceso tiene la particularidad de no ser una fotografía, estática e inmutable, sino una película, dinámica y cambiante. Los padres en sus hogares, los docentes en los establecimientos educativos y quienes nos dedicamos a la protección de los datos personales con más ahínco todavía, ya que pesa sobre nosotros la responsabilidad en la difusión de lo que consideremos las mejores herramientas educativas para una prevención y concientización exitosas.

Pensar globalmente y actuar localmente

Es importante procurar el desarrollo de herramientas que utilicen un vocabulario que pueda ser entendido en cualquiera de los países de la región. Y en caso de que eso no sea posible, hay que proveer a las herramientas –sitios web, manuales, guías– que puedan ser utilizadas por los educadores, de sinónimos idóneos para cada país. De esta forma, el esfuerzo puesto en movimiento en un país o en un organismo determinado puede ser aprovechado regionalmente por otro. Y así también se derriban las fronteras y se hermanan los países, ya que, en definitiva, el objetivo es el mismo.

La formación y capacitación de los educadores en la comprensión y reflexión en los diferentes aspectos que incluya la tecnología en los ámbitos educativos es fundamental a fin de contribuir a la generación de herramientas que conlleven a un mayor entendimiento y diálogo entre los diferentes participantes del proceso educativo.

Por todo lo expuesto, entendemos que se debe actuar en varias líneas programáticas:
Con los educadores: durante su formación inicial se les debe orientar en el uso seguro de las TIC, tanto de forma pedagógica como de forma crítica en su vida personal, ya que es realmente complicado formar a alguien sobre conceptos que se desconocen. Además, se debe facilitar y animar a que los docentes se involucren en un proceso constante de "reciclaje formativo" para poder dar la mejor respuesta a los problemas que les surjan a sus alumnos.

Con los alumnos: haciendo una fuerte apuesta por la formación en la privacidad y la protección de datos para que puedan acceder al mundo digital en un ambiente amigable y seguro, conociendo los riesgos a los que se exponen y dotándoles, finalmente, de herramientas que les permitan ejercer otros tantos derechos fundamentales que les son inherentes.

Con las familias: creando espacios en los que se relacionen padres e hijos, nativos e inmigrantes digitales, que potencien los canales de información y en los que todos sean profesores y alumnos al mismo tiempo.

A nivel estatal: actuando en dos líneas que entendemos esenciales:
Impulsando políticas activas en educación. Creemos necesario para alcanzar los objetivos marcados anteriormente, la creación de una asignatura obligatoria en los Planes de Estudios sobre "Privacidad", en la que profesionales expertos en la materia aconsejen y enseñen a los menores a proteger su intimidad en la red y a evitar ser potenciales víctimas de un delito informático. Estos profesionales también podrían formar al resto de educadores y, por qué no, a los progenitores o tutores legales a través de charlas, cursos o conferencias.

Proveyendo no solo de dispositivos a los ciudadanos, sino también dando la formación necesaria a toda la población para que puedan sacarle el máximo partido a dichos dispositivos para que

no se conviertan en objetos que solo sirven para ser observados, como si de una escultura se tratase, fomentándose de esta forma políticas realmente inclusivas, que permitan la igualdad de acceso al conocimiento a todos los sujetos.

A nivel internacional: generando programas y experiencias de "intercambios virtuales", en los que tanto alumnos como profesores desarrollen trabajos colaborativos y cooperativos, para alcanzar una globalización que permita a todos los participantes un enriquecimiento cultural, personal y cognitivo que acerque al individuo al presente en el que va a tener que desenvolverse, formado por equipos de trabajo internacionales y en los que aspectos como el idioma o la condición social, no supongan barreras.

Finalmente, entendemos que también se debe implicar al sector privado en la labor educativa. Los desarrolladores de dispositivos, programas, aplicaciones, webs o redes sociales deben facilitar la configuración de privacidad de los usuarios finales, utilizando un lenguaje sencillo y comprensible tanto para menores como para personas con escasos conocimientos tecnológicos, proporcionando herramientas sencillas y "a la vista" para proceder a una óptima configuración de privacidad, proporcionando mecanismos de bloqueo parental y facilitando la comunicación de denuncias o abusos que se puedan estar cometiendo por parte de otros usuarios, no quedándose meramente en un simple "bloqueo del mismo".

DECLARACIÓN DE SANTIAGO DE CHILE, HACIA UNA UNIFICACIÓN DE CRITERIOS SOBRE SEGURIDAD Y PROTECCIÓN DE DATOS EN INTERNET[4]

La protección de datos personales es un derecho humano universal y fundamental reconocido a nivel global en la Declaración Universal de los Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos. Íntimamente ligado con la libertad individual, la libertad de expresión y el derecho a la intimidad, honor y dignidad personal, está consagrado por el artículo 8 de la Carta Europea de Derechos Fundamentales, y regulado como garantía constitucional en la mayoría de ordenamientos jurídicos iberoamericanos en el marco del "habeas data".

Sin embargo, la revolución tecnológica en la que nos hallamos inmersos como consecuencia de la aparición de Internet ha producido y está produciendo innumerables cambios en los hábitos y las relaciones humanas, que obligan a las distintas legislaciones a un ejercicio de permanente adaptación a una realidad cambiante y transfronteriza. Con el uso de las nuevas tecnologías y, en particular, con la eclosión de la red y las nuevas formas de interacción de las personas, diariamente se ven afectados los derechos y libertades individuales y colectivas; aquellos derechos referidos a propiedad sobre bienes inmateriales, como los relacionados con los derechos de autor y la propiedad industrial, todos los relacionados con el comercio electrónico, como los derechos de consumidores y usuarios, o aquellos relativos a la libertad de expresión e información. Pero sin duda, el derecho más amenazado y vulnerable, y sobre el que deviene fundamental articular una regulación unificada, adecuada, solvente y eficaz, es el derecho a la protección de datos personales, dentro del marco de la protección a la intimidad personal que, si bien –como hemos apuntado en la introducción– ya es objeto de regulación a nivel nacional, supranacional e internacional, aún carece de una regulación actualizada y unificada que garantice su tutela efectiva, debido a la realidad cambiante derivada de los constantes avances tecnológicos, y a la ausencia de un marco común que supere las barreras nacionales, ya que solo así puede ser tratado un fenómeno que no entiende de fronteras.

Internet se ha consolidado en una herramienta de gran utilidad con múltiples usos y finalidades. La posibilidad de poder encontrar cualquier tipo de información en segundos, las utilidades para el teletrabajo, el almacenamiento de información, el ocio o las relaciones sociales son

4. La Declaración de Santiago, hacia una unificación de criterios sobre seguridad y protección de datos en Internet, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, presentada en la ciudad de Santiago (Chile), el 12 de septiembre de 2013, por Pedro Huichalaf Roa, en el transcurso del Seminario de Datos personales, organizado en la Facultad de Derecho de la Universidad de Chile, en colaboración con la ONG META y la Asociación de Defensa, Educación y Protección de los Consumidores del Perú. En la elaboración de la Declaración intervinieron Javier Villegas Flores, Marta Sánchez Valdeón, Romina Florencia Cabrera, Pedro Huichalaf Roa, Braddy Leonardo Alave Apaza, Yarina Amoroso Fernández, Claudio Magliona y Santa Matilde Reyes Valenzuela, coordinados por Daniel López Carballo y Francisco Ramón González-Calero Manzanares.

ilimitadas. No podrá negarse que la tecnología digital, se ha convertido en eje fundamental de los grandes cambios a los que asiste esta generación nuestra, tanto en la manera de relacionamos con los demás, como en la forma de entender los negocios.

Los productos o servicios disponibles a través de la red pueden ser remunerados o gratuitos. Ambas presentan problemas para mantener a buen recaudo la privacidad de los datos de sus usuarios y la manera en cómo se brinda la información relevante para que el usuario tome una decisión, elección, uso o consumo de un determinado servicio.

Los servicios remunerados usan los datos de sus usuarios para su propio beneficio y así poder brindar mejoras en la prestación, ya que mantienen a su alcance datos analizados con los cuales generan perfiles de usuarios, lo cual es lícito siempre que se les brinde información relevante, oportuna, veraz, suficiente, de fácil comprensión y fácilmente accesible, debiendo ser brindada en el idioma oficial del país de cada usuario.

Los servicios gratuitos también están obligados a cumplir con brindar información relevante, entendiendo esta como la información mínima sin la cual el usuario no hubiera adoptado la decisión de usar el servicio y entablar una relación de consumo cuya ejecución se extiende hasta que el usuario decida darse de baja.

En los servicios gratuitos, si bien no existe como medio de transacción expreso el dinero, en su reemplazo se hallan los datos que brindan los usuarios, los cuales sirven al proveedor para generar perfiles de usuarios mediante análisis a través de algoritmos, lo cual es lícito siempre que cumpla con su obligación de brindar información relevante, oportuna, veraz, suficiente, de fácil comprensión y fácilmente accesible, debiendo ser brindada en el idioma del usuario.

Estos últimos son los que pueden llegar a plantear mayores problemas, ya que la gratuidad suele llevar aparejada la pérdida de privacidad. Además, como toda herramienta en manos humanas, puede ser usada con fines lícitos o ilícitos, legítimos o ilegítimos.

El desarrollo de aplicaciones que generan plataformas de intercambio de datos y contenidos, y el nacimiento de la web 2.0. y de los sitios web colaborativos (blogs, wikis y redes sociales) en los que los usuarios de la red dejan de ser meros “consumidores” para transformarse en Prosumidores generadores de contenidos, lo que acentúa más los riesgos para la privacidad, particularmente en las redes sociales, en las que los datos personales pasan de ser un elemento accesorio para convertirse en el elemento clave para el funcionamiento de las mismas.

Para que los diferentes usos y finalidades de Internet se consoliden y se generalicen, los usuarios necesitan contar información relevante, oportuna, fácilmente accesible y de fácil comprensión que les genere confianza entre otros factores. Y esa confianza solo puede ganarse protegiendo y

garantizando la privacidad y la seguridad de los mismos. En una anterior Declaración, ya se hizo hincapié en los diferentes tipos penales que se dan en Internet, y ahora toca analizar los problemas que afectan a la privacidad en Internet desde la perspectiva de la protección de datos personales de sus usuarios. Como venimos recordando a lo largo de todas las Declaraciones presentadas, al existir un componente de internacionalidad y universalidad en la red, las diferentes legislaciones nacionales por sí solas no pueden dar una respuesta adecuada a estos problemas y, por ello, deben unificarse para evitar que estas empresas y sus servidores se ubiquen en países que no ofrezcan niveles adecuados de protección en materia de privacidad.

Un primer uso de Internet se da en el comercio electrónico. La posibilidad de poder comprar desde cualquier lugar y a cualquier hora tiene un gran potencial de crecimiento. Pero una de las causas que ralentizan el mismo es la falta de seguridad que perciben sus potenciales usuarios, sobre todo, si la empresa con la que queremos contratar se encuentra ubicada en otro Estado y, por ello, se encuentra sometida a una legislación sobre privacidad y comercio electrónico que desconocemos, o que ni siquiera existe. El usuario tiene que tener confianza en quién está detrás de ese sitio Web y del uso que va a dar a sus datos personales. Es por ello que las diferentes legislaciones deben exigir la implantación de avisos legales ubicados en lugares visibles de las páginas webs, que de forma clara y precisa nos informen de quién está detrás de ese dominio y que cuenta con todos los permisos y autorizaciones necesarios para el ejercicio de esa actividad, cómo podemos contactar con él, qué garantías legales tenemos como consumidores, y qué piensa hacer con nuestros datos personales y de qué manera podemos oponernos a ese tratamiento en un futuro. De la misma manera, las diferentes legislaciones deben imponer ciertas obligaciones a los responsables de estos tratamientos en lo que no se ve por parte del usuario, pero que puede darle confianza el saber que ese responsable tiene obligación de cumplir unos requerimientos legales sobre seguridad en los tratamientos, ejercicios de derechos, encargados de tratamiento, transferencias internacionales de datos, cesiones de datos, deber de información y consentimientos. En las distintas legislaciones resulta fundamental reforzar, por tanto, la idea del control sobre los datos de los cuales se es titular, lo que conlleva a favorecer la protección de los datos de carácter personal frente a toda intromisión de terceros, sean éstos públicos o privados, y por tanto, establecer las condiciones bajo las cuales estos últimos podrán efectuar legítimamente el tratamiento de tales datos.

Conforme a los lineamientos internacionales, la regla general debe ser un consentimiento previo, inequívoco e informado para el tratamiento de datos personales. Lo que interesa es que las formas del consentimiento estén acordes a los usos y costumbres de los usuarios de Internet y, a la vez, provean a éstos la información suficiente para que tomen una opción –expresa o a través del mero uso– debidamente informada.

Todo proveedor de servicios debe brindar información relevante, oportuna, veraz, suficiente, de fácil comprensión y fácilmente accesible, debiendo ser brindada en el idioma oficial del país

de cada usuario; agregar además que no solo se debe cumplir con el mero hecho de brindar información de manera textual sino que, a su vez, se presente a través de animaciones al momento de entablar la relación de consumo y en el transcurrir de la misma enviando al correo electrónico del usuario la información relevante para hacer valer sus derechos.

El Cloud Computing es otro de los servicios (gratuitos o de pago) que puede incrementar su volumen de negocio en los próximos años. La posibilidad de alojar datos y que estos sean accesibles desde cualquier lugar o dispositivo con conexión a Internet ofrece posibilidades desconocidas aún. Estos servicios no tienen ningún impedimento técnico a la hora de plantearse su contratación con un prestador de otro país, pero si no se armonizan las diferentes legislaciones imponiendo unas obligaciones a estos encargados de tratamiento en lo que respecta a la limitación de usos de esos datos, implantación de medidas de seguridad o derecho a la portabilidad, sí que pueden existir impedimentos de tipo legal a la contratación de un prestador ubicado en un país extranjero o que no exista este impedimento, pero no se produzca la contratación por falta de confianza.

Como ya hemos reflejado anteriormente, la gratuidad suele conllevar a cambio una pérdida de privacidad. Es legítimo ofrecer un producto o servicio gratuito y pretender obtener ingresos por otras vías, pero lo que no se puede permitir es que bajo la apariencia de "falsa gratuidad" se comercie con nuestros datos a través de la construcción de perfiles de usuarios, mediante las cuales se elabore un perfil comercial basado en nuestros hábitos o preferencias y se nos bombardee con publicidad sin habernos informado de forma clara y sencilla antes de prestar nuestro consentimiento del tratamiento de nuestros datos y la finalidad y usos de los mismos, así como de nuestros derechos respecto a los mismos.

Igualmente hay que garantizar la protección de los usuarios cuando se producen cambios unilaterales y sobre la marcha de las reglas del juego, a fin de garantizar que se sigan cumpliendo los principios básicos antes mencionados. Es por ello que las legislaciones nacionales deben uniformarse para evitar que los propietarios de estas redes sociales y servicios de mensajería instantánea y sus servidores se ubiquen en países permisivos en materia de privacidad donde puedan dar rienda suelta a prácticas prohibidas por ley en otros Estados. Independientemente de donde se encuentren ubicadas estas empresas, deberían mediante avisos legales informarnos previamente al alta como usuario o a la instalación de esa aplicación en nuestro dispositivo electrónico, de una manera clara y precisa del tratamiento y usos que se va a dar a nuestros datos y de la manera de oponernos a ello. De la misma manera, si cambia la política de privacidad, se nos debería avisar con suficiente antelación del cambio, de manera que podamos oponernos a ello o solicitar, en su caso, la baja del servicio o red social. Y lo que debería quedar terminantemente prohibido en todas las legislaciones es el mantenimiento de esos datos una vez que el usuario se ha dado de baja y los plazos legales de reclamación judicial o administrativa han prescrito.

Otro problema que afecta a la privacidad de los ciudadanos o los trabajadores son los sistemas de geolocalización instalados en los dispositivos y aplicaciones móviles. Las diferentes legislaciones deberían armonizarse obligando con carácter previo a informar sobre los tratamientos y usos previstos, dar la posibilidad de oponerse a ellos, informar sobre el modo de ejercitar los derechos reconocidos y permitir su desconexión temporal o definitiva por parte del usuario, solicitando permiso previo para su posterior activación. También se debería obligar a los fabricantes e instaladores a que por defecto dejen deshabilitada esta opción. Las diferentes legislaciones deben ser especialmente protectoras con la privacidad del menor cuando estos sistemas vayan dirigidos a ellos o puedan ser utilizados por sus padres o representantes legales como herramientas de control parental.

Las recurrentes informaciones en los últimos tiempos relativas a casos de espionaje en la red, así como las relativas a los llamados "delitos informáticos", han puesto en boga el derecho a la protección de datos en la red de redes. Esto se plasma en un cada vez mayor celo de los usuarios en el uso de Internet a la hora de compartir información, y gracias a esta labor divulgativa de los medios los ciudadanos identifican con mayor claridad este derecho y sus implicaciones y riesgos, aunque la información aún es insuficiente, como recientes estudios señalan.

Por tanto, urge que las autoridades nacionales e internacionales, entidades públicas y privadas, asociaciones de consumidores hagan un esfuerzo en materia de formación y concienciación de los usuarios sobre la seguridad de la información en Internet, como medida preventiva fundamental a fin de que el usuario sea consciente de los riesgos y se convierta en el principal garante de su privacidad; muy especialmente en el caso de padres y menores, ya que estos últimos acceden desde edad muy temprana a la red, y son el colectivo más vulnerable y susceptible de sufrir ataques a su intimidad.

Todos los servicios antes mencionados, sean gratuitos o pagados significan un flujo transfronterizo de datos personales, materia que debe ser recogida en las distintas legislaciones. Justamente una adecuada normativa resulta clave para el desarrollo de mercados emergentes tales como el de offshoring o servicios globales.

Por otra parte, es indiscutible que actualmente el acceso a las políticas de privacidad, avisos legales o condiciones generales de contratación o uso de los sitios web es marginal. Los usuarios cuando entran en un portal, suben un vídeo, comparten un archivo, o compran un producto, no conocen el tratamiento, uso o cesión de sus datos personales, la cesión o no de la titularidad o uso del contenido, o los derechos que le asisten como consumidor.

En definitiva, no se presta el consentimiento basado en una información clara y confiable, por lo que tal y como hemos ido apuntando, es necesario la realización de estándares internacionales que garanticen la protección eficaz de estos derechos.

Este estado de cosas obliga a proponer estándares internacionales compartidos que garanticen la transparencia y el acceso a la información de forma clara y comprensible.

En relación a este tema, otro de los problemas mayores que se da en Internet es que es muy fácil entrar y muy complicado salir. De igual forma, una vez que el contenido entra, se pierde el control sobre el mismo, siendo cualquier usuario de la red potencial visualizador o descargador del mismo. Deviene por tanto necesaria una unificación legislativa para poder acceder, modificar, trasladar, retirar u oponerse al uso de contenidos, independientemente del lugar donde se encuentre ubicado el servidor y el particular o la empresa que lo ha subido. En cuanto a la eliminación de datos de la red, siempre que por la tipología del dato no exista una obligación temporal de conservación, o que no pueda ser requerido por un juzgado, tribunal o administración pública en el ejercicio de sus competencias, o que esa retirada atente contra la libertad de expresión o de información, ese dato o información debería ser eliminado mediante una simple solicitud de su titular. Se deberían unificar y clarificar estos criterios o supuestos de retirada, así como avanzar en el reconocimiento y ejecución de resoluciones judiciales, de manera que el afectado solo tenga que actuar en los tribunales de su país de residencia sin necesidad de acudir a multitud de jurisdicciones.

En definitiva, se debe garantizar y brindar las herramientas necesarias para que los usuarios tengan un control del tratamiento de sus datos y de los contenidos publicados en la red.

Otro de los riesgos que presenta Internet en cuanto a la privacidad son las grandes bases de datos que se almacenan en sitios web o grandes plataformas tecnológicas en red, como las relativas a los usuarios de consolas de videojuegos, los perfiles de las redes sociales, los datos almacenados en las bases de datos de sitios web de grandes bancos, compañías o entes públicos, etc. No pocos casos han sido noticia de ataques cibernéticos a estas plataformas, con fugas de información, robo de datos, publicación de información confidencial, phishing, y todo tipo de delitos informáticos. Por tanto, es necesaria garantizar la seguridad tecnológica de la estructura donde se alojan todas esas inmensas "bolsas" de datos personales e información confidencial, para minimizar los riesgos de estos ataques.

En relación con este punto, hay que subrayar como fundamental la colaboración de estas grandes plataformas, junto con los prestadores de servicios de Internet, con la policía y cuerpos de seguridad nacionales e internacionales, estableciendo canales de comunicación rápidos y eficaces para atajar de forma inmediata los ilícitos que pudieran llevarse a cabo. Es necesario en este punto la existencia y el reforzamiento de brigadas especializadas en el ámbito tecnológico en las fuerzas y cuerpos de seguridad de los Estados.

Asimismo, las legislaciones deben unificarse regulando los supuestos en los que un Estado puede acceder a la información que los usuarios (residentes en ese país o en terceros Estados)

de Internet tienen alojados en los servidores de sus empresas. De la misma manera que para la intervención de las comunicaciones telefónicas, la mayoría de los países democráticos obligan a la necesidad de contar con autorización judicial, el acceso a los datos y comunicaciones de los usuarios de Internet debería contar con la preceptiva autorización judicial. Esa autorización judicial debería ser individualizada y ser limitada en el tiempo, evitándose así la tentación de realizar espionajes generalizados y masivos, como hemos tenido la ocasión de comprobar.

El o los organismos encargados de control o fiscalización del tratamiento adecuado de los datos personales deben promover políticas públicas para educar o instruir a las personas con el fin de que tomen control de su seguridad y privacidad. En la actualidad, uno de los principales temores de los usuarios es que sus datos personales se filtren y sean utilizados de manera maliciosa o que terceros accedan a sus datos y/o cuentas sin su consentimiento. Los organismos de control tienen la responsabilidad de educar a la población sobre buenas prácticas de seguridad digital.

El lenguaje informático común conocido como el Internet, en estrecha unión con la liberalización de las comunicaciones y los avances tecnológicos, ha supuesto una sacudida socio-cultural de proporciones similares a la que en sus tiempos significó la Revolución Industrial. Nos hallamos, en fin, sumergidos en la sociedad de las nuevas tecnologías, cuyos avances hacen posibles los flujos de información en dimensiones desconocidas hasta la fecha. Los bastidores de la red permiten la marea constante de una revelación de hechos que, urdida en la globalización, trasciende mucho más allá de las fronteras de cada territorio y como no podía ser de otro modo, la aparición de las redes digitales ha conmovido, también, los pilares de la dignidad humana. La información concerniente a la vida particular de los individuos se enfrenta, cada vez con mayor energía, a las transmisiones en línea por redes telemáticas como Internet; lo que comporta una potencial agresión a la esfera privada de la persona, pues resulta incuestionable la facilidad de recolectar y comunicar datos, que pueden ser capturados por los internautas en las redes y transmitidos con gran sencillez de un usuario a otro. Ya no sirven las viejas estructuras burocráticas. La nueva sociedad exige la redefinición de los conceptos, actitudes y habilidades de los dirigentes políticos y de la función pública.

La protección de datos debe estar presente en las agendas internacionales, siendo un tema de relevancia actual y especialmente en el futuro, dado la expansión del llamado entorno digital, principalmente del fenómeno Internet y, dentro de ella, las redes sociales, debiéndose enfatizar en la necesidad de restaurar las relaciones de confianza y reformar los procedimientos de consentimiento, todo en aras de una mayor protección de la intimidad, el honor y la privacidad de las personas, garantizando sus derechos.

DECLARACIÓN DE LA PLATA, HACIA LA UNIFICACIÓN DE CRITERIOS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DE NIÑAS, NIÑOS Y ADOLESCENTES[5]

La historia nos acostumbró a observar ciclos evolutivos con un ritmo de instalación, crecimiento y asentamiento que permitía la adaptación, en mayor o menor medida, a los cambios. Una de las características que observamos a partir del surgimiento de la denominada "era digital" es una velocidad en los cambios tecnológicos que dificulta la adaptación a los mismos, sobre todo para los adultos.

Cuando pensamos en todos los fenómenos tecnológicos de los últimos años relacionados con el surgimiento de internet, vemos una clara diferencia en la forma que adultos y no adultos (entendiendo como tales a niñas, niños y adolescentes) procesamos esos cambios. Así surgieron términos como "nativos digitales" e "inmigrantes digitales" para tratar de distinguir a aquellos que han nacido en un contexto tecnológico-comunicacional básicamente regido por las redes digitales, y aquellos que han tenido que adaptarse y metabolizar esta explosión tecnológica.

Si bien el debate sigue abierto, hay un concepto que los que trabajamos la temática manejamos con certeza: después de internet ya nadie descansó en el mundo de la protección de los datos personales.

La historia de la expansión de internet y sus servicios (páginas web de lectura, blogs, buscadores, salas de chat, juegos en línea, correo electrónico, redes sociales, sistemas de transmisión de archivos de todo tipo, conexiones punto a punto, etc.) es la historia de un constante y exponencial crecimiento. En ese contexto de permanente cambio, se produce una proliferación de datos personales de la mano de la multiplicación de las fuentes que los exponen. Este proceso de cambio hace convivir datos públicos con privados y genera otros que sin la existencia de la web no hubiesen cobrado publicidad.

Los adultos fuimos asistiendo a este crecimiento y aprendiendo a entenderlo en etapas. Los niños, niñas y adolescentes, en cambio, nacieron con ellos y no necesitaron asimilar las novedades tecnológicas, generando una naturalización respecto a su evolución.

5. La Declaración de La Plata, hacia la unificación de criterios en protección de datos personales de niñas, niños y adolescentes, fue presentada por Noemí Olivera, Docente-investigadora y Directora del Grupo de Estudio de la Complejidad en la Sociedad de la Información, el miércoles 20 de noviembre de 2013, en la Universidad Nacional de La Plata (Argentina), en el transcurso de la Jornada "El Mundo de Internet y las Redes Sociales: Aprendiendo a Cuidarnos", organizada por el Programa Nacional Con Vos en la Web de la Dirección Nacional de Protección de Datos Personales, el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires, y el Grupo de Estudio de la Complejidad en la Sociedad de la Información de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata. La Declaración fue elaborada por Ines Tornabene, Ezequiel Passeron, Lucía Fainboim, Ernesto Liceda, Noemí Olivera, Romina Florencia Cabrera, Francisco Ramón González-Calero Manzanares, Javier Villegas Flores, Marta Sánchez Valdeón, Heidy Balanta, Dolores Dozo, Santa Matilde Reyes Valenzuela, Violeta Guerra Ramos, María Paulina Casares Subía y Camilo Alfonso Escobar Mora, coordinados por Daniel López Carballo.

Podríamos pensar entonces en dos características de esta era tecnológica: la irreversibilidad de su avance y la velocidad de los cambios.

Los datos personales de los niños

Un ser humano genera datos personales desde el mismo momento de su concepción, la cual debe ser confirmada por un test de sub unidad beta (HCG), tal vez el primer dato sensible en la vida de una persona. A eso le siguen las ecografías prenatales, los estudios y análisis genéticos y toda la batería de herramientas con la que cuenta la medicina actual para el cuidado prenatal de un bebé.

En el momento del nacimiento se sigue un determinado protocolo. El objetivo es claro: determinar la identidad del recién nacido y que no se produzcan confusiones sobre la misma. Esto se observa desde la colocación de un brazalete en el niño y la madre desde el mismo momento del nacimiento, hasta la obtención de las huellas plantales, la identificación del grupo sanguíneo, talla, peso, circunferencia craneana, la incorporación de un código de barras en las pulseras, la conservación del cordón umbilical, test de Apgar, etc. El establecimiento de la identidad de un recién nacido es un derecho reconocido, y se hace en base a la recolección de una serie de datos personales y sensibles.

De ahí en más, y hasta que sea declarado por la legislación de cada país como ciudadano mayor de edad, quienes ejerzan la representación del niño serán sus padres (o sus representantes legales. dependiendo de cada caso), y además, el Estado, a través de diversos organismos destinados, en cada ordenamiento jurídico deberá velar por su integridad.

Por lo tanto, cuando hablamos de los derechos a la identidad, a la privacidad y a la intimidad del niño, o sea, cuando nos referimos al cuidado de sus datos personales, parecería que solamente nos estamos dirigiendo a los padres, tutores, encargados, representantes legales, docentes y a los funcionarios públicos vinculados con esta competencia. Sin embargo, y tal vez la óptica nueva que pretendemos difundir desde este Observatorio, es que los principales involucrados a la hora de defender sus datos personales deben, necesariamente, ser los propios niños y adolescentes. Y eso no quita responsabilidad a quienes legalmente deben ejercer dicho cuidado.

Más que nunca, el desafío es acompañar a los niños, niñas y adolescentes en el desarrollo de una personalidad completa, lo que incluye la consciencia de la importancia de su intimidad. Es obvio que esta responsabilidad es ineludiblemente de los padres, pero también lo es del Estado, principalmente del sistema educativo. No todo se reduce a fórmulas jurídicas que busquen resarcir daños ya creados. Justamente el objetivo debe ser que esos daños nunca ocurran y los que se encuentran en la mejor situación de lograrlo son los mismos jóvenes. Para ello debemos darles las herramientas necesarias para que puedan seguir creciendo, acertando y equivocándose con sus decisiones, pero que esos errores no sean irreversibles, que sean solo otra forma de aprender.

Esto se encuentra en consonancia con el derecho a ser escuchado consagrado en el artículo 12 de la Convención de las Naciones Unidas sobre los Derechos del Niño, que implica dar su opinión libremente y tenerla en cuenta en función de su edad y madurez.

De este permanente debate y, sobre todo, de la experiencia de escuchar a los niños es que pudimos asumir que ellos ya no son, y creemos que no volverán a ser, aquellos que se tuvo en mira al dictar las legislaciones civiles que todavía siguen vigentes. Los niños deben ser protegidos en forma rotunda por cada uno de los responsables en dicha tarea, pero también han demostrado una evolución en su pensamiento y participación que requiere que tomemos conciencia de que es imprescindible transmitirles la necesidad de que se involucren en el cuidado de su propia privacidad e incluso en la de sus pares.

El acceso a internet como un derecho

Que el acceso a Internet es un derecho humano universal y reconocido internacionalmente no es una novedad, como tampoco que Internet es una herramienta de comunicación que es considerada imprescindible para materializar la libertad de expresión y la circulación de la información. Tampoco es un concepto nuevo, pero sí se ha replanteado en el ámbito internacional, que esa libertad de expresión y esa posibilidad de comunicarse que nos permite Internet debe ser defendida y protegida.

A su vez, el reconocimiento que se ha hecho del derecho que tienen los niños de acceder a la información implica que, como contrapartida, debamos realizar un esfuerzo particularizado para que ese acceso sea valorado en un doble sentido: como un beneficio, con todas las posibilidades positivas que abre, y como un riesgo, por todas las implicancias negativas que presenta. Este esfuerzo debe, en definitiva, orientarse a una educación en habilidades.

Una nueva forma de ver el mundo

Para poder educar niños en habilidades que les permitan discernir entre beneficios y riesgos, es indispensable entender que la forma de ver el mundo de los niños de hoy no es necesariamente similar a la de los adultos. La brecha generacional, sumada a la brecha digital, plantea diferentes formas de percibir el contexto y de apropiarse de las herramientas tecnológicas.

Los términos “nativo” e “inmigrante” digital sirven para entender las diferencias que surgen entre aquellos que deben aprender sobre las TIC y los que, al haber nacido y crecido con ellas, las utilizan como algo natural que no requiere aprendizaje.

Los nativos digitales no usan sino que atraviesan la tecnología. No hay un planteamiento sobre cómo funciona un dispositivo, o cómo funciona una herramienta. Hay un uso intuitivo

y el dispositivo es un tema secundario, es una herramienta que les sirve para acceder a la conexión. Como concepto unificador de los distintos dispositivos surge la "pantalla". Los niños hoy se conectan a través de pantallas, preferentemente táctiles.

No se trata de haber nacido a partir de un año determinado; se trata de haber nacido en un contexto donde el uso de la tecnología ya se encontraba incorporado y donde no se tiene registro de una vivencia sin el tipo de tecnología del cual estamos hablando.

¿Cuál es la utilidad de esta clasificación tan de moda? Que pueden establecerse a partir de esta distinción situaciones de investigación, estudio y análisis, pero siempre teniendo en cuenta que la variable "fecha de nacimiento" no es la definitoria. Sin embargo, a los fines prácticos no vemos una utilidad en la utilización de una clasificación que divide entre nativos digitales o no, ya que profundiza una brecha a la hora de encarar la concientización.

Cuando tenemos que abordar la tarea de concientizar a los niños y adolescentes, debemos pensar que no le hablamos a una masa compuesta exclusivamente por nativos digitales. Nuestro discurso debe tener en cuenta distintas realidades y distintos aspectos de un mismo fenómeno, y no profundizar las diferencias.

El rol de los padres

Los padres de niñas, niños y adolescentes que hoy acceden a las tecnologías tienen diversa formación respecto a este fenómeno. Algunos pueden comprender el alcance de la temática, pero seguramente sea un grupo minoritario.

Hemos visto que a lo largo de los últimos años se ha enfocado en la necesidad de que los padres se involucren con lo tecnológico, como también se han sostenido los beneficios de que utilicen las mismas redes sociales que sus hijos.

Sin negar que es sumamente positivo que los padres aprendan a manejar las herramientas tecnológicas, aprovechar sus ventajas y conocer sus riesgos, el rol del padre debe enfocarse en lo preventivo y lo educativo. Primero, debe existir una comprensión del fenómeno, más allá de la cuestión tecnológica. Esto quiere decir comprender que hoy existe una banalización de la privacidad, una sobreexposición de la imagen y una falta de límites entre lo que es íntimo, lo que es privado y lo que es público. Frente a esto, el uso en sí mismo no es lo más urgente para que un padre aborde, como sí lo es que tome conciencia de esta nueva fenomenología.

El rol del padre se presenta dentro de lo que es su misión fundamental: construir la socialización de su hijo, poner un límite claro y tener una presencia acorde a la edad y al nivel madurativo. Por eso el desafío para los adultos debe ser participar en el proceso de socialización y

crecimiento de los niños en su interacción con las TIC, más allá de que no cuenten con los conocimientos técnicos que ellos poseen. La importancia del rol del adulto pasa por brindar una mirada crítica y reflexiva de todo este proceso, y brindar los consejos y/o el asesoramiento correcto ante determinadas cuestiones que derivan del uso de la tecnología.

Para poder también incluir su rol educativo y formador (absolutamente distinto al rol educador de un docente) debe haber una comprensión sobre las conductas típicas de los niños, niñas y adolescentes presentes en el uso de las tecnologías. Hay que hacer una evaluación de la situación desde el marco de valores de cada familia, ya que la valoración ("esto es bueno", "esto es malo") es absolutamente privativa del ámbito familiar, y es en función de eso que se podrá determinar qué conductas son las esperadas en el uso de lo tecnológico dentro de esa familia. El análisis debe estar seguido también de un razonamiento. Hoy los niños, niñas y adolescentes manejan un cúmulo de información que les permite el debate, por lo tanto, más allá del límite concreto que puede y debe establecer cada padre, debe brindarse también una explicación clara de las razones.

Para poder brindar esas razones, debe tenerse un conocimiento de las consecuencias de los actos de nuestros hijos en el uso de la tecnología. Por ejemplo, un padre debe saber que una imagen subida hoy con un contenido inadecuado, no podrá ser recuperada, pero además producirá un perjuicio a largo plazo. Los niños y adolescentes se caracterizan por no representarse las consecuencias de sus actos presentes en un futuro que les parece muy lejano, cuando en realidad se trata de futuros que pueden ser tanto cercanos como lejanos (por ejemplo, las consecuencias de una imagen subida a una red social en el ámbito escolar).

El rol del estado

Uno de los cambios más relevantes que conlleva internet es que obliga a replantear la territorialidad en general y del Estado en particular.

Las leyes, normas y reglas que regían antes de internet podían enmarcarse en un país, comunidad o cualquier otro tipo de territorio delimitado. La web puso en jaque ese tipo de límite y obliga a repensar la forma en que un Estado puede ejercer sus obligaciones en el marco de las nuevas tecnologías.

Sin embargo, dentro del desafío de ubicar al Estado en el contexto de las TIC, encontramos algunos roles que con seguridad debe representar y que son propios de nuestra área: debe comunicar, informar y concientizar sobre aspectos tanto generales como particulares acerca de la temática de la protección de los datos personales en internet.
El espacio de la prevención en el área que abordamos no requiere de un territorio definido y es por eso que el Estado puede y debe estar presente. Los riesgos que existen en el mundo digital respecto

de los datos personales, la intimidad y la privacidad, tienen que ser informados por programas estatales que focalicen sus acciones en llevarle a la población información seria sobre el tema.
La información que debe proveer el Estado es necesario que cuente el detalle tanto de los riesgos que puede la población encontrarse como las formas de prevenirlos y gestionarlos en caso que ocurran. Debe asimismo informar sobre otros organismos estatales o de la sociedad civil que trabajen las temáticas y a los que se pueda recurrir para asesoramiento.

Es también responsabilidad estatal fomentar la idea de que cada persona es dueña de sus datos personales y por lo tanto, responsable por cuidarlos y elegir quién y cómo los tiene. Apoderarse de la información que habla de nosotros debe ser el núcleo de un cambio de conducta que se vuelve indispensable en un contexto donde internet atraviesa nuestras rutinas casi en su totalidad. Este cambio de conducta debe ser liderado por el Estado que, como protector de los derechos de los ciudadanos, y sin buscar fines de lucro, debe cuidarlos y brindarles información para manejarse en un mundo liderado por grandes empresas con grandes intereses.

En lo que respecta a los ámbitos legales y jurídicos, resulta indispensable que los Estados de una misma región trabajen en conjunto para acompañar la dinámica de Internet, que no respeta fronteras. Cerrar puertas y legislar para un país sería anacrónico y, por lo tanto, de escasa utilidad.

Cuando los Estados piensen acciones legales en conjunto, va a ser necesario que ubiquen a internet como lo que es: una herramienta que potencia o expone distintas temáticas existentes fuera de ella. Es por eso que va a ser clave no legislarla como un espacio separado, sino entender tanto su dinámica como las acciones que en su marco ocurren.

DECLARACIÓN DE RIOBAMBA, HACIA LA UNIFICACIÓN DE CRITERIOS Y MEDIDAS DE SEGURIDAD EN PROTECCIÓN DE DATOS[6]

Desde la evolución del ser humano, el acceso y la creación de la información ha sido constante, es así que al verse vasta y extensa en el mundo entero ha necesitado de un cierto cuidado, sobre todo por el tipo de información que se percibe y recepta entre intercomunicadores, con más motivo la de carácter sensible, por lo que para la protección de la información y el dato, y con el pasar del tiempo, se han creado medidas que pueden asegurar su privacidad y legitimidad frente a terceras personas que quieran hacer un mal uso de esta o, inclusive, apoderarse con fines pecuniarios.

La ausencia de una cultura en seguridad de la información por parte de administraciones públicas, empresas y ciudadanos es palpable. Ello origina riesgos de seguridad de los datos ante la no adopción de medidas que precautelen su seguridad, así como para evitar la obtención de ventajas derivadas de la implantación (mejora de la imagen corporativa, aseguramiento de la continuidad del negocio ante eventos relacionados con la seguridad de la información).

La Comisión Europea en el documento «La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI», de 25 de enero de 2012, utiliza la expresión "nuevo y complejo entorno digital actual" para referirse al contexto en el que se le plantean retos a la protección de los datos de carácter personal, una expresión que también resulta de aplicación a los retos que, con carácter general, se le plantean a la seguridad de las tecnologías de la información y la comunicación.

Esa complejidad a la que hace referencia la Comisión Europea está formada por diferentes variables, todas y cada una de ellas, a su vez, con sus complejidades:

1. La rápida evolución de las tecnologías y de su uso social: en el desarrollo e implementación de los productos y soluciones tecnológicas, pero también en su uso, se prioriza la funcionalidad por encima de otros criterios, como el de la seguridad de la información, que suele descuidarse o dejarse en un segundo término; ese acelerado

6. La Declaración de Riobamba, hacia la unificación de criterios y medidas de seguridad en protección de datos, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en la Universidad de Chimborazo (ciudad de Riobamba de la República del Ecuador), el 29 de marzo de 2014, por Alexander Cuenca Espinosa, en el transcurso de la Inauguración del Curso de Formación y Especialización para Peritos Profesionales en Ecuador. La Declaración fue elaborada por Ramón Miralles López, Alberto Cuesta Ureña, Francisco Ramón González-Calero Manzanares, Alexander Cuenca Espinosa, Romina Florencia Cabrera, Javier Sempere Samaniego, Javier Villegas Flores, Dulcemaría Martínez Ruíz, Marta Sánchez Valdeón, María Paulina Casares Subía, Edgar David Oliva Terán y Alexander Díaz García, coordinados por Daniel López Carballo.

ritmo de propuestas tecnológicas y de servicios difícilmente pueden ser asumido por los legisladores y reguladores, al menos con los mecanismos normativos tradicionales.

2. La extraordinaria capacidad de procesamiento de la información: tanto desde la perspectiva cuantitativa (volumen de información), como cualitativa (diferentes tipos de informaciones), con efectos positivos, pero también con impactos negativos, ya que esas capacidades también se ponen al servicio de lo ilícito.

3. El hecho de que la información tenga un valor económico: la información es un objeto susceptible de comercialización, la compra/venta de información tanto de manera lícita como ilícita, constituye una actividad más de negocio, formando ya parte esencial y motor de la economía del siglo XXI, donde el desarrollo de la sociedad de la información y progreso económico van estrechamente unidos, pero en paralelo también se ha incorporado al catálogo de actividades delictivas de grupos altamente organizados y profesionales. Los "ciberataques" masivos, sin otro objetivo que entorpecer o importunar, han pasado a la historia, ahora se trata de ataques directos, absolutamente dirigidos, que tienen objetivos e intereses claros y definidos. Hay que destacar que incluso personas en el mercado de la Deep Web venden sus conocimientos para el hurto de información a terceras personas, como industrias, corporaciones, para otras en ventaja de la información que poseen pueden generar más que las empresas de su competencia, en lo que se denomina "competencia desleal", más por la atribución de tener información adicional ilícitamente.

4. La confrontación entre la seguridad pública y los derechos y libertades individuales: las tecnologías, y especialmente Internet, están mermando sustancialmente los logros en derechos y libertados conseguidos a lo largo de varios decenios, la intromisión en la vida privada, la alteración de la presunción de inocencia o la censura de Internet, son tan solo unos ejemplos de las actividades lideradas por los Estados cuando actúan como garantes de la seguridad pública o nacional.

5. La globalidad del entorno digital: lo que comporta, a la práctica, la transformación del concepto de territorialidad y de las fronteras entre Estados, con las dificultades que ello conlleva para la aplicabilidad de las normas, la determinación de la jurisdicción competente y la ejecución de las decisiones de las autoridades, aunque todo ello solo sea, en estos momentos, "la punta del iceberg".

Si a esa complejidad le añadimos los diferentes actores que despliegan su papel en ese escenario, esa complejidad se ve claramente amplificada. Las empresas y grandes corporaciones con sus intereses empresariales, los ciudadanos de manera individual o colectiva (lo que incluye a los menores, los grupos de presión de diversa índole y tendencia, los Estados con sus servicios de

inteligencia y cuerpos de seguridad, la delincuencia organizada, los grupos de activistas, y otros actores) todos ellos actuando en el mismo plano pero con diferentes intereses y capacidades. Incluso, se está produciendo un cambio en los hábitos de la criminalidad y del espionaje y "guerra" entre países. Así, sobre el primero crece la criminalidad en la red bajando la que se produce en el mundo real; sobre la segunda, se habla de "ciber-guerra".

A toda esa magnitud del entorno digital se une el hecho de que las relaciones laborales, interpersonales, educativas, de ciudadanía, de negocio, etc., se despliegan tanto en el plano presencial como en el plano lógico o virtual, de manera que la realidad finalmente está formada por la suma de ambos espacios, lo que sucede en el plano virtual tiene consecuencias en el plano físico y viceversa.

Si a todo lo antedicho le sumamos una generalizada falta de cultura de seguridad de la información, especialmente entre la ciudadanía, pero no exclusivamente, ya que también afecta a las empresas y al sector público, que con carácter general no son conscientes de los riesgos que para sus actividades, incluso para su supervivencia, conlleva la no implantación de las medidas de seguridad de la información adecuadas, es decir, basadas en la evaluación y gestión de los riesgos a que están sujetos sus sistemas de información, junto con el hecho de que tampoco dedican demasiados esfuerzos a la gestión de su seguridad, da como resultado un panorama, al menos desde la perspectiva de la seguridad de la información, cuando menos, caótico.

Estamos ante un cambio de paradigma de las amenazas a que están expuestos los sistemas de información, lo que hace preciso un cambio de actitud, si bien los principios tradicionales de la seguridad de la información siguen siendo vigentes, deben ser potenciados y reforzados para minimizar los impactos negativos.

Los impactos negativos se disminuirían educando a los ciudadanos en los lineamientos de la Sociedad de la Información, brindando herramientas para que estos puedan proteger sus datos del entorno digital que hoy en día compromete y rodea al menos a un cuarto de la población mundial, quien tiene acceso a algún tipo de tecnología en donde su información personal puede ser vulnerada.

Cuestiones tan simples como la implantación de medidas de seguridad preventivas, reactivas y de recuperación, es decir, saber cómo actuar para protegerse antes, durante y una vez se ha producido el incidente, no forman parte de las prioridades, ni tan solo de la cultura, de la mayoría de los actores que desarrollan sus actividades en plena sociedad de la información.

Las consecuencias negativas de no tener en cuenta, con suficiente antelación y de manera planificada, cómo proteger los sistemas de información resultan evidentes, lo mismo de evidentes deberían ser los impactos positivos derivados de la capacidad para prevenir y reaccionar antes de que se produzcan los ataques a los sistemas de información, y de recuperar la situación previa al incidente de seguridad, con las mínimas afectaciones posibles.

La seguridad de la información debe ocupar por tanto el lugar que le corresponde, debe estar presente, junto con los aspectos funcionales y de negocio, en las primeras etapas de desarrollo de las soluciones y productos tecnológicos, y de sociedad de la información, pero también debe gestionarse de manera continuada y adecuada. La apuesta e impulso por el privacy by desing, es decir que el producto o servicio desde su gestación esté empapado de privacidad ofrece gran utilidad, ya que uno de sus pilares debe ser la seguridad de los datos.

Cada empresa está constituida por diversos elementos, cada uno de ellos son los que le otorgan la eficacia y sostenibilidad necesaria para que la empresa pueda mantenerse estable. Dentro de estos activos, necesariamente se debe hablar de la seguridad de información, esto en el entendido de que las empresas y su "saber industrial", su "saber cómo" y "datos privados sobre sus clientes" es traducido y plasmado en bits, es decir, su manera de comportarse y con quiénes se comportan las empresas, se encuentra almacenado de manera digital, ya sea en sus mismas oficinas o en un servicio de cómputo en la nube externo.

Es precisamente este elemento de información aquel que podría reflejarse como el esqueleto del modelo de negocios de la empresa; es tal la importancia de esta información que de ser obtenida de manera ilegítima, podría significar la desacreditación de la empresa.

Mientras más importante sea un elemento en la empresa mayor debe ser la tutela que reciba por la misma, al momento en que se comprende el valor de la información y su fragilidad en cuanto a su destrucción, manipulación y acceso indebido, es cuando las empresas deben velar por la implementación de medidas de seguridad.

Cuando pretendemos respetar las normativas de privacidad de los distintos Estados iberoamericanos, lo natural es acudir a la legislación propia de cada territorio y comprobar cuáles son los principios rectores y las medidas de seguridad aplicables. Pues bien, ese listado de medidas de seguridad tanto técnicas, organizativas como jurídicas, se deben implementar en toda entidad que trate datos de carácter personal en aras de protegerlos. Son medidas que deben ser homogéneas para permitir la interoperabilidad de protocolos de seguridad, redes y sistemas en un mundo globalizado. Estas medidas además no tienen en cuenta la dimensión y especificidades de las organizaciones basándose, en su mayoría, únicamente en la sensibilidad de la información personal tratada.

Además, no debemos considerar que la adopción de las medidas de seguridad es únicamente un trámite impuesto por la normativa, sino que su función principal es asegurar los activos de la organización, que no son otros que los datos de las personas.

Pero la tendencia de las legislaciones de privacidad es alcanzar una mayor personalización al proteger la información personal de los individuos que se relacionan con las entidades y conseguir que éstas controlen y resuelvan más eficazmente las posibles fugas de información.

Para lograr este segundo objetivo un ejemplo es Europa, en el nuevo Reglamento que se está preparando, encontramos la obligación de comunicar a las autoridades de control las brechas de seguridad que se produzcan en un periodo de tiempo relativamente corto, 72 horas. Esta obligación de notificar es incluso posible que se extienda a los afectados por la misma, como ya ocurre con los operadores de servicios de telecomunicaciones. De esta forma, se busca una proactividad, de manera que los afectados puedan adoptar las medidas que fuesen necesarias para proteger sus datos (como por ejemplo, cambiar una contraseña si ha habido una fuga de las mismas que afecten a gran cantidad de usuarios), así como una transparencia en la gestión por parte de las organizaciones. Por lo tanto, la tendencia de introducir medidas destinadas a favorecer el principio de accountability o rendición de cuentas por parte de empresas, corporaciones o administraciones públicas, debería generalizarse, ya que obligan a tomar en cuenta la seguridad de los datos.

Por otra parte, se intenta personalizar las medidas a ejecutar estableciendo la obligación de elaborar las llamadas "evaluaciones de impacto sobre privacidad" (Privacy Impact Assessment). Se trata de un informe que al igual que la Privacidad por Diseño, también está previsto en el futuro Reglamento de Protección de Datos de la Unión Europea y se encuentra vigente ya en algunos países, sobre todo de influencia anglosajona. Así, por ejemplo, el organismo supervisor de protección de datos en el Reino Unido, el ICO (Information Commissioner´s Office), ha elaborado varios manuales en los que se explica cómo elaborar una PIA. En España la Agencia Española de Protección de Datos está trabajando en esa misma línea, aunque de momento no será obligatorio realizarla. Con este panorama y siendo una medida que refuerza la seguridad de los datos, se hace necesario su generalización en las diferentes legislaciones sobre privacidad y seguridad de la información.

Esta "declaración de impacto" es una obligación similar a las evaluaciones de impacto ambiental exigidas en las distintas normativas. Una declaración de impacto no debe ser una mera verificación de cumplimiento normativo. Consiste en la elaboración por parte del Responsable del Tratamiento de un análisis de riesgos con la finalidad de determinar si el tratamiento que llevará a cabo entraña riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines. Un hecho a destacar es que las autoridades de control podrán conocer estas evaluaciones de impacto puesto que deberán hacerse públicas las conclusiones por el equipo encargado de realizarlas, por ejemplo por medio del sitio web de la organización.

Las evaluaciones deberían contener, como mínimo una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a los riesgos y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales.

Además, para realizar un PIA es importante que exista una colaboración total en la organización, de forma que participen todos los agentes implicados (por ejemplo, el departamento jurídico junto con el departamento que haya desarrollado una aplicación).

El responsable del tratamiento tiene que recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

Otra buena práctica –aun sin ser obligatoria– puede ser la autorregulación por parte de la entidad adoptando un sistema de gestión de seguridad de la información ISO 27001. Esta medida reforzaría uno de los pilares de una Declaración de Impacto, a saber la seguridad de los datos, eso sí, teniendo presente que los riesgos de incumplimiento normativo deben ser evitados o eliminados, nunca asumidos, como así se indicó en la 6ª Sesión Anual Abierta de la Agencia Española de Protección de Datos.

Desde un punto de vista jurídico, la adopción o no de las medidas de índole técnica y organizativas destinadas a garantizar la seguridad de los datos tiene unas claras consecuencias.

Así, nos encontramos ante una normativa de privacidad relativamente joven en todos los países de Iberoamérica. Este hecho provoca el desconocimiento de los preceptos que conforman las mismas. Un problema, sin duda, en el momento de implementar las obligaciones recogidas, pero que se acrecienta cuando una organización recibe una sanción establecida en dichas normativas por la desestabilización económica que puede sufrir la entidad.

Para garantizar el adecuado tratamiento de los datos personales, uno de los elementos más importantes para cumplirlo y alcanzarlo son las medidas de seguridad, las cuales y como encontramos en diversas legislaciones iberoamericanas, no solo se refieren a elementos técnicos o informáticos, sino que se refieren también a elementos administrativos o físicos que permitan la protección de los datos personales y que eviten la pérdida, alteración, destrucción, acceso, uso o tratamiento no autorizado.

Ahora bien, realizando un viaje por algunas de las legislaciones que en materia de datos personales existen en Iberoamérica, nos encontramos con el hecho de que en términos generales se establece la obligación para el responsable, encargado o usuario de los archivos de datos que adopte las medidas de seguridad técnicas, administrativas o físicas, que le permitan garantizar la seguridad y confidencialidad de los datos personales, evitando con ello riesgos o usos, accesos y tratamientos no autorizados o fraudulentos.

En algunas legislaciones como la mexicana y la costarricense, se establece que para el establecimiento de las medidas de seguridad los responsables no adoptarán medidas de

seguridad menores a las que utilicen para su propia información o los que sean adecuados a los desarrollos tecnológicos o mecanismos de seguridad adecuados.

Para lo anterior, el esquema de implementación de las medidas de seguridad consistirá en la adopción de ciertos elementos y características generales que se irán adecuando a las necesidades de las empresas, organizaciones o modelos de negocio de los que se trate.

Citando lo establecido en las mencionadas legislaciones de México y Costa Rica, para determinar las medidas de seguridad el responsable o, en su caso, encargado del tratamiento deberá considerar al momento de determinar las medidas de seguridad aplicables a cada organización el riesgo inherente por tipo de dato personal, la sensibilidad de los datos personales tratados, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, el número de titulares de datos personales, las vulnerabilidades previas ocurridas en los sistemas de tratamiento, el riesgo por el valor potencial (cuantitativo/cualitativo) que pudieran tener los datos personales tratados para terceras personas no autorizadas y los factores que puedan incidir en el nivel de riesgo o que provengan de otra legislación aplicable al responsable.

Una vez definidas las medidas de seguridad por parte del responsable, para garantizar su cumplimiento, ejecución y seguimiento, a su vez, el responsable deberá considerar acciones tales como la descripción detallada del tipo de datos tratados y almacenados, el inventario de datos personales, sistemas de tratamiento e infraestructura tecnológica utilizada, análisis de brecha (diferenciación entre medidas de seguridad existentes y las faltantes) y el plan de trabajo para implementar las medidas de seguridad faltantes (análisis de brecha), entre otras.

Adicional a lo anterior, México, por ejemplo, remitió las Recomendaciones en materia de seguridad de datos personales y mediante las cuales, se exhorta a los responsables y en su caso, encargados, para que adopten un Sistema de Gestión de Seguridad de Datos Personales basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Con dichas Recomendaciones se pretende facilitar a los responsables el contar con una guía que les permita mantener vigente el cumplimiento de la legislación y fomentar las buenas prácticas en materia de datos personales.

Por otra parte, nos encontramos otro tipo de legislaciones que catalogan los datos personales o las medidas de seguridad en niveles, y en base a los mismos, establecen o enuncian los diferentes parámetros o elementos que permitan garantizar la seguridad de los datos personales.

Ejemplo de lo anterior lo encontramos en la legislación argentina, la Disposición 11/2006 sobre las Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y privados,

se clasifican las medidas de seguridad en tres niveles: básico, medio y crítico (aplicable a archivos, registros, bases y bancos de datos personales sensibles).

Sigue un sistema similar en cuanto a la implementación de las medidas de seguridad, es Perú, ya que tanto en el Reglamento de la Ley de Datos Personales como en la Directiva de Seguridad de la Información establecen diferentes niveles de datos personales y sus correspondientes medidas de seguridad, donde se establecen los lineamientos para determinar las medidas de seguridad mediante un sistema de categorización más complejo y detallado que en el caso anterior; para cada grupo se consideran variables sobre el tipo de dato, así como variables cuantitativas relacionadas con el número de personas respecto de las cuales se maneja la información y el número de datos personales que son contenidos o tratados en cada base de datos, estableciéndose los niveles básico, simple, intermedio, complejo y crítico.

De manera relacionada a las medidas de seguridad, las distintas legislaciones contemplan el hecho de que en caso de que lleguen a existir vulneraciones a la seguridad durante el tratamiento de los datos, los responsables tendrán la obligación de informar de manera inmediata al titular (en el caso de México, Uruguay y Costa Rica) o a la autoridad competente (en el caso de Colombia). Con la finalidad de que el titular pueda tomar las medidas necesarias o prudentes en defensa de sus derechos y/o de que las autoridades puedan ejercer las acciones que permitan efectuar las investigaciones o procedimientos judiciales o administrativos que correspondan.

Las sanciones que más proliferan son las administrativas a lo largo de los textos legales, y en caso de no implementar alguna de las medidas de seguridad, las sanciones alcanzan sumas económicas muy elevadas, llegando a poner en jaque la estabilidad del negocio del que las recibe. En todo caso, no debemos olvidar que la normativa europea permite que en la vía jurisdiccional ordinaria una persona reclame a una entidad privada una indemnización cuando considera que la vulneración de sus derechos le ha provocado daños y perjuicios. En el caso de las entidades públicas, como norma general, la indemnización se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En tanto, el tratamiento de datos personales afecta a la esfera más íntima de las personas y su protección viene recogida en la mayor de las Constituciones iberoamericanas; en aras a una mayor defensa del derecho al honor, a la privacidad, al buen nombre y la intimidad de las personas, se debe dotar el ordenamiento penal de instrumentos preventivos y coercitivos que eviten conductas delictivas que pongan en juego la seguridad de la información, ataques, tráfico de datos, accesos no autorizados, suplantación de identidades o utilización de la información con finalidades al margen de la ley.

Por otra parte y desde el punto de vista administrativo, existe la figura del apercibimiento que se ha introducido en los últimos tiempos con el objetivo que las instituciones reaccionen y cumplan con las medidas de seguridad bajo la amenaza de sanción económica.

En cambio, en algunos Estados como México sí que se establecen sanciones penales o privativas de libertad en caso de no cumplir con las obligaciones fijadas en la normativa de protección de datos. Alcanzando hasta los diez años de cárcel en los casos más graves.

No cabe duda que en innumerables ocasiones las sanciones económicas han sido desproporcionadas y no han tenido en cuenta la dimensión de la entidad que las recibe. Se han debido cerrar negocios por el hecho de no poder afrontar la cuantía impuesta por una autoridad de control, por ello la tendencia actual es a modular la sanción en relación al volumen de negocio de la entidad y, sobre todo, atenuarlas en base al espíritu y preocupación empresarial en la implementación de medidas de seguridad de protección de datos personales.

La seguridad en toda la amplitud de la palabra debe hacer referencia a otorgar intangibilidad al activo, la certeza que no será destruido ni dañado, o accedido por terceros no autorizados. La seguridad que ha de buscarse dentro de una institución no debe ser solo la seguridad informática, sino la seguridad de la información, en el entendido de que una cultura de seguridad debe ser cultivada de manera interna y en todos los niveles, tanto administrativos como ejecutivos, no siendo confiada solo a dispositivos electrónicos programados.

Si bien la información es un activo de la empresa, y la fuga o vulneración del mismo supone grandes pérdidas monetarias, no se puede olvidar que la implementación de medidas de seguridad es una inversión cuyas ganancias son vistas a largo plazo. Estos beneficios se traducen en generación de confianza, imagen corporativa, optimización de recursos y capital humano y trazabilidad de la información entre otros.

Mediante la delimitación de perfiles de usuarios en el acceso a la información conforme a las funciones que desarrollan y su puesto de trabajo se optimiza el tiempo dedicado, asignando a cada empleado los recursos necesarios para desarrollar su trabajo, con lo que conseguimos, por un lado, optimizar el tiempo real de trabajo (ya que solo podrá acceder a la información precisa para sus funciones) y por otro, un uso racional de los recursos. Como consecuencia de la adecuación de los procedimientos y sistemas en protección de datos, se pueden descubrir procesos innecesarios, redundantes, o ineficientes que pueden mejorarse sustancialmente con muy poco esfuerzo.

Proteger la información adoptando medidas de seguridad debe seguirse de una mayor educación, cultura y prevención, que son los lineamientos más avanzados en materia de seguridad. Estos son controles regulares que se realizan al personal de la empresa para ver qué tipo de actos cometen y si es que estos podrían traer consecuencias desfavorables para la seguridad.

La libertad de expresión, el honor, la intimidad, la privacidad y la protección de datos personales, como derecho autónomo e independiente, deben estar equilibrados con el concepto de seguridad, tanto en materia empresarial como pública.

La seguridad de los datos personales implica un delicado balance de distintas cuestiones, tales como el nivel de riesgo, la cantidad de datos protegidos por persona, el número de personas cuyos datos personales están siendo tratados, los posibles daños o amenazas, costos financieros y de eficiencia de las medidas de seguridad implementadas para reducir el riesgo y las que se relacionen con las características específicas de la industria de que se trate, tal y como lo mencionaba Daniel Solove.

La integración económica y social resultante del establecimiento y funcionamiento de un mercado globalizado ha implicado un desarrollo notable de los flujos transfronterizos de datos personales entre distintos agentes públicos y privados establecidos en diferentes países.
Este flujo de datos se ha visto favorecido por factores como el avance de las tecnologías de la información y, en particular, el desarrollo de Internet, que facilitan considerablemente el tratamiento y el intercambio de información, y que permiten compartir recursos tecnológicos, centralizar determinadas actividades y procesos, y abaratar costes en la prestación de servicios por la propia empresa fuera del país en el que se encuentra establecida.

DECLARACIÓN DE CIUDAD DE PANAMÁ, HACIA LA UNIFICACIÓN DE CRITERIOS Y GARANTÍAS PARA LA PROTECCIÓN DE LA IDENTIDAD DIGITAL Y EL DERECHO AL OLVIDO[7]

El mundo virtual de Internet y las Redes Sociales posibilitan un sinfín de interconexiones y comunicaciones ilimitadas y heterogéneas que logran efectos de conectividad e interacción social antes impensados, pero que también logran traspasar límites físicos, psicológicos, emocionales, económicos, culturales, políticos, laborales, educativos y sociales, perdiendo el protagonista del mismo, el ser humano, el control sobre sus acciones en la Red.

Su Identidad como persona se ve trasformada en lo que se denomina "Identidad Digital", un espacio virtual donde la subjetividad de los individuos da lugar al surgimiento de una identidad en entornos virtuales anónimos, en donde los individuos suelen jugar roles diferentes a los de su vida real. En este contexto, se establece un fuerte vínculo entre las estructuras psicológicas y los procesos sociales que conforman y atraviesan al sujeto, es decir, entre las normas que regulan el comportamiento colectivo y las estrategias del sujeto dentro del contexto social, que permiten su articulación con la trama social.

La construcción de la identidad es un proceso que se establece si hay coincidencia entre posicionamiento y aceptación. En las interacciones cara a cara, es difícil pretender ser quien no se es, en cambio, en el entorno de una red social es posible interactuar con otros sin que nada se revele sobre nosotros (subliminalmente muchas veces sí) construyendo la identidad deseada que en el mundo real no se puede obtener, construyendo los actores sus identidades y redundándolas, adaptándolas a sus expectativas y a lo que el mundo social les demanda.

Pese a que se puede recurrir a las herramientas jurídicas para rectificar errores o reclamar daños y perjuicios, depende de su acto voluntario, de conciencia, de decidir qué información personal o íntima va a darse a conocer públicamente y cuál no.
Muchas veces los ciber-delincuentes utilizan métodos de captación ilegítima de información o software especializado en vulnerar sistemas informáticos y no hay prevención que se puede utilizar, pero en los casos cotidianos en que nuestra vida es expuesta en el mundo virtual,

7. La Declaración de Ciudad de Panamá, hacia la unificación de criterios y garantías para la protección de la identidad digital y el derecho al olvido, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en el Auditorio Harmodio Arias del Colegio Nacional de Abogados de Panamá, el 23 de julio, en un evento organizado por la Comisión de Derecho de las Nuevas Tecnologías del Colegio, por el Presidente del Colegio, José Alberto Álvarez Álvarez. En el acto también intervinieron el Rigoberto González Montenegro, así como Lía P. Hernández Pérez, como Presidenta de la Comisión de Nuevas Tecnologías del Colegio. En la elaboración de Declaración intervinieron Francisco Ramón González-Calero Manzanares, Romina Florencia Cabrera, Javier Villegas Flores, Dulcemaría Martínez Ruíz, Marta Sánchez Valdeón, Edgar David Oliva Terán, Lía P. Hernández Pérez, João Ferreira Pinto, José R. Leonett, Diego Pérez Gutiérrez, Ruth Benito Martín y Alberto Martín Hernández, coordinados por Daniel López Carballo.

depende de nosotros mismos equilibrar la información personal que compartimos en la Sociedad de la Información.

La mejor herramienta de la seguridad es la prevención. Se debe tratar con un criterio razonable poder disfrutar del maravilloso mundo digital, resguardando nuestra información personal y nuestro derecho a la intimidad. El individuo debería tener protección de su persona y sus propiedades; es un principio tan antiguo como la ley, pero de vez en cuando es necesario definir de nuevo la naturaleza y el alcance de esa protección. Cambios políticos, sociales y económicos suponen el reconocimiento de nuevos derechos, y la ley, en su eterna juventud, debe crecer para satisfacer las nuevas demandas de la sociedad. Inicialmente, la ley dio remedio a la interferencia física con la vida y la propiedad privada, y ahora le toca hacerlo con la virtual.

Se debe lograr el equilibrio entre intimidad, privacidad, protección de datos personales, derecho al honor, a la asociación y a la libertad de expresión. Son todos Derechos Humanos reconocidos por los tratados internacionales, protegidos en las legislaciones nacionales y al alcance de la jurisdicción de los tribunales nacionales e internacionales que conocen sobre estas cuestiones, para proteger los derechos de los ciudadanos y de la comunidad internacional en general. Los Derechos Humanos deben estar siempre presentes en todo momento y lugar, como regla del ius cogens.

Los Derechos Humanos basan sus principios en la dignidad y valor de la persona humana; así lo estableció la Convención de Viena. Crean obligaciones de los Estados con los ciudadanos directamente; y más aún que su mención en los diferentes ordenamientos legales, vale el compromiso de los individuos con estos derechos que nos permiten relacionarnos en un entorno globalizado.

La identidad digital y su protección

El concepto de Identidad debe entenderse como el conjunto de rasgos propios de un individuo o de una colectividad que lo caracteriza frente a los demás; llevado al ámbito digital o a la exposición y desarrollo de tal identidad, en este contexto, tendremos conceptos como el que establece el Instituto Nacional de Tecnologías de la Comunicación (INTECO), "… puede ser definida como el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital".

La formación de la identidad es algo casi inconsciente, pues se forma a medida que nos desplazamos por el ciberespacio, es así como cada contacto cuenta, al igual que cada pensamiento o acto que realizamos en nuestras diversas redes sociales.

Si bien la identidad digital, en primera instancia, es generada por nosotros, se debe recordar que son otras personas también las que pueden ayudar a generar esta información, con solo

subir fotografías, comentarios y diversas actuaciones que puedan ser digitalizadas e indexadas a nuestro nombre, se estaría así contribuyendo a la formación de nuestra imagen digital.

Debe diferenciarse entre identidad digital e identidades parciales, cada identidad parcial corresponde a cada servicio o aplicación en Internet, como las redes sociales, usuarios de correo electrónico, entre otros, pero al final la suma de estas identidades parciales es lo que constituye la identidad digital.

Si bien en sus orígenes los componentes base de la identidad estaban disponibles por medios físicos o periodísticos tales como nombres, certificados de nacimiento, títulos universitarios o profesionales, cartas de no antecedentes penales o información de notas periodísticas, sin embargo, con la aparición de los instrumentos de digitalización, del impulso en el uso de computadoras personales y con el incremento en el uso de Internet, los datos e información que componen la identidad de una persona no solamente se dispersaron con mayor facilidad, sino que se incrementaron, al grado que ahora no solo tenemos dispersada en internet información que corresponde a la identidad de las personas en lo individual, sino también de las empresas, autoridades, grupos de trabajo u organizaciones varias.

Además, con los nuevos sistemas informáticos y de comunicación, sobre todo los móviles, día a día estamos arrojando información que incrementa datos a nuestra identidad digital, tal es el caso de los datos que arrojan la geolocalización, aplicaciones que predicen nuestros gustos y deseos, las que involucran reconocimiento biométrico.

Es Internet un espacio masivo de usuarios, donde muchas veces surge el temor de no saber con quién se está conversando, de si es o no es quien dice ser, es por ello que la identidad digital podría llegar a ser útil cuando cumple su labor de identificar a los usuarios, por ello se entiende que Internet acerca a sujetos que se encuentran tan distantes, que la única forma de conocerse es mediante estos medios.

Actualmente, el que cualquier persona pueda investigar y conocer nuestra identidad digital desde cualquier parte del mundo y, con ello, hacer un buen o mal uso de la información es tan importante y al mismo tiempo conlleva un gran nivel de riesgo, lo cual nos lleva a la reflexión de que deberíamos cuidarla como uno de los aspectos más preciados de nuestra vida.

Sin embargo, es preocupante cuando nuestra identidad digital sale de nuestro control, ya que la misma se va construyendo además con la información y datos que otras personas vayan generando respecto de nosotros, incluso, nuestra identidad digital llega a ser alimentada con la percepción o comportamiento que tienen las personas con las cuales nos relacionamos, de manera que incluso existen aplicaciones con las que no solo se analiza si las personas son susceptibles de recibir un préstamo o crédito, sino que además se toma en cuenta la

información que nuestros familiares y amigos en Facebook aportan sobre nosotros o, incluso, la información que arroja el mero hecho de tener a ciertas personas como nuestros contactos o la forma en la que interactuamos con ellos.

Las redes sociales, si bien son círculos meramente privados entre el usuario y sus contactos, en el supuesto que no se haya configurado bien el apartado de privacidad, puede ocasionar que esa información pase a formar parte de Internet, al ser indexada por cualquier buscador. Esto solo es una muestra de que la imagen que se ve de cada persona no es derivada exclusivamente por la pertenencia a una red social, y no son únicamente los contactos los que pueden llegar a acceder a esta información, sino que se debe hablar de usuarios de Internet y ya no tanto de contactos de redes sociales.

La identidad digital se compone por lo menos de información proveniente de tres grandes grupos: la generada por el propio individuo, la generada por terceros y la que se genera en el contexto de las relaciones del individuo.

Uno de los problemas de la identidad digital es la posibilidad que tiene un solo individuo de generar una pluralidad de identidades, si bien es cierto que hay a quienes les conviene trabajar en la correcta construcción de su identidad digital para adquirir más impulso o reconocimiento social o político, también lo es que pueden existir motivos por los cuales una persona desee permanecer en el anonimato que brinda Internet, ello por distintos motivos, tales como temas de seguridad, libertad de expresión, para ocultar o disfrazar los actos o consultas de información, o cuando simplemente se tenga el interés de que tales actos no afecten la identidad principal.

Esta cuestión puede representar un problema para las empresas, las autoridades o para quienes prestan servicios vía web, o cuando la contratación de los productos o servicios se realiza mediante estos medios, ya que es muy complicado saber quién es la persona que en realidad está realizando la transacción, quedando expuestos por ejemplo a fraudes cometidos por el uso de identidades digitales falsas, lo cual en combinación con el uso de tarjetas de crédito clonadas o robadas puede ser una herramienta muy peligrosa.

Debe tenerse en cuenta que, a diferencia de la identidad en el medio físico, en el cual es más fácil identificar a la persona que está realizando la operación, en el medio digital tenemos el problema de la falta de conexión entre una persona determinada y una identidad digital, tan incierto puede ser que al momento de offline la identidad digital puede dejar de existir.

La suplantación de identidad es otro de los problemas que afecta a una de las identidades parciales del individuo, es decir, se da una afectación a una de las cuentas o aplicaciones a las cuales tiene acceso el individuo, lo cual a su vez y dependiendo del grado de intromisión y del daño causado, puede llegar a cambiar en grado considerable la identidad digital del individuo.

Lo anterior puede ser realizado mediante distintos procedimientos, entre ellos, el uso del nombre o usuario de la persona, la generación de una identidad que ridiculice a la identidad original o el uso no autorizado de una cuenta; como sea, la consecuencia será la afectación a la privacidad, bienes, honor o reputación de una persona.

Otros de los problemas más comunes asociados a la identidad digital son las violaciones a los derechos a la privacidad, los derechos autorales, daño reputacional, sexting, bullying, entre otras actividades que van deteriorando o violentando la identidad digital de una persona, llegando a grados en los que incluso se llegue a afectar las relaciones personales y la vida íntima de la persona.

Reputación personal on-line y daño reputacional

Se toma la reputación como la opinión o consideración en que se tiene a alguien o algo o el prestigio o estima en que son tenidos alguien o algo. Según la definen diferentes autores, "la reputación online es el reflejo del prestigio o estima de una persona o marca en Internet. A diferencia de la marca, que se puede generar a través de medios publicitarios, la reputación no está bajo el control absoluto del sujeto o la organización, sino que la 'fabrican' también el resto de personas cuando conversan y aportan sus opiniones".

Debemos considerar que la identificación virtual es el conjunto de datos que nos permiten diferenciarnos suficientemente del resto de personas en un ámbito concreto. Estos datos suelen ser el nombre, apellidos, entre otros.

Resulta prácticamente imprescindible identificarse en redes sociales tales como Facebook o LinkedIn, cuyo principal objetivo es relacionar al usuario y permitirle que los demás usuarios lo identifiquen y compartir con ellos cierta información, en el caso de la primera red, con fines de ocio, en la segunda, por motivos profesionales.

Sin embargo, cuando los usuarios no persiguen el fin de comunicarse con los demás, sino que pretenden simplemente hacer comentarios (en muchas ocasiones dañinos), prefieren esconderse tras el anonimato.

Esto genera una problemática inmensa, sobre todo cuando los comentarios dañan la reputación de personas, que no pueden defenderse frente a estas personas anónimas.

Por ello, la reputación online no es un tema que preocupe solo a las empresas. También los particulares pueden verse afectados por suplantaciones, difamaciones o por el contenido que ellos mismos han subido a la red. El derecho al olvido pretende solucionar este problema.

Además de los métodos más comunes para dañar la imagen de una persona, como pueden ser las críticas en foros de opinión, últimamente se está poniendo "muy de moda" suplantar identidades virtuales; de hecho, este fue el principal motivo de denuncias relacionadas con Internet ante las diferentes autoridades de control en protección de datos en los últimos años.

Lo que antes se limitaba a aparecer en alguna página de contactos, porque alguien facilitaba tus datos a desconocidos, hoy se ha reemplazado por la creación de perfiles falsos en redes sociales, comunicándose el suplantador con tus amigos y conocidos, con el único fin de dañar tu imagen.

En el mundo 2.0, este tipo de suplantación es fácil, accesible y gratuita, ya que no se puede requerir y comprobar la identidad de la persona que se da de alta en una red social. Sin embargo, los suplantadores en algunos casos no son conscientes de que están cometiendo un delito de suplantación de identidad, tipificado en el artículo 401 del Código Penal, por el cual se prevén penas de seis meses a tres años de cárcel.

A pesar de ello, las reacciones más comunes ante este tipo de delito no son las denuncias, sino las solicitudes de baja a través de las propias redes sociales y las denuncias ante la Agencia de Protección de Datos.

Las redes sociales deben estar preparadas para este tipo de controversias y disponer de formularios para denunciar los hechos. No solo se pueden denunciar suplantaciones, también se puede denunciar si alguien considera que existen contenidos inapropiados en un determinado perfil.

Cuando una persona fallece, ya no solo hay que preocuparse de las repercusiones directas en la vida real, también hay que decidir sobre las repercusiones en la Red.

Internet se ha convertido en una herramienta de comunicación casi imprescindible para millones de personas, muy atractiva e interesante, entre otras ventajas, porque los servicios que ofrecen son gratuitos. Pero esa fácil accesibilidad es precisamente la que provoca que el problema surja cuando no se trata de introducir datos, sino de borrarlos, como por ejemplo, en el caso de fallecimiento de una persona.

La muerte de estas personas abre a sus familiares dos posibilidades: eliminar el perfil en la red social o permitir que se realice un homenaje en el mismo. Pero ¿están preparados los familiares para superar, no solo la muerte de una persona querida, sino también para borrar su huella?

No cabe duda que es difícil tomar cualquiera de las dos decisiones, pues en la primera te enfrentas a la repercusión que todos más tememos respecto a la muerte, el olvido y, en la segunda, te enfrentas al recuerdo permanente de quien se ha ido.

Las redes sociales han previsto “el homenaje” permitiendo a los familiares directos conservar el perfil del fallecido, con el fin de que no se produzca esa disminución masiva de usuarios de la red social.

Y el mismo derecho a conservarlo tenemos de eliminarlo: basta con que comprobemos la política de privacidad de la red y la familia solicite la cancelación de datos de la referida persona.

Y en el caso de personas sin familia, ¿qué ocurre con ellos? En este caso deberemos iniciar actuaciones judiciales.

El problema no se produce cuando un usuario le pide al titular de una red social que cancele toda su información, sino cuando esa información ha pasado de una red a otra, y ha traspasado muchas fronteras tecnológicas y geográficas. Es entonces cuando el derecho de cancelación de datos se convierte en una ingente tarea de búsqueda desesperada, dando lugar en la mayoría de los casos a la imposibilidad práctica de eliminar de manera permanente esta huella en Internet.

Reputación corporativa online

La identidad online de la empresa viene definida por el conjunto de información que aparece en Internet sobre la misma: datos, imágenes, registros, comentarios, etc. Dicha información engloba tanto aquellos contenidos que activamente genera la organización, como los comentarios y opiniones que los demás vierten en la corriente social. Este hecho hace que cada vez sea más importante la monitorización de la valoración que el público hace de la compañía en la Red y llevar a cabo una adecuada gestión de reputación online corporativa.

Las organizaciones difunden su imagen en Internet mediante herramientas como páginas web corporativas, blogs empresariales, perfiles y páginas en redes sociales. Más allá de lo que la propia empresa publique y dé a conocer de sí misma, la identidad digital corporativa se ve complementada con lo que los propios usuarios y clientes opinan sobre la empresa en Internet.

Incluso, no es necesario que una empresa se encuentre presente en Internet para que puedan surgir este tipo de opiniones sobre ella. Así pues, el contenido generado por terceros forma parte de su identidad digital de la misma manera que el creado por la propia empresa. La identidad digital corporativa, por tanto, puede ser definida como el conjunto de la información sobre una empresa expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha organización en el plano digital.

La Web 2.0 constituye un nuevo canal masivo de comunicación para las empresas, y las redes sociales representan una herramienta mediante la cual las organizaciones disponen de un feedback en tiempo real de clientes y usuarios. En la Web 2.0 cualquier empresa o profesional puede tener presencia digital gracias a clientes y usuarios sin necesidad siquiera de tener una

página web, tanto para hablar maravillas como para maldecir un servicio o producto. Es por ello que surge un nuevo concepto: la reputación online.

La reputación corporativa es el concepto que mide cuál es la valoración que hace el público de una compañía. Podría definirse como la valoración alcanzada por una empresa a través del uso o mal uso de las posibilidades que ofrece Internet.

Al mismo tiempo que la presencia de la empresa en medios sociales (por sí misma o por la acción de terceros) le reporta efectos positivos, existen diferentes amenazas que pueden generar impactos negativos en su imagen y reputación online. Una pérdida de confianza en la marca a partir de comentarios perjudiciales sobre un producto es un ejemplo de ello. Además, el efecto multiplicador de Internet posibilita que un incidente aislado (incluso generado fuera de la Red) se convierta en una situación de difícil solución.

En este sentido, cada vez es más frecuente descubrir noticias sobre crisis reputacionales en Internet, que impactan de tal forma en la imagen de la empresa, que los efectos perduran en el tiempo. A continuación se describen las principales amenazas para la identidad digital y reputación online desde el punto de vista de la seguridad.

Otro de los problemas a los que se enfrentan las empresas es la suplantación de identidad: la suplantación de identidad de la empresa en Internet es la usurpación de los perfiles corporativos por terceros malintencionados, actuando en su nombre. Dentro de este riesgo se contempla la creación o el acceso no autorizado al perfil de una empresa o entidad en un medio social y la utilización del mismo como si se tratara de la organización. Los atacantes crean perfiles falsos con varios propósitos, destacando el robo de información sensible de los usuarios de la empresa suplantada para la comisión de fraude online.

Registro abusivo de nombres de dominio: la amenaza se produce cuando terceros malintencionados registran uno o varios nombres de dominio que coinciden con la marca de la empresa, impidiendo a esta última utilizar dichas denominaciones en su negocio.

Ataque de seguridad DDoS: Ataque de Denegación de Servicio Distribuido, o ataque DDoS. Es el conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo, hablando en términos de seguridad informática. Para poder llevar a cabo el ataque, se requiere que varios equipos trabajen coordinadamente para enviar peticiones masivas a un servidor concreto, por ejemplo, accediendo a la página web y descargando archivos, realizando visitas, etc. Así consiguen saturar dicho servidor y provocar su colapso, al no poder este responder tal flujo de peticiones.

Fuga de información: en este caso, la buena imagen y el prestigio de una entidad puede verse comprometida por el robo de información sensible y/o confidencial (como por ejemplo,

datos personales de trabajadores y clientes, datos bancarios, informaciones estratégicas de la organización, etc.) y su revelación en Internet. De nuevo, el objetivo suele ser el lucro (por ejemplo, al obtener información bancaria de la empresa y sus clientes, o al extorsionar a la propietaria de los datos a cambio de un rescate), aunque también se distinguen otros motivos, como el espionaje industrial o el desprestigio a la organización.

Publicaciones por terceros de informaciones negativas: las críticas a las entidades son parte de la interactuación que ofrecen las plataformas colaborativas: no solo se está en la Red, sino que se conversa en ella. El hecho de que una falta de atención, un error en el servicio, un defecto en un producto, etc., sea comentado en Internet es igualmente una información valiosa para la empresa, que puede corregir el fallo en base a estos comentarios negativos. En estos casos, la diligencia de la empresa para dar una respuesta apropiada permitirá solucionar o aliviar la corriente de crítica que se ha generado y, en consecuencia, la recuperación de su imagen y reputación online. Asimismo, la realización de comentarios negativos o falsos sobre una organización puede tener consecuencias legales, contemplándose acciones tanto civiles como penales (en caso de que la ofensa en cuestión sea considerada una injuria o una calumnia) dirigidas a proteger el honor y reputación de la empresa.

Utilización no consentida de derechos de propiedad intelectual: Estos derechos tienen una doble dimensión: permiten a su propietario su utilización e impiden que un tercero lo haga, salvo que le ampare la correspondiente licencia de uso otorgada por el primero. Si se están utilizando o comercializando a través de Internet de forma no autorizada, la empresa propietaria de sus derechos se convertiría en víctima de un delito contra los derechos de propiedad industrial y posiblemente, en un delito de competencia desleal.

La empresa que haya visto dañada su reputación online tiene a su disposición una serie de herramientas legales para que su imagen se vea reparada. La Red no altera el contenido esencial de los derechos de las personas jurídicas. Sin embargo, sí existen particularidades específicas derivadas del entorno online que las empresas deben tener en cuenta a la hora de gestionar su reputación.

En primer lugar, el daño derivado del ataque a la reputación de una empresa realizado a través de Internet es difícilmente reparable de manera total. La difusión de una información publicada en la Red no tiene límites y, aun en el caso de que la información en cuestión sea retirada (por contravenir los derechos de la empresa), siempre se pueden mantener copias, pantallazos o descargas realizados antes de la eliminación.

En segundo lugar, y relacionado con lo anterior, las empresas deben considerar el llamado “efecto Streisand”, fenómeno en el que un intento de ocultamiento de cierta información en Internet resulta contraproducente, ya que ésta acaba siendo ampliamente divulgada, recibiendo mayor publicidad de la que habría tenido si no se la hubiese pretendido acallar.

Las legislaciones nacionales suelen reconocer los derechos al honor, a la intimidad personal y familiar y a la propia imagen, teniendo cabida en algunos ordenamientos jurídicos dentro del derecho al honor el derecho a la reputación corporativa. Así, reconocen expresamente que la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando la difame o la haga desmerecer en la consideración ajena. Por tanto, las empresas y organizaciones, en defensa de su derecho al honor, deben poder iniciar acciones civiles o penales para solicitar la retirada de la Red de informaciones que produzcan un perjuicio a su reputación. En la mayoría de las ocasiones nos encontraremos ante supuestos donde entran en conflicto, de un lado, el derecho al honor y, de otro, el derecho a la libertad de expresión e información.

El derecho al olvido o cancelación de datos

Resulta indudable que hay una serie de derechos que en el entorno digital quedan más expuestos a posibles vulneraciones, y por lo tanto su desarrollo y aplicación pasan a adquirir, en dicho entorno, mayor relevancia.

Hablamos, cuanto menos, del derecho a la intimidad personal y familiar, del derecho al honor, del derecho a la propia imagen (no olvidemos que de estos tres, aunque estrechamente interrelacionados, cada uno protege aspectos distintos de la persona y a cada uno se aplican criterios jurisprudenciales diferentes), de la libertad de expresión, el derecho de información, los de propiedad intelectual y por supuesto, también, el derecho a la protección de los datos personales. Todos ellos se encuentran íntimamente ligados a la identidad digital de la persona, en la medida en que inciden directamente en la construcción de aquellos de los rasgos que caracterizan a un individuo que quedan puestos de manifiesto en la denominada web 3.0.

Internet, tal y como lo disfrutamos hoy en día ha sufrido gran cambio respecto al que conocimos en los años noventa, que era mucho más estático y unidireccional, y en el que el usuario ejercía un papel casi del todo pasivo, sin que su conducta conllevara normalmente una reacción en la Red. Actualmente, en cambio, el usuario interactúa constantemente en Internet, se ha convertido en parte activa en la construcción del tejido de esta red de redes y su comportamiento puede llegar a provocar grandes reacciones. Este escenario, regido bajo el principio de neutralidad de la Red y teniendo en cuenta que el acceso a Internet llega cada vez a una mayor población (como es deseable), y además, por medio de más dispositivos (no digamos ya cuando vivamos el gran apogeo del Internet de las cosas), arroja unas características propias de la denominada web 3.0 que resultan de gran impacto para todos estos derechos. Tales características son: la amplificación (repercusión, alcance, rapidez y facilidad en la transmisión de la información), la accesibilidad a la información, más fácil, cómoda y barata, y la permanencia de la misma.

Ninguno de los derechos mencionados es absoluto y todos ellos, en su aplicación, encuentran su límite en otros derechos e intereses legítimos. Y en la ponderación que se haga en el

conflicto entre unos y otros, adquieren especial importancia estas características de la Internet de hoy en día.

Son varias las definiciones que se han dado, sin embargo la mayoría lo ponen en relación exclusivamente con el derecho a la protección de los datos de carácter personal, así, por ejemplo, la Comisión Europea lo definió en un principio, en su comunicación "A comprehensive approach on personal data protection in the European Union", como "the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes", entendido como el derecho de las personas a que sus datos dejen de ser tratados y sean eliminados cuando ya no sean necesarios para los fines legítimos para los que fueron recabados.

Otros autores lo definen como el derecho a que los buscadores no localicen tus datos personales en la red. A la vista de la Sentencia del TJUE de 13 de mayo de 2014, dictada en el caso C-131/12, y siguiendo bajo el prisma de la protección de datos personales, en todo caso, tendría que definirse como el derecho que tiene un individuo a que los gestores de motores de búsqueda en Internet cesen en el tratamiento que de sus datos personales realicen en el territorio de la Unión Europea al enlazar a y al mostrar determinado contenido relativo a su persona, debido a que, habida cuenta de las circunstancias del caso en particular, dicho tratamiento ha dejado de ser legítimo, con independencia de que el tratamiento en origen continúe siendo lícito, porque, en relación con la finalidad que justificaba el tratamiento y con el tiempo transcurrido, los datos ya no son adecuados y/o pertinentes, y ahora son excesivos.

Debe entenderse, del mismo modo que se viene haciendo con el derecho de cancelación de los datos personales, que podríamos hablar de un derecho al olvido desde el prisma del derecho al honor, la intimidad personal y familiar y la propia imagen, o en relación con la propiedad intelectual (concretamente el derecho del autor a retirar su obra del comercio por cambio de sus convicciones morales o intelectuales). En tal caso, eso que se ha dado en llamar derecho al olvido podría llegar a alegarse también de las personas jurídicas en ámbitos diferentes a los de la privacidad.

El derecho al olvido en un primer tipo de supuestos serían aquellos en los que, siendo, en el origen, cierta la información que se revela respecto a un individuo, éste debe soportar esa intromisión en su intimidad por estar legitimada en virtud del derecho de información (ya sea éste ejercido a través de los medios de comunicación, ya de boletines oficiales o tablones edictales), pero en los que, debido al transcurso del tiempo, puede decirse que tal legitimación debe caducar a fin de que el individuo no tenga que soportar dicha carga durante el resto de su vida, impidiéndole su propio pasado, en mayor o menor medida, vivir en paz un presente enmendado.

En segundo término, aquellos en los que, aun siendo incierto lo manifestado respecto a una persona y viendo ésta, así, mancillado su honor, el perjudicado prefiere no actuar contra dicho ataque porque en ese momento éste no ha transcendido lo suficiente como para no poder soportar sus efectos y, sin embargo, un tiempo después, pasados ya los plazos para ejercitar

cualquier acción, es recuperada esa falsa información alcanzando, en esta ocasión, mucha mayor repercusión gracias al estado de la tecnología.

A la hora de tomar decisiones, las personas lo hacemos en función de las circunstancias que entonces nos rodean y sopesando las consecuencias que nos cabe esperar con lo que conocemos en ese momento.

Teniendo en cuenta que hay determinadas circunstancias en que, ni acudiendo al derecho a la intimidad o, al derecho al honor o, al de protección de datos personales, podemos dar una solución a quien ahora se ve perjudicado por hechos sucedidos en su vida pasada, que ya habían sido olvidados por la colectividad que en su momento supo de ellos, que ahora son traídos al presente, incluso puede que con mayor virulencia que en su origen, sin que exista una necesidad que así lo justifique, provocando que dicha persona no pueda disfrutar en paz de la vida digna que ahora lleva.

El derecho al olvido debe garantizar el desarrollo de la persona acorde a lo que cabe esperar dentro del modo en que ésta dirige su vida en la actualidad, evitando que cualquier pasado, más o menos oscuro, pueda frustrar dicho desarrollo cuando no existe ya necesidad ni justificación alguna para que tenga que continuar soportando tal carga. En el entorno digital, por tanto, el derecho al olvido adquiriría una gran relevancia como medio de protección de la identidad digital o del libre desarrollo de la persona en dicho entorno, pero, sin duda, también transcendiendo de éste.

Debe tenerse en cuenta que el derecho a la intimidad, a la privacidad y el derecho al honor deben ser derechos erga omnes, cuya protección debe ir más allá de las fronteras de los Estados, su garantía (recogida en la mayoría de las constituciones) debe quedar salvaguarda con independencia del lugar de nacimiento o donde se encuentre el ciudadano, debe contemplarse que, de no ser así nos encontraríamos con diferentes clases de ciudadanos y derechos de diversas generaciones.

Solo mediante el compromiso de los Estados y órganos jurisdiccionales, mediante la unificación de criterios normativos y jurisprudenciales, de tipos penales, sanciones y definición del bien jurídico protegido, puede garantizarse una correcta protección de la privacidad en la red.

Por ello, con independencia de las partes intervinientes, responsable del fichero, tratamiento, buscador, las diferentes entidades se deben dotar de medios materiales y organizativos que garanticen el correcto ejercicio de derechos por los ciudadanos, la efectiva retirada de contenidos y una información clara y concisa, entendibles por todos.

La educación debe ser un factor clave en la protección de la identidad digital de las personas, quienes en primer término son responsables de su propia información, de aquella que

comparten en Internet y en las redes sociales, de sus opiniones o comentarios. Solo desde una formación en el uso de las nuevas tecnologías y en las repercusiones que tiene compartir en la red, se puede llegar a un sistema efectivo, junto con las garantías de ordenamientos comunes y mecanismos para la protección de los derechos fundamentales de las personas.

Es obligación de cada uno cuidar qué imagen se genera en Internet, en el entendido de que es por nuestra identidad digital que se gana presencia en la esfera laboral. Somos libros abiertos para las empresas, para los clientes, y nuestra información personal ahora se puede visualizar tal como se visualiza un curriculum vitae, pues ahora existen redes sociales para concretar relaciones laborales. Son los jóvenes los que más deben concienciarse sobre las consecuencias futuras de sus acciones presentes y a nosotros nos toca formarlos y concienciarlos para que así ocurra.

DECLARACIÓN DE MÉXICO D.F., HACIA LA IMPLANTACIÓN DE GARANTÍAS PARA LA PROTECCIÓN DE DATOS EN LOS TRATAMIENTOS DE BIG DATA[8]

Hoy en día, en un mundo digitalizado, la naturaleza de la información es diferente a la que disponíamos en el pasado. Es así debido a la abundancia de orígenes disponibles, cada uno con su peculiar variedad de datos. Un tipo de fuentes son las que se refieren a datos creados directamente por las personas, como pueden ser la informática tradicional corporativa, redes sociales, transacciones de comercio electrónico, formularios web, blogs, centros de atención a clientes, etc., y sus posibles indexaciones en motores de búsqueda. Otro tipo, que se prevé sea dentro de poco el segmento más grande de toda la información disponible, se refiere a los datos obtenidos por máquinas, como pueden ser sensores, micrófonos, cámaras de video, escáneres médicos, equipos industriales, GPS, dispositivos móviles, nuevas generaciones de electrodomésticos, electrónica para vestir (wearable devices), etc., que también puede ser indexado.

Todos estos tipos de datos forman parte del tejido de nuestras vidas más profundamente que nunca. La recolección, el almacenamiento, el procesamiento y el posterior análisis de datos se encuentra en una fase de expansión paradigmática, impulsada por el aumento de la capacidad de procesamiento y el creciente número de tecnologías integradas en dispositivos de todo tipo.

Además, se debe tener en cuenta que tanto en el presente como en el futuro, a los datos se les ha asignado un valor estratégico en varias industrias y mercados. Es decir, se han convertido en una clase de activos, esto es, lo equivalente al petróleo, sobre todo, por su fácil disponibilidad y procesamiento. Lo cual va a permitir llevar a cabo una nueva interpretación de los mismos de manera novedosa, dándoles un mayor valor agregado.

El valor de los datos no es solo económico sino también social, científico, político y cultural. Son innegables, inimaginables y hasta inevitables las cosas que pueden alcanzarse con el trío conformado por datos personales, tecnología y análisis. A partir de ellos puede contarse con instrumentos para tomar mejores decisiones con información amplia y detallada y predecir algunas cosas.

8. La Declaración de México D.F., hacia la implantación de garantías para la privacidad en los tratamientos de Big Data, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada el sábado 23 de agosto de 2014 por Dulcermaría Martínez Ruíz, en el transcurso de la Jornada académica de protección de datos personales en internet, dentro de la bienvenida para los alumnos de la cuarta generación de la Maestría en Derecho de las Tecnologías de la Información y Comunicación de INFOTEC, en la ciudad de México Distrito Federal. La Declaración fue elaborada por Ramón Miralles López, José Luis Colom Planas, Dulcemaría Martínez Ruíz, Laura Vivet Tañà, Héctor E. Guzmán Rodríguez, Analía Aspis, Nelson Remolina Angarita, Lorenzo Martínez Rodríguez, Horacio Gutiérrez Gutiérrez, Edgar David Oliva Terán, Adela Goberna, J. León Unger, Violeta Guerra Ramos, Aristeo García González, Patricia Reyes Olmedo, Romina Florencia Cabrera, Marta Sánchez Valdeón, Javier Villegas Flores, Maria Paulina Casares Subia, Philipe C. Bienvenue Martin del Campo, Olivia Andrea Mendoza Enríquez, Federico César Lefranc Weegan, Jorge Moreno Loza, Cynthia Téllez Gutiérrez y Joab Andrés Mora, coordinados por Francisco Ramón González-Calero Manzanares y Daniel López Carballo.

En este contexto podemos definir Big Data como los sistemas y herramientas que son capaces de tratar ingentes cantidades de datos en un tiempo muy inferior en el que lo harían los equipos tradicionales, permitiendo su almacenamiento, búsqueda, visualización, compartición, segmentación y análisis. En la misma línea está la definición dada por McKinsey Global Institute (MGI), que lo entiende como el "conjunto de datos cuyo tamaño, y demás características, van más allá de las capacidades de captura, almacenamiento, tratamiento y análisis mediante herramientas tradicionales de gestión de base de datos".

Suele argumentarse que Big Data se encuentra intrínsecamente relacionado con el Internet de las Cosas (IoT), es decir, con el diseño de una estructura de red interconectada que permite que dispositivos físicos se comuniquen entre sí con la capacidad para transmitir, compilar y analizar datos. Ordenadores de bajo consumo, teléfonos más planos, tablets con pantallas más grandes, electrodomésticos "inteligentes" como cámaras Web con sensor de movimiento, alarmas, Smart TV, aspiradoras robotizadas, o los famosos "wearables", entre otros, en forma de pulsera, que se encarga de medir parámetros de nuestro cuerpo: sudoración, ritmo cardiaco, calorías consumidas, horas de sueño efectivo, elementos que forman parte de nuestra vida cotidiana, cuyo denominador común es contar con una pila TCP/IP, que les dota de conexión a un ecosistema en el que interactúan con otros dispositivos. Debido a la naturaleza ubicua de objetos conectados en la IoT, se espera un número sin precedentes de dispositivos que se conecten a Internet, estimándose cerca de 26 mil millones de dispositivos en el Internet de las Cosas en 2020, siendo esta última una fuente de recolección de datos que crece exponencialmente y, en consecuencia, adecuada para ser procesada mediante sistemas Big Data.

Las características principales de un sistema Big Data suelen estar referidas a sus 5 "V" , es decir, su capacidad relacionada con el volumen de datos para almacenar y procesar; la velocidad de transformación de los datos en información útil en el menor tiempo posible; la variedad de datos que un sistema de Big Data procesa y la heterogeneidad de sus formatos (bases de datos, HTML, XML, texto plano, imágenes, video, audio, código fuente, etc.); la veracidad de los datos y el valor del sistema Big Data en sí mismo, esto es, su capacidad para obtener valor de todos los datos disponibles a través de un almacenamiento y procesamiento eficiente y al menor coste posible.

Según lo señalado, el análisis de los datos no estructurados no es una aplicación trivial, y tratar de analizar petabytes o conjuntos de datos más grandes puede magnificar las dificultades que entrañan la extracción, transformación, carga, almacenamiento y procesamiento de datos. El análisis basado en la transmisión de grandes cantidades de datos sociales ofrece la posibilidad de crear perfiles sociales, por lo que la puerta que se ha abierto para los nuevos tipos de tratamiento puede crear problemas legales. La creación de perfiles para la predicción de conductas, la observación y modelación del comportamiento de las personas (profiling) surgen entonces, como un alerta a la necesidad de una protección legal de los datos, su seguridad y el

respeto a la privacidad cuando estas tecnologías van ligadas a contratos de adhesión o a usos delictivos de estos datos (saber por tu consumo eléctrico cuando no estás en casa). Así, estos grandes volúmenes de datos han expresado ya problemas concretos: falta de coordinación transnacional, infraestructura y financiación inadecuada, falta de expertos en información y conocimientos relacionados y un marco jurídico fragmentado y complejo. Los análisis de Big Data y su recopilación, sin un determinado marco jurídico, esgrime el surgimiento de nuevos problemas de privacidad y autodeterminación informativa.

Trabajos previos o en preparación a nivel internacional

A nivel internacional, contamos con los siguientes estudios, recomendaciones y documentos.

1. En enero de 2014, el presidente Barack Obama, presionado por las revelaciones de Edward Snowden, se vio forzado a presentar un discurso ante el Departamento de Justicia de los Estados Unidos donde se comprometió a modificar el programa de vigilancia sobre datos telefónicos. En ese mismo discurso dispuso que un grupo de expertos confeccionara rápidamente un informe que detalle las consecuencias relevantes del Big Data y se emitieran una serie de recomendaciones.

El informe, titulado "Seizing opportunities, preserving values" (mayo de 2014), reafirma que las tecnologías de Big Data, como toda tecnología, no son per se buenas o malas, pueden ser utilizadas para el bien general de la sociedad o para producir daños. Afirma que en su faz positiva puede fortalecer la democracia, generar crecimiento económico y mejorar la calidad de vida de los ciudadanos al mejorar los servicios de salud, educación, así como la seguridad interior y nacional.

También considera que los datos generados son ahora más valiosos e invasivos. Si bien indica que el potencial positivo es enorme, también pueden darse usos perjudiciales que afecten valores básicos de justicia y equidad. Debido a que no siempre todos los agentes que acceden a grandes volúmenes de información poseen los mismos recursos para procesarlos, es esperable la aparición de nuevas asimetrías entre instituciones e individuos.

Asimismo, identifica un fuerte interés del sector privado, pues esta tecnología permite crear perfiles de consumidores con mayor facilidad y precisión, que además también pueden ser comercializados. Expresamente se resalta el problema resultante de la falta de conocimiento de los consumidores, quienes, en la mayoría de los casos no son conscientes en qué medida ellos mismos son los productos que se comercializan.

Respecto de la discriminación y su relación con los derechos ciudadanos, señala que el tratamiento de datos habilita a los gobiernos a realizar prácticas discriminatorias por medio

de la implementación de determinadas políticas públicas, sin tomar en consideración las necesidades de grupos minoritarios. Finalmente, concluye que los principales valores en peligro son los relacionados con la privacidad, por lo que es necesario preservarlos mediante la protección de toda información personal, con mejores y más actualizadas leyes de protección a los consumidores y a los ciudadanos en general, garantizando que la información recolectada sea utilizada para los fines permitidos y declarados con anterioridad.

El 23 de abril del 2014, bajo el lema "Rewards and Risks of Big Data" (Recompensas y riesgos de los grandes volúmenes de datos) se presentó la 13ª edición de The Global Information Tecnology Report, documento elaborado por el Foro Económico Mundial y el INSIDE. Dicho informe recoge las debilidades que aún subsisten en el sistema empresarial y de innovación en las Tecnologías de la Información y las Comunicaciones de 148 economías.

Entre otras cosas, en el citado informe se hace un análisis respecto a la postura que deben asumir los países frente a los volúmenes de las grandes bases de datos; así como la manera en que deben ser tratados, a fin de obtener de los mismos mayores beneficios comerciales y organizativos. Sin dejar de lado la necesidad de que se cuente con políticas adecuadas para que la Internet de Todo pueda concretar su promesa de proporcionar inmensos beneficios económicos y sociales. La importancia de este documento radica en que a través del mismo se puede medir el impacto que puede llegar a tener el Big Data en la privacidad de las personas y los beneficios que podrían representar para las empresas, incluso, para los propios gobiernos.

Y sin duda, puede ser un referente a la hora de buscar una armonización de los reglamentos sobre la protección de datos a nivel mundial.

2. En abril de 2013, el Grupo de trabajo internacional de Berlín sobre protección de datos en las Telecomunicaciones, presentó el "Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy". El documento expresa que uno de los fundamentos de la protección de datos es el derecho de los sujetos a controlar su propia información, teniendo el derecho a que se elimine la información procesada ilegalmente o la producida sin su consentimiento. En este sentido, el "derecho al olvido" se presenta como esencial, en los casos en donde hay interés legítimo avalado legalmente, asegurando que no se afecte la libertad de expresión y la libertad de prensa.

En el caso de la información existente en Internet, dada su estructura, el "derecho al olvido" sería más bien un "derecho a no ser encontrado". Actualmente no hay forma técnica de identificar y localizar todas las copias disponibles de algún archivo o información específica en Internet, lo cual no obsta que con la nueva información generada sea posible establecer mecanismos que funcionen como fechas de vencimiento, garantizando que dejen de estar disponibles pasadas determinadas fechas de forma automática. El grupo de trabajo alienta

a los actores relevantes (sector privado, académico y gobiernos) a fortalecer sus esfuerzos para progresar en este campo. Asimismo, debe tenerse presente que puede restringirse la disponibilidad de determinada información restringiendo los resultados ofrecidos por los servicios de búsqueda, y que es posible otorgar a los usuarios herramientas para eliminar su propia información personal.

3. La Cloud Security Alliance, por medio de su Grupo de Trabajo, emitió en marzo de 2014 un comentario sobre Big Data y el futuro de la privacidad, sintetizando que el interés por parte de los gobiernos en el tratamiento de información debería centrarse simultáneamente en cuestiones de acceso, propiedad, privacidad, transparencia y responsabilidad.

Señala que la protección de la privacidad se ha convertido en un objetivo difícil de alcanzar, ya que investigadores han demostrado que los individuos pueden ser re-identificados fácilmente mediante el cruce de diferentes bases de datos. Asimismo, el lugar en donde se almacenan los datos, el lugar en donde se procesan y los lugares en donde se distribuyen los resultados derivados de su análisis determinan la competencia de diferentes jurisdicciones, las cuales protegen con diferente intensidad la privacidad de los sujetos.

Remarca también que nuevas tecnologías de encriptado de datos posibilitarían un uso efectivo del Big Data resguardando al mismo tiempo la privacidad de los sujetos generadores de información, aunque estas tecnologías no deberían implementarse en forma aislada sin ser acompañada por un marco de leyes adecuadas y buenas prácticas.

4. Otros antecedentes existentes en materia de seguridad de la información pueden ser examinados a la luz de la problemática específica del Big Data. El National Institute of Standards and Technology (NIST), publicó en septiembre de 2011 el SP 800 – 137 "Information Security Continuous Monitoring for Federal Information Systems and Organizations". El documento reconoce que para garantizar la seguridad de la información se requiere de órganos específicos que identifiquen y respondan frente a las nuevas vulnerabilidades emergentes y amenazas cambiantes, en un entorno de cambio de organización e infraestructura.

El informe resalta la importancia de un control constante como parte de los procesos de administración de riesgos, para alcanzar un nivel de riesgo aceptable y es por ello que recomienda a las organizaciones públicas o privadas definir en primer lugar una estrategia de control constante sobre la seguridad de la información, establecerla en un programa de acción e implementarla para luego analizar la información resultante y las vulnerabilidades descubiertas, y responder frente a ellas para así poder, en última instancia, revisar la estrategia y el programa de acción diseñado, para actualizar y mejorar el esquema general de seguridad y aumentar la calidad de la seguridad de la información al final de cada ciclo.

5. El grupo de estudio ad hoc "Next Generation Analytics and Big Data" –integrante del comité sobre gestión de datos y normas de intercambio (SC32) del JTC1 de la Organización Internacional de Normalización (ISO/CEI) – publicó en junio de 2013 su reporte preliminar sobre la gestión de grandes cantidades de datos. El documento reconoce que la protección de la privacidad es un factor a considerar, y que no tenerlo en cuenta puede derivar en temores públicos generales sobre la existencia de un "Gran Hermano", diferentes sanciones de organismos protectores de la privacidad, y acciones judiciales, incluso colectivas.

6. El reporte "Right to Privacy in the Digital Age" (junio de 2014) fue presentado por el Alto Comisionado para los Derechos Humanos de las Naciones Unidas sobre la cuestión de la recolección masiva de datos vista desde el derecho a la privacidad.

El Alto Comisionado afirma que el derecho internacional de los derechos humanos contiene el marco frente al cual toda interferencia al derecho a la privacidad debe ser confrontada, aclarando que este no es el único derecho violado frente a prácticas de vigilancia masiva, intercepción de comunicaciones privadas y recolección de datos personales.

El reporte cuestiona el grado en que los consumidores son realmente conscientes de los datos que están compartiendo, de qué manera lo hacen, con quiénes y para qué fines, frente a las posiciones que sostienen que el transporte e intercambio de información personal a través de medios electrónicos es parte de un acuerdo consciente mediante el cual los individuos entregan voluntariamente información sobre sí mismos y sus relaciones, a cambio de acceso digital a bienes, servicios e información.

También definen como no convincente a la distinción entre datos y metadatos. Cualquier captura de datos de comunicación interfiere potencialmente con la privacidad, y la recolección y el almacenamiento de estos datos conforman una injerencia en la vida privada, sean esos datos posteriormente consultados o no. Incluso la mera posibilidad de que esa información pueda ser interceptada crea una injerencia en la vida privada por el potencial efecto negativo sobre varios derechos, incluidos los de la libertad de expresión y de asociación.

Nadie puede ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Las injerencias permitidas por leyes nacionales pueden ser ilegales si aquellas leyes están en conflicto con el derecho internacional de los derechos humanos. Los Estados deben probar que las injerencias son necesarias, proporcionales y que respetan los principios de legalidad.

El reporte reconoce que estamos presenciando la emergencia de una práctica de los Estados que consiste en externalizar las tareas de vigilancia masiva en terceros. Reconoce la existencia

de fuerte evidencia de una creciente dependencia de los gobiernos para con el sector privado, en cuanto a llevar a cabo y facilitar tareas de vigilancia digital.

Cuando una compañía suministra los datos o la información de un usuario a un Estado en respuesta a una solicitud que contravenga el derecho a la privacidad según el derecho internacional, o una empresa ofrezca tecnología de vigilancia de masas o equipos a los Estados sin salvaguardas adecuadas, o cuando la información se utiliza de alguna manera en violación de los derechos humanos, las empresas corren el riesgo de ser cómplices o verse involucrados en violaciones de los derechos humanos.

Cuando las empresas se enfrentan a demandas de gobiernos para acceso a datos que no cumplen con las normas internacionales de derechos humanos, se espera que traten de honrar los principios de los derechos humanos en la mayor medida posible y que sean capaces de demostrar sus continuos esfuerzos en ese sentido.

7. El 28 de julio de 2014 el Information Commisioner´s Office del Reino Unido ha publicado un informe titulado "Big Data and Data Protection". Para el ICO operar dentro de la ley no debería considerarse como una barrera a la innovación. El Informe expone cómo se aplica la ley cuando Big Data utiliza la información personal. Detalla qué aspectos de la ley necesitan considerar particularmente las organizaciones para poder innovar sin situarse al margen de la ley. Las organizaciones necesitan pensar en formas innovadoras para decir a los clientes lo que quieren hacer y lo que esperan lograr. El informe también aborda las inquietudes planteadas por algunos comentaristas que no encajan en la actual ley de protección de datos con Big Data. Para el ICO los principios de protección de datos básicos ya establecidos en la ley del Reino Unido y la Directiva 95/46 son lo suficientemente flexibles para cubrir Big Data. Los principios todavía son aptos para el propósito, pero las organizaciones necesitan innovar al aplicarlos. También valora positivamente las nuevas herramientas previstas en la Propuesta de Reglamento General de Protección de Datos de la UE para este tipo de tratamientos.

Big Data como servicio de TI

Big data es uno más de los servicios que ofrece el área de Tecnologías de la Información (TI) a la organización con el objetivo de poder obtener valor a partir de la información. Esa finalidad se consigue mediante el análisis de los datos, obtenidos a partir de múltiples orígenes y con diferentes formatos, mediante técnicas analíticas implementadas en sistemas informáticos especializados.

En consecuencia, Big Data debe ser administrado con el mismo rigor que el resto de servicios de la organización, integrándose bajo el paraguas de las estructuras de Gobierno y Gestión de TI.

Para comprender el alcance de esta necesaria integración, podemos aproximarnos a una definición de gobierno y gestión que clarifique los conceptos: mientras que la gestión únicamente

pretende mejorar la eficacia y la eficiencia de los servicios, y de los procesos en que éstos se sustentan, el gobierno pretende asegurar unos objetivos, partiendo de unos recursos y en base a la estrategia corporativa acordada, manteniendo el riesgo a un nivel aceptable. Y es en este último concepto de riesgo donde, desde el punto de vista de la protección de datos, debemos prestar especial atención.

El riesgo puede incidir en la privacidad como la probabilidad de que se materialicen las diferentes amenazas que representan un impacto negativo de seguridad en los datos personales, pudiendo comprometerse la confidencialidad, la integridad o la disponibilidad de los mismos. Pero también, desde un punto de vista jurídico, el riesgo puede surgir de la adopción inadecuada o insuficiente del marco normativo y regulatorio o debido a la ausencia, en determinados países, de legislación aplicable sobre protección de datos personales.

En algunas legislaciones Iberoamericanas, las acciones y los avances que permiten identificar un marco regulatorio adecuado para "hacer frente" al Big Data que involucra datos personales, para su completa comprensión y aplicación podría adoptar un axioma general: "Lo importante no es la cantidad de datos personales tratados, sino que son datos personales".

De esta forma, de la misma manera que es recomendable atender a la realidad económica y organizativa de todos aquellos sujetos que tratan datos personales y, por lo tanto, bienvenida la elaboración y difusión de textos como el "Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas", también resulta recomendable (quizás, indispensable) el análisis de Big Data como servicio de TI y sus implicaciones con la protección de datos personales y la privacidad de las personas.

La seguridad de los datos

Los tres atributos básicos de la seguridad de la información pueden llegar a verse comprometidos en los tratamientos de Big Data:

En relación a la confidencialidad, existe la posibilidad real –a partir de un análisis basado en volúmenes de datos que pudieran llegar a correlacionarse con algún dato identificativo personal– del trazado de perfiles de conducta de los afectados. Precisamente, el volumen de datos es una de las características esenciales de Big Data, junto a la aplicación de la analítica adecuada. Es en este punto donde se considera fundamental la determinación, previa a ese tipo de tratamientos, de la finalidad de los mismos. El principio de finalidad, además del de consentimiento, debería ser la estrella polar de la protección de datos referida a Big Data. Otras actitudes, como es el permitir un acceso individualizado o granular a los grandes volúmenes de datos almacenados en los sistemas de Big Data, puede representar elevado riesgo para la privacidad si los datos se almacenan sin la debida anonimización o están insuficientemente protegidos mediante controles de acceso ineficaces.

En cuanto a la integridad de la información, representada en un sentido más amplio por la calidad de los datos, debe considerarse que si el objetivo principal de Big Data es facilitar ayuda para la toma de decisiones, la falta de integridad provocará la obtención de conclusiones erróneas y, en consecuencia, decisiones también erróneas.

Y, por último, sin el atributo de disponibilidad no será posible dar en todo momento el debido cumplimiento al derecho de acceso, considerado como un mecanismo de verificación y control de los propios datos por parte del interesado, amparado por la legislación aplicable en materia de protección de datos. En él se incardinan relacionados todos los demás derechos de rectificación, cancelación y oposición.

Una peculiaridad del derecho de acceso, en entornos de Big Data, no es solo posibilitar el conocimiento de todos los datos personales, en sí mismos, de que dispone una organización relacionados con el interesado. También sería deseable un acceso transparente a los diferentes perfiles que el sistema haya podido construir del propio afectado de forma automatizada y, a ser posible, una descripción de la lógica de los algoritmos empleados para obtenerlos, conocer para qué han sido obtenidos esos perfiles y, si procede, a quién se han facilitado.

En México, como en otras legislaciones iberoamericanas, la normativa vigente cuenta con las disposiciones necesarias para obligar a los responsables que tratan datos personales en un entorno de Big Data a la adopción de las medidas de seguridad que garanticen los tres atributos anteriormente identificados.

Bajo un enfoque neutral (y por ello positivo para los objetivos perseguidos) el artículo 19 de la LFPDPPP dispone: “todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado”. Se establece, además: “los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico”.

La generalidad y neutralidad de estas disposiciones, en relación con Big Data, requerirá que cada tratamiento de datos personales sea valorado (v.g. mediante un “Privacy Impact Assesment”) para tomar en cuenta, precisamente, el riesgo existente sobre el tratamiento de los datos, las posibles consecuencias del mismo para los titulares, la sensibilidad de los datos tratados y el desarrollo tecnológico que se utiliza para tratar los datos de forma masiva, pero con objetivos definidos.
En Perú, la Ley de Protección de Datos Personales, Ley 29733, define un dato personal como toda información que identifique o pueda volver identificable a un individuo, cuyo Reglamento de la Ley, Decreto Supremo 003-2013-JUS, en su artículo 24 complementa que es toda

información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados, definición que comprendería la protección de los datos obtenidos a partir del Big Data, dado que estos datos a partir de sistemas de gestión de información pueden elaborar un perfil de un individuo.

La ley peruana regula la información que debe ser comunicada cuando el titular de un dato ejerce su derecho de acceso, sobre quién es el titular del banco de datos personales o responsable del tratamiento, la información relativa a sus datos personales debe proporcionar todas las condiciones y generalidades del tratamiento de los mismos. Además se recalca que la respuesta debe ser amplia y comprender la totalidad del registro correspondiente al titular de datos personales, aun cuando el requerimiento solo comprenda un aspecto de dichos datos.

Es decir, si existiera la aplicación de una herramienta como el de Big Data, se debe poner en conocimiento este procedimiento con toda la información correspondiente al tratamiento llevado a cabo por este tipo de análisis de datos personales, que en el caso del Big Data comprendería señalar el método y tipo de análisis de la obtención o generación del dato personal

La calidad de los datos

Hay dos formas de abordar la calidad de los datos en entornos de Big Data: Desde un punto de vista jurídico y desde otro más tecnológico. La conjunción de ambos nos garantizará el marco adecuado para confiar en la certeza de los resultados obtenidos a partir de los tratamientos y contribuir a la protección de los derechos fundamentales de los afectados.

La mayoría de normativas de protección de datos disponen que los responsables del tratamiento deberán observar, entre otros, el principio de calidad de los datos. Se cumplirá con este principio cuando los datos personales tratados sean exactos, completos, pertinentes, necesarios, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.

El responsable deberá establecer los mecanismos que considere necesarios para preservar esos atributos, evitando así que se altere la veracidad de la información. Ya hemos visto que en entornos de Big Data la calidad de los datos es algo sustancial a la vez que, debido a los grandes volúmenes de datos tratados y su variedad, se requerirán mayores esfuerzos para lograrlo.
Vemos que el principio de calidad de los datos debe contemplarse como un binomio indisociable del principio de finalidad, que limita el alcance de los tratamientos a la finalidad concreta, o compatible, para la que éstos fueron recabados y los interesados informados.
Partimos de la presunción de que en todo tratamiento de datos personales existe la expectativa razonable de privacidad, entendida como la confianza que deposita el titular de esos datos, respecto de que los datos personales que ha proporcionado serán tratados conforme a lo que

acordaron las partes. El valor de esa expectativa es lo que, amparado por la legislación aplicable en materia de protección de datos, proporciona confianza y seguridad jurídica. En consecuencia, es imprescindible en tratamientos de Big Data un análisis basado en el principio de limitación de finalidad en relación a aquello que se le informó al interesado y éste aceptó, y que los datos tratados son los irrescindibles para logar esa finalidad: derecho de información, minimización de datos y principio de consentimiento. Siempre debería informarse al interesado sobre la finalidad con que se recaban sus datos y el posible alcance de los tratamientos posteriores.

El grupo de trabajo consultivo europeo conocido como del Artículo 29 (GT29) ya se ha pronunciado mediante el análisis de diferentes posibilidades en su opinión wp203. Según esa opinión el principio de limitación de la finalidad es una piedra angular de la protección de datos.

No obstante, los datos que ya han sido recogidos pueden ser realmente útiles para otros propósitos, que no han sido previstos inicialmente. Por lo tanto, también hay valor en permitir, dentro de límites cuidadosamente equilibrados, un cierto grado de uso adicional. Así, consideran que el principio de limitación de la finalidad está diseñado para ofrecer un enfoque equilibrado: por una parte, tiene como objetivo conciliar la necesidad de la previsibilidad y la seguridad jurídica en relación con los fines del tratamiento que deben ser explícitos, legítimos y determinados y, por otra, la necesidad pragmática de proporcionar flexibilidad sin incurrir en tratamientos incompatibles con dichos fines.

El procesamiento adicional para un propósito diferente no significa necesariamente que sea incompatible, pero la compatibilidad debe evaluarse caso por caso, teniendo en cuenta todas las circunstancias, lo que no siempre será una tarea fácil y dificulta la tutela por parte de las autoridades de control al desplazarse desde el plano basado en el derecho objetivo hacia el plano de lo subjetivo en función de las circunstancias.

A nivel ilustrativo, cabe citar el artículo 7.f de la Directiva europea 95/46/CE, que establece dos únicos requisitos acumulativos para legitimar un determinado tratamiento no consentido explícitamente: la necesidad de satisfacer un interés legítimo y que no prevalezcan derechos y libertades fundamentales de los afectados.

También adquiere esencial relevancia en el principio de calidad de los datos el ejercicio de derechos y la posibilidad de revocación de los consentimientos otorgados por los afectados.

Desde un punto de vista más tecnológico, en relación a la calidad de los datos, habitualmente se hacen clasificaciones basándose en diferentes atributos de ellos: éstos deben ser íntegros en el sentido que los datos, que en Big Data deben conciliarse procedentes de múltiples orígenes y diferentes formatos, continúen siendo completos, precisos y preservados de cambios no autorizados; completos, evitando truncamientos que los desvirtúen durante el almacenamiento

y demás tratamientos y permaneciendo vinculados los conjuntos de datos complementarios entre sí; actuales, manteniendo la trazabilidad desde cuando la información fue dada de alta o modificada en el sistema de Big Data y su fecha real o estimada de prescripción; consistentes, que describe la coherencia lógica de la información; la validez de los datos, que obliga a que sean confiables en su origen y acordes a la situación actual que representan; precisos, que consiste en mantener la exactitud de los datos de entrada en los sistemas de Big Data, con independencia de los diferentes orígenes, ya sean humanos, informáticos, sensores, etc.

Como en otras tantas jurisdicciones, México ha adoptado el principio de calidad como parte de aquellos otros rectores de la protección de datos personales y que, materializado, debe garantizar que los datos tratados sean exactos, completos, pertinentes, correctos y actualizados, según se requiera para el cumplimiento de la finalidad para la cual son tratados por el responsable (Art. 36 del RLFPDPPP).

Cabe señalar que la redacción adoptada por la ley mexicana de protección de datos en relación con este principio abre la puerta a diversas interpretaciones en relación con su cumplimiento. En el entorno Big Data, la necesidad de interpretar lo dispuesto por el artículo 11 de esta Ley se anticipa como inevitable, pues no cabe duda que al disponer este numeral que "el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados", si bien es cierto se atiende a una realidad en relación con la posibilidad material de mantener datos correctos y actualizados de los interesados, también es cierto que se abren posibilidades indefinidas para flexibilizar en determinados escenarios la rigurosidad de esta obligación.

Por lo anterior, es recomendable, como para tantos otros principios, invitar al análisis, estudio y difusión de las particularidades de Big Data y su enorme vinculación con la protección de datos personales y la privacidad de las personas, procurando en todo momento que tanto la generalidad de los principios como la especialidad de los entornos en que estos deben respetarse, garantice la protección de los bienes jurídicos protegidos por la normativa y la viabilidad de las actividades económicas de los "responsables Big Data".

Lo anterior cobra mayor sentido a la luz de la reciente sentencia emitida por el Tribunal de Justicia de la Unión Europea en el Asunto C-131/12 (ya conocida como la "sentencia del derecho al olvido"), que entre otros varios aspectos se pronuncia sobre el cumplimiento del principio de calidad por parte de los gestores de motores de búsqueda en Internet, concluyendo que dichos gestores son "responsables" del tratamiento de los datos personales que efectúan estos motores de búsqueda y que, por lo tanto, están obligados al cumplimiento de las disposiciones establecidas en la Directiva europea 95/46/CE (entre otras, las relativas a la calidad de los datos que tratan en el ámbito de sus actividades e intereses económicos).

Big Data y Privacy by Design (PBD)

Una de las herramientas que se demuestran más útiles a la hora de respetar la privacidad en los tratamientos de Big Data es el Privacy by Design, que podría definirse como abordar la privacidad de forma temprana, especialmente en proyectos complejos como pueden serlo los de Big Data, representando una mayor efectividad a un coste menor. Por eso cabe considerarla desde la fase de diseño (Privacidad por diseño).

El principio de privacidad por diseño fue creado por la Comisaria de Privacidad de Ontario, Canadá, Ann Cavoukian, y puede ser aplicado a cualquier tipo de datos. Se fundamenta en 7 principios básicos:

1. Proactivo no reactivo / preventivo no correctivo: la privacidad por diseño se anticipa a los riesgos antes de que se produzcan. Se trata de adoptar medidas que impidan que estos riesgos se materialicen y, por tanto, tiene un carácter preventivo, se trata de actuar antes, no después.

2. Privacidad por defecto: cualquier sistema ha de estar configurado de forma que, por defecto otorgue una mayor protección a la privacidad de las personas, de modo que no se comparta la información del usuario salvo que éste realice una acción o cambie su configuración.

La privacidad por defecto otorga un mayor control sobre la propia información, ya que el usuario está protegido aunque no haga ninguna acción y decide libremente cuándo, cómo y con quién comparte sus datos.

3. Privacidad integrada en el diseño: la protección de la privacidad ha de estar integrada en el sistema desde el momento en que se diseña, sin que ello disminuya su plena funcionalidad.

No se trata de una opción que se añade a posteriori sino que es uno de sus componentes integrales.

4. Funcionalidad: seguridad y privacidad no han de ser características excluyentes, sino que ambas han de estar garantizadas e integradas en cualquier sistema.
5. Protección durante todo el ciclo de vida de los datos: la protección de la información se ha de configurar desde el momento en que se recaban los datos, durante todo su ciclo de vida hasta que son destruidos, garantizando también que se eliminen de forma segura y confidencial, respetando los periodos de retención establecidos.

6. Transparencia: la entidad que trate los datos ha de estar sujeta a los términos y condiciones informados desde un principio, que no podrán modificarse sin el previo consentimiento del afectado. También podrá estar sujeto a una verificación independiente.

7. Velar por los intereses del usuario como objetivo: el interés del individuo siempre ha de estar presente en el diseño y configuración de sistemas y aplicaciones, por ejemplo, mediante fuertes medidas de seguridad (encriptación, verificación en dos pasos, etc.), información completa y comprensible, opciones "user-friendly", privacidad por defecto.

Ann Cavoukian ha elaborado un nuevo principio basado en aquellas entidades que disponen de grandes y complejos sistemas informáticos que ya están creados y que, por tanto, no han aplicado desde el principio la privacidad por diseño. Se trata de "Privacy by ReDesign" (rediseño), que se basa en las 3 Rs: "Rethink, Redesign and Revive" (repensar, rediseñar y revivir):

- Rethink: consiste en que las organizaciones revisen sus estrategias de mitigación de riesgos, procesos y sistemas considerando opciones que otorguen una mayor protección a la privacidad. Revisar periodos de retención de datos, controles de acceso a los datos, etc.

- Redesign: consiste en implementar mejoras en el funcionamiento de los sistemas desde un punto de vista de respeto a la privacidad y permitiendo obtener los mismos objetivos. Por ejemplo, valorar la disminución en el tipo de datos recabados, etc.

- Reviving: revivir el sistema en base a un nuevo enfoque más protector de la privacidad.

Para cumplir con estos cometidos, podemos utilizar diferentes principios y herramientas, que pasamos a analizar a continuación y que creemos que deben presidir cualquier sistema de Privacy by Design.

Los derechos de acceso y rectificación junto con el principio de transparencia son pilares básicos que han de gobernar el Big Data y, por tanto, también se han de configurar desde el inicio. Igualmente, siempre se ha de facilitar un derecho de oposición fácil y gratuita, especialmente para la utilización de los datos con fines comerciales y de publicidad.

El principio de transparencia también exige que la información sea facilitada en un lenguaje sencillo y accesible para todos los sectores de población. Y la utilización de sistemas, como la información por capas, permiten al usuario localizar la información que necesita de forma más rápida.

Es importante que los términos y condiciones de cualquier producto y servicio sean vinculantes para la entidad que los ofrezca, obligando a recabar el consentimiento de los usuarios antes de su modificación.

Conviene tener presente el carácter internacional de muchos de los productos y servicios que se ofrecen en la sociedad de la información, y la dificultad jurídica que puede representar

determinar las leyes que resultan de aplicación a un determinado producto o servicio. Por ello, el principio de transparencia es de suma importancia, conviene que los productos o servicios que se ofrezcan a los ciudadanos de un país permitan conocer de entrada cuál es su expectativa de privacidad al utilizarlo y cuáles son sus derechos reales. Ello le permitirá, al menos, poder discriminar entre diferentes proveedores y escoger con propiedad el que más le convenga.

Con carácter previo puede ser conveniente realizar una evaluación de impacto de la protección de datos (Privacy Impact Assessment. PIA). En esta evaluación de impacto a la privacidad es necesario tener muy en cuenta las finalidades concretas del tratamiento con el fin de determinar si es posible obtener el mismo resultado mediante información anónima.

Además, la finalidad del tratamiento nos ayudará a definir periodos de retención y tipo de datos que sean estrictamente necesarios para el cumplimiento de la finalidad. De este modo, se podrán definir plazos a partir de los cuales la información puede eliminarse y cuando sea posible, se permitirá disociar la información de carácter identificativo.

Este punto es especialmente importante teniendo en cuenta el impacto energético que resulta del actual consumo de datos y de asegurar su permanente accesibilidad. Es necesario poder discriminar entre la información relevante y estrictamente necesaria para el cumplimiento de la finalidad, de la que resulta no adecuada, irrelevante u obsoleta para poder facilitar la eliminación segura de esta última.

Otro punto que será necesario tener en cuenta es el concepto de "dato de carácter personal" ya que, depende del país de que se trate, dicha definición tendrá un carácter más o menos amplio.

Será conveniente determinar qué se consideran "datos sensibles", teniendo en cuenta que con el Big Data se podrán relacionar diferentes tipos de datos que, si bien en un principio puedan ser considerados de nivel básico, valorados en su conjunto permitan crear perfiles detallados de personas, hábitos y comportamientos que merezca una mayor protección por pertenecer al ámbito íntimo de la persona.

También es importante instaurar mecanismos de control de acceso a la información, ya sean por terceros o por los responsables del tratamiento que sean estrictos, especialmente cuando se trate de datos sensibles, partiendo de la regla general que solo podrían acceder a ellos o conocerlos aquellos que previamente han obtenido el consentimiento del titular del dato personal o, que exista una normativa de alto rango, como la ley que contemple excepciones en mérito del interés público.

En relación al tratamiento de datos de menores con carácter general, se intentará adoptar medidas que impidan o restrinjan su tratamiento. Cuando sea necesario, ya sea a nivel educativo,

de salud o social se procurará que el tratamiento cumpla especiales cautelas, sirva para el cumplimiento de unas finalidades concretas y en beneficio del menor, contando siempre con el consentimiento de sus padres o tutores. Ha de procurarse que no se produzcan consecuencias negativas para el menor (evaluaciones, notas, ayudas, becas, temas de adopción, custodia, etc.) derivadas de un tratamiento automatizado de datos, siempre han de existir mecanismos que aseguren un tratamiento y evaluación individualizada, con un trato humano y personal.

En lo que respecta a la relación entre el Big Data y el Internet de las Cosas o la interconexión de datos entre máquinas (M2M), obliga a tener muy presentes la transparencia, la privacidad por diseño y por defecto.

El usuario cuando compra determinados productos de este tipo debe saber cuáles son sus reales expectativas de privacidad, ha de poder gestionar con facilidad sus preferencias y determinar qué información, para qué finalidad y con quién la quiere compartir. También ha de conocer los periodos de retención de los datos y tener garantizados sus derechos de acceso, rectificación, oposición y cancelación.

En lo que respecta a la utilización de las técnicas de análisis de sentimientos (sentiment analysis) que sirven para analizar los sentimientos de los usuarios para intentar determinar sus preferencias a la hora de comprar un producto u opinar sobre una decisión, al tener una connotación muy invasiva, solamente se deberían poder utilizar con el consentimiento inequívoco del usuario. Evidentemente, deberían de gobernar el resto de principios (transparencia, retención limitada de datos, derechos de acceso, cancelación, etc.).

Marco del gobierno de los datos

El gobierno de los datos es un "marco de organización que armoniza la estrategia, define objetivos y establece políticas para la información corporativa", el cual engloba la elaboración de un marco normativo al interior de las organizaciones enfocado en la protección y gestión de los datos personales, abarcando, por ejemplo, la definición de los procesos y políticas internas que reglamenten la gestión de los datos personales.

Una vez definido el modelo de gobierno de datos, será importante el proceso de implementación, capacitación y adaptación, ya que la implementación de dicho modelo no tendrá impacto únicamente en la definición de los procesos y políticas internas, sino que se deberá trasladar tanto a la organización, como a la propia cultura organizacional.

Es por lo anterior que se habla de generar en las organizaciones una estructura de gobierno de datos que entre otros contemple temas como la calidad, ciclo de vida de los datos, seguridad y cumplimiento legal en materia de protección de datos personales, y más aun tratándose de empresas que están en contacto, procesan o generan información mediante Big Data, ya que

por los grandes volúmenes de información que manejan, una adecuada gestión de los datos es indispensable.

En alguna de las legislaciones iberoamericanas ya se contempla el que los responsables puedan allegarse de estos modelos de gobierno de datos para el cumplimiento de las obligaciones a su cargo, ya que se establece que el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo adecuado para tales fines.

En lo que respecta a la calidad de los datos, dentro de las organizaciones y como parte de los puntos de control de las políticas y procesos que se establezcan en los modelos de gobierno de datos, se deberán contemplar los riesgos que implican factores como los registros manuales de los datos, errores humanos, flujo de información entre departamentos, errores en procesos o, incluso, en los mismos sistemas, ello incluso cuando hablemos de entornos controlados donde las cantidades de datos o el flujo de los mismos sea muy poco.

Pero si este tipo de errores los trasladamos a entornos globales de información, como lo es el uso de herramientas de Big Data que utilizan como fuente de información los datos generados o circulantes en plataformas Web y dispositivos móviles, los errores se pueden disparar exponencialmente, no solo por los errores que se pueden dar al interior de la organización sino también por lo complicado que es saber si tales datos son confiables o verídicos.

En pro de que el uso de los datos utilizados mediante Big Data sean lo más confiables posibles, existen algunos modelos que ofrecen técnicas para mejorar la calidad de los datos, como por ejemplo, el perfilamiento, estandarización, mapeo, categorización o anonimización de los datos.

Al principio, la implementación de estos modelos podría ser vista por las empresas como muy costosa, pero en realidad a la larga se convierte en una ventaja, ya que al utilizar las técnicas de Big Data se busca que los equipos de marketing o ventas puedan realizar, por ejemplo, campañas dirigidas a sus clientes de una forma más efectiva; pero si partimos del hecho de que muchos de los datos pueden ser falsos, en realidad los esfuerzos empleados no obtendrán resultados certeros.

Por el contrario, si se emplean las suficientes medidas que permitan eliminar datos inexactos, incompletos o no estandarizados, aunque la muestra sea menor el resultado será más exacto. Es decir, al final lo importante no es tener más y más datos personales sino que los mismos sean de calidad.

El velar por la calidad de los datos personales no solo es importante para lograr la satisfacción de las preferencias de los clientes, para optimizar la labor de los departamentos de ventas y de mercadotécnica o, incluso, para mejorar el procesamiento de los datos en las áreas de

tecnologías de la información, sino que también es importante para el cumplimiento de las disposiciones legales aplicables en materia de protección de datos personales.

Siendo, por ejemplo, el caso de la legislación mexicana en la materia y la Directiva 95/46/CE, que establecen como obligación para los responsables el dar cumplimiento y garantizar el principio de calidad de los datos personales, por medio del cual:

- Los datos deberán ser exactos, completos, pertinentes, correctos y actualizados.

- Si los datos personales son proporcionados por el titular, se presume que se cumple con la calidad, hasta que se manifieste o acredite lo contrario.

Estableciéndose además que el responsable adoptará los mecanismos que sean necesarios para cumplir con esos dos puntos, aún y cuando la información no se obtenga directamente del titular.

Es por ello que al ser un problema el que el Big Data no pueda garantizar que los datos sean veraces, que mejor que dentro del modelo de gobierno de datos de las empresas se empleen técnicas que nos ayuden a deputar los datos para quedarnos únicamente con los datos que cumplan con el principio de calidad.

En lo concerniente al ciclo de vida de los datos, en un modelo de gobierno de datos es elemental considerar el ciclo de vida de los datos o livecycle management, ello sobre todo para las organizaciones que procesan datos mediante plataformas de Big Data, ya que como se ha mencionado, los volúmenes de información que procesan son muy grandes.

Dentro del ciclo de vida de los datos se deben considerar tanto aspectos técnicos, como el volumen, velocidad y complejidad, así como aspectos legales que tienen que ver con la creación, almacenamiento, tratamiento, transferencia, remisión, archivado definitivo o destrucción de los datos personales, así como las finalidades del tratamiento de dichos datos.

En algunas legislaciones iberoamericanas, se establece que los plazos de conservación de los datos personales no deberán exceder de los que sean necesarios para el cumplimiento de las finalidades del tratamiento, ello tomando en cuenta la legislación aplicable en casos especiales, como los datos financieros, de salud, contables, fiscales e históricos, los cuales por sus características y particularidades suelen tener plazos de conservación especiales (normas sectoriales).

Cuestión no menos importante es la relativa a la seguridad, ya que como se analizó en el apartado de seguridad de los datos, existen diversos riesgos que pueden poner en peligro la seguridad, la confidencialidad, la integridad, la disponibilidad e incluso la privacidad de los datos; es así que la seguridad no solo debe estar contemplada en las plataformas y elementos

de las tecnologías de la información y comunicaciones, ya que agentes diversos como el descuido de una persona o por el mal acondicionamiento y seguridad de las instalaciones, también se pueden poner en riesgo los datos personales.

Es por ello que adicional a las medidas de seguridad técnicas, se deben implementar también las administrativas y las físicas, entre las que destacan: la capacitación, actualización y concienciación de las personas que intervienen en temas de seguridad y protección de datos al interior de la organización.

Esto se puede realizar mediante programas de capacitación, ya que incluso, al realizar tales capacitaciones de manera periódica se evita que por cambios o rotación de personal lo impartido quede en el olvido o que las nuevas personas no tengan los conocimientos necesarios.

El empleo de técnicas de anonimización logra que los datos personales no puedan ser asociados con su titular, es decir, después de aplicar una técnica de anonimización deberá ser irreversible el ligar un dato con su titular.

Se deberá realizar el análisis de riesgos que consiste en detectar la diferencia entre las medidas de seguridad existentes y las faltantes que resulten necesarias para la protección de los datos personales.

La importancia de este análisis de riesgos reside en que no solo se quede en la detección de los elementos ausentes, sino que se realice un plan de trabajo que permita su implementación en la organización, precisamente para subsanar las deficiencias detectadas.

Se deberá contemplar el procedimiento y las acciones a realizar; en caso de sufrir vulneraciones o brechas de seguridad, se debería tener en cuenta:

- Se entiende como vulneración a la seguridad de datos personales la pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizados.

- Cuando el responsable detecte vulneraciones de seguridad, informará al titular cuáles fueron las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales (informe sobre vulneraciones).

- El informe sobre vulneraciones se realizará en cuanto se confirme que ocurrió la vulneración y se hayan tomado las acciones para detonar la revisión exhaustiva de la magnitud de la afectación.

Esto con la finalidad de que los titulares afectados puedan tomar las medidas adecuadas para proteger sus datos e información con ellos relacionada.

El responsable deberá analizar las medidas que correspondan para que la vulneración detectada no vuelva a ocurrir.

En lo referente a la protección de los menores, los datos personales deben recibir una protección y tratamientos especiales. Es así que las empresas pueden establecer lineamientos en donde se estipule si existe o no la necesidad de recopilar datos de menores de edad, los límites o rangos de edad de los menores respecto de los cuales se recopilen datos, así como los productos y servicios a los que tendrán acceso, lo anterior ayudará a su vez a la definición de las finalidades del tratamiento de los datos.

Una vez definidos los casos en los que será procedente la recopilación de datos de menores de edad, se tomarán medidas para:

- Informar en el aviso de privacidad sobre la recopilación de los datos de los menores y sobre las finalidades de su tratamiento.

- Establecer los mecanismos mediante los cuales los padres o tutores otorgarán su consentimiento para el tratamiento de los datos personales de los menores de edad, así como para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales, ello también a través de sus padres o tutores. De otorgar el consentimiento el propio menor, al ser por ejemplo español mayor de 14 años, se deberá utilizar un lenguaje adecuado a su edad.

- Decidir si es indispensable que los datos personales de menores de edad sean tratados mediante las técnicas de Big Data y, en su caso, establecer medidas como la anonimización o depuración de los datos personales, de manera que no se causen afectaciones a los menores y se utilicen únicamente los datos que sean indispensables.

La obligación de transparencia en estos tratamientos de Big Data conlleva a que entre la información que debería contener el aviso de privacidad, se encuentre el dar a conocer las finalidades del tratamiento de los datos personales recopilados, lo que en caso de que se realice el procesamiento de información mediante las técnicas de Big Data, tal finalidad también deberá ser informada al titular.

En el Aviso de Privacidad también se debería informar respecto a las medidas de seguridad físicas, administrativas o técnicas que limiten el uso, acceso o divulgación no autorizada de los datos personales, así como en los casos en los que se realiza el procesamiento de información mediante Big Data se informará sobre de las técnicas especiales utilizadas, tales como la anonimización de los datos.

Es también importante que la información contenida en el aviso de privacidad y, sobre todo, la referente a las finalidades del tratamiento y medidas de seguridad utilizadas, sea redactada de una forma clara, sencilla y que se enfoque al tipo, grupo o sector al que van dirigidos los productos o servicios, en caso que la explicación comprenda inevitablemente algún nombre técnico también se deberá dar una breve explicación de este, elemento que podría ser probable dado las aplicaciones tecnológicas de la herramientas de Big Data.

En lo que respecta a los derechos de acceso, rectificación, cancelación y oposición (ARCO), el análisis sobre el ejercicio de los derechos se puede realizar en dos partes: respecto de los datos personales obtenidos de fuentes de Internet en las cuales cualquier persona tiene acceso, y respecto de los datos obtenidos directamente de su titular, o cuando se obtienen de manera indirecta pero que es posible localizar al titular:

- En plataformas o sistemas de Big Data alimentadas por datos personales obtenidos de fuentes de Internet accesibles al público, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, es realmente complicado y desproporcionado al ser casi imposible saber cuántos responsables de tratamiento los han utilizado.

- Respecto de los datos obtenidos directamente de su titular –o de manera indirecta pero cuando es posible localizar al titular– desde el aviso de privacidad se deberá dar a conocer al titular de los datos que los mismos serán tratados para el procesamiento de información mediante Big Data, dando oportunidad al titular para otorgar o no su consentimiento.

Una vez obtenido el consentimiento para el tratamiento de los datos mediante Big Data, se deberá establecer el procedimiento y medidas necesarias al interior de la organización para garantizar la atención de los derechos de acceso, rectificación, cancelación y oposición, ello cuando exista la posibilidad de identificar al titular, ya que respecto a datos estadísticos o datos cuya disociación se haya realizado de manera previa y plena, no hay posibilidad de identificar a sus titulares.

Para finalizar, indicaremos que en base al principio de accountability, al igual que el resto de las empresas, personas u organizaciones que recopilan, tiene acceso o tratan datos personales, quienes recopilen o procesen información mediante Big Data están obligados al cumplimiento con las obligaciones que conforme a la legislación les sean aplicables, debiendo justificar su actuación conforme a la legalidad vigente y respondiendo en caso de incumplimiento.

Big Data y Cloud Computing

Cuando las empresas no pueden costearse la infraestructura física necesaria para analizar grandes volúmenes de datos desestructurados, recurren al sistema conocido como Cloud Computing.

Muchos proveedores de almacenamiento de datos se erigen en Cloud Services Provider (CSP) directamente o mediante acuerdos y ofrecen soluciones basadas en Cloud Computing como parte de su actividad de negocio (catálogo de servicios además del catálogo de productos) y las comercializan entre los clientes como soluciones más asequibles y accesibles.

En esencia, las empresas cliente alquilan espacio de almacenamiento y potencia de proceso en servidores virtuales, a los que pueden acceder en línea. Estos servidores están equipados con sofisticadas aplicaciones que han sido diseñadas especialmente para manejar y analizar grandes volúmenes de datos.

La ventaja para los clientes es que pueden conseguir resultados rápidamente a un coste razonable. Además pueden acceder al asesoramiento y soporte del proveedor como apoyo al diseño y a la ejecución de los proyectos.

Desde el punto de vista de la protección de la privacidad, lo primero que tenemos que tener en cuenta a la hora de contratar una herramienta de estas características es que se va a producir un acceso a datos y, por ello, se deben reflejar en el contrato que nos ofrece el proveedor las estipulaciones sobre el acceso a datos reguladas en las diferentes legislaciones nacionales que se han tomado en serio esta materia.

Es por ello que antes de contratarla se nos debe facilitar información transparente que posteriormente debe quedar plasmada en el contrato sobre los usos, finalidades y alcance del acceso a datos, la implantación de medidas de seguridad, la devolución o destrucción de los datos cuando finalice el servicio, las subcontratas previstas y, en el caso de no conocerse en ese momento, la manera de solicitar autorización previa al responsable del tratamiento.

Otro aspecto vital del Cloud Computing es la ubicación del servidor (o alguna de sus copias de seguridad), puesto que según en qué lugar del mundo esté ubicado nuestro servidor virtual en el Cloud Computing, cuando introduzcamos datos personales en él, podrá considerarse una simple cesión (que puede resolverse mediante la suscripción del preceptivo contrato entre responsable y encargado del tratamiento) o bien, una Transferencia Internacional de Datos (TID), que conlleva obligaciones legales adicionales en los países que cuentan con legislación en protección de datos.

El tercer aspecto a considerar en los servicios de Cloud Computing es la necesidad de garantizar la disponibilidad, la integridad y la seguridad de la información. Adquieren especial relevancia en este tipo de tratamientos, aunque por el nivel de seguridad no se esté obligado a implantarlas, la posibilidad de permitirnos la realización de backups o copias de seguridad externas a la aplicación, la posibilidad de configurar perfiles de usuarios que delimiten los recursos a los que se puede acceder y con qué privilegios de acceso, la gestión de una política de renovación periódica de contraseñas y que estas sean robustas (incluyendo mayúsculas,

minúsculas, números y símbolos especiales), la aplicación de mecanismos de cifrado, sobre todo, si estas herramientas utilizan la funcionalidad del Cloud Computing o si se realizan continuas importaciones o exportaciones de datos, la de poseer un registro de incidencias en la que se puedan consignar aquellas que afectan a la seguridad o a la integridad de los datos y la de tener activado el registro de accesos al sistema con revisión periódica del mismo.

También son más que recomendables para estos tratamientos masivos de datos la limitación y registro de las importaciones y exportaciones de datos desde o hacia la herramienta al personal debidamente autorizado y la monitorización de esas actividades, ya que en caso contrario sería recomendable la eliminación o capado de sitios Web de correo electrónico o Cloud Computing, de grabadoras de CD-DVD o puertos USB y la instalación de herramientas de monitorización de equipos y correos electrónicos a los usuarios de estas herramientas.

En el Dictamen 05/2012, de 1 de julio de 2012 sobre la computación en nube, el Grupo de Trabajo del artículo 29 (GT29) analiza todas las cuestiones pertinentes en materia de Proveedores de Servicios de Cloud Computing (CSP) que operan en el Espacio Económico Europeo (EEE) y sus clientes, especificando todos los principios aplicables de la Directiva europea sobre protección de datos (95/46/CE) y de la Directiva sobre privacidad 2002/58/CE (modificada por la Directiva 2009/136/CE), según proceda.

El GT29 advierte que, a pesar de las claras ventajas de la computación en nube, tanto en términos económicos como sociales, el despliegue a gran escala de los servicios de computación en nube puede provocar diversos riesgos para la protección de datos, principalmente la falta de control sobre los datos personales, así como la insuficiente información en relación a cómo, dónde y por quién son los datos tratados o subtratados.

Los organismos públicos y las empresas privadas deben evaluar estos riesgos cuidadosamente al contratar los servicios de un CSP.

- En el dictamen examina cuestiones relacionadas con:
- La puesta en común de recursos con otras partes.
- La falta de transparencia de una cadena de externalización compuesta por múltiples encargados del tratamiento y subcontratistas.
- La inexistencia de un marco común general de portabilidad de datos.
- La incertidumbre con respecto a la admisibilidad de la transferencia de datos personales a los proveedores establecidos fuera del EEE.

Del mismo modo se aborda en el dictamen, como cuestión preocupante, la falta de transparencia en cuanto a la información que un responsable del tratamiento puede proporcionar a los interesados sobre la manera en que se tratan sus datos personales. Los interesados deben ser informados de quién trata sus datos y para qué fines, a fin de poder ejercer los derechos que tienen a este respecto.

Una de las principales conclusiones es que las empresas y las Administraciones públicas que deseen utilizar la computación en nube deben efectuar, como un primer paso, un análisis de riesgos completo y riguroso.

Los proveedores en el EEE deben proporcionar al cliente toda la información necesaria para evaluar adecuadamente los pros y los contras de la adopción de tal servicio.
Los principales impulsores de la oferta de servicios de computación en nube para los clientes deberán ser:

- La seguridad
- La transparencia
- La seguridad jurídica

Por lo que respecta a las recomendaciones contenidas en el dictamen, se subrayan las responsabilidades de un cliente de servicios de computación en nube como responsable del tratamiento, y se recomienda, por tanto, que el cliente seleccione un proveedor de servicios de computación en nube que garantice el cumplimiento de la legislación de la UE sobre protección de datos.

El dictamen aborda las salvaguardias contractuales apropiadas estableciendo la condición de que todo contrato entre el cliente y el proveedor deberá ofrecer garantías suficientes en términos de medidas técnicas y organizativas. También es importante la recomendación de que el cliente de servicios de computación en nube deberá verificar si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos.

Otros aspectos a considerar

Las incertidumbres sobre los potenciales impactos negativos que pueda generar el tratamiento masivo de información aconsejan adoptar posturas garantistas, especialmente en relación al derecho a la protección de los datos de carácter personal, la privacidad o la intimidad, pero también respecto de la salvaguarda de otros derechos y libertades, tanto individuales como colectivos, que pudieran verse afectados por el conjunto de actividades que se ocultan bajo el concepto Big Data.

Todo y que el punto de partida sea de una cierta desconfianza y recelo, a priori generada por los propios agentes relacionados con el Big Data en base a la opacidad con la que llevan a cabo sus actividades, sin duda pueden encontrarse puntos de encuentro entre:

- Las necesidades, ya sean públicas o privadas, del tratamiento masivo de la información;

- las condiciones y límites que necesariamente deben imponerse a ese tipo de tratamientos y a los usos posteriores.

A título de ejemplo, como comentamos anteriormente, el estudio "Big Data: aprovechar las oportunidades, preservando los valores", publicado el 1 de mayo de 2014 por la Casa Blanca, elaborado a petición del presidente Obama, que encargó a sus asesores que elaboraran un informe que dictaminara sobre la manera en que el Big Data podía afectar la vida de las personas, ponen de relieve la preocupación que el Big Data suscita en los poderes públicos; estos deben tomar partido y adoptar políticas adecuadas para minimizar los riesgos que puedan derivarse del tratamiento masivo de información.

No hay duda de los potenciales beneficios que para la sociedad en su conjunto pueden derivarse del Big Data, entre ellos, su aportación al crecimiento y desarrollo económico, pero hay que estar alertas respecto de los nuevos retos y riesgos que el Big Data puede suponer, tanto para la privacidad como para otros derechos y libertades individuales y colectivas.

En ese sentido, las políticas públicas y las tecnologías juegan un papel importante en la protección de los derechos y libertades que puedan verse afectados por el tratamiento masivo de información y, especialmente, respecto del uso que se pueda hacer del resultado del procesamiento de esa información.

Las actividades relacionadas con el Big Data no siempre implican el tratamiento de datos de carácter personal, por tanto, no siempre se va a dar la componente de impacto sobre la autodeterminación informativa, ahora bien, no debemos perder de vista que la información relacionada con las personas, una vez tratada, es la que puede llegar a aportar más valor a los procesos de negocio, a la investigación científica o a las necesidades de inteligencia de los Estados, en tanto garantes de la seguridad pública o para la definición y aplicación de políticas públicas.

Los datos personales pueden estar presentes de dos maneras, una de tipo indirecto, cuando en origen los datos eran de carácter personal, y han sido sometidos a tratamientos de disociación –aparentemente dejan de ser datos personales, pero existe el riesgo de re-identificación–, y por tanto, a priori, los resultados de su tratamiento no aplican a personas concretas identificadas o identificables; o bien, de manera directa, cuando el tratamiento Big Data se lleva a cabo directamente sobre datos personales.

Por tanto, podemos afirmar que, si bien hay situaciones en que Big Data y privacidad van en paralelo, no es menos cierto que pueden existir abundantes casuísticas en que se crucen, y aparezcan puntos de contacto o fricción que hay que gestionar convenientemente.

Desde el punto de vista del uso social de la tecnología, en un primer momento esta suele provocar en las personas un estado de cierta "fascinación", de ahí su rápida adopción, que suele al poco tiempo llevar a una fase de "deslumbramiento", en el que se producen efectos hasta cierto punto contradictorios: por un lado, lo último siempre es lo mejor, de manera que las tecnologías emergentes son rápidamente adoptadas, pero a la vez se impone el "discurso tecnológico dominante", que gana adeptos de manera continuada, solo por el hecho de ser dominante, sin que como individuos entremos en otras consideraciones o reflexiones respecto de la utilidad o conveniencia de su uso.

Del "deslumbramiento" se pasa a la siguiente etapa de la más absoluta "ceguera digital", y es en ese estado en el que emergen los riesgos. ¿Aceptamos una sociedad con un conocimiento filtrado y mediatizado? En definitiva, sociedades controladas. ¿Estamos dispuestos a que ciertas tecnologías limiten el libre desarrollo de la personalidad? ¿Solo vamos a atender los riesgos individuales, dejando de lado los riesgos colectivos derivados del Big Data?

El uso de Big Data para llevar a cabo predicciones es más que conocido, pero tal vez el futuro nos depara otros usos, por ejemplo, el de la inducción o modificación de comportamientos; o acabemos en un escenario donde impere el determinismo del dato, en el que solo el "análisis mecánico" de los datos vaya a mover las decisiones, llevándonos a un "estado totalitario del dato", en el que decisiones transcendentales que afecten a las personas de manera colectiva o individual se vayan a tomar exclusivamente en base al análisis de datos, lo que puede llevar a la aparición de nuevos modos de discriminación en base a esos análisis de información masivos.

Tal vez como rechazo a esos riesgos empecemos a hablar en un futuro no muy lejano de "la objeción de conciencia digital", es decir, tener la capacidad de oponernos a que nuestros datos sean utilizados, incluso aunque sea de manera anonimizada, pero eso sí, sin renunciar a los beneficios de las tecnologías.

Conviene plantearse la necesidad de regular esas actividades, y ante el escenario descrito pueden adoptarse diferentes posturas desde la perspectiva regulatoria:

- Optar por la postura de que en tanto exista tratamiento de datos personales se aplica la regulación vigente, y cuando no hay dato personal se deja de aplicar, con lo cual nos encontramos en una situación de desregulación del Big Data, con la inseguridad jurídica que ello puede generar para todas las partes, de hecho, este es el estado actual de la cuestión.

- O si bien hay que ampliar el alcance de la regulación de los datos personales a situaciones en que ya no hay datos personales, lo que supondría una excepción más que relevante por lo que respecta al ámbito de aplicación material de la regulación del derecho a la protección de los datos de carácter personal

- Si tal vez debe de ser una actividad regulada de manera específica, a la que apliquen unos límites, garantías y condiciones propios, en virtud de los riesgos colectivos que puede implicar.

Lo "peligroso" no es el Big Data en sí mismo, si no dejarlo exclusivamente en manos del mercado y sin ninguna regulación. Una regulación que debería desarrollarse en base a unos principios claros, tales como:

- El "principio de inocuidad", por el que los usos del Big Data bajo ninguna circunstancia deben perjudicar ni a los individuos, ni a "la humanidad" y que, en todo caso, las excepciones a este principio deben ser establecidas por los legisladores desde una perspectiva restrictiva y garantista.

- El "principio de objeción", por el que las personas puedan oponerse, de manera previa o a posteriori, a que su datos sean tratados, incluso de forma anonimizada, y sin que ello les impida usar las tecnologías.

- El "principio de seguridad", las actividades de Big Data deben estar especialmente protegidas, a fin de evitar incidentes accidentales o malintencionados que pongan en riesgo a la información.

- El "principio de respeto al libre desarrollo de la personalidad", deben prohibirse usos del Big Data que impliquen la modificación de comportamientos y el determinismo del dato.

- El "principio de responsabilidad", por el que en todo momento debe poder atribuirse una determinada actividad de Big Data a una persona física o jurídica y, en su caso, exigirle responsabilidades.

- El "principio de transparencia", por el que deben articularse mecanismos que permitan que las personas afectadas sean conocedoras del uso que se hace de sus datos.

Especialidades de Big Data
OPEN DATA, SMART CITIES Y ADMINISTRACIONES PÚBLICAS

Si Big Data se define por su tamaño y el Open Data por su utilidad, Open data es el concepto utilizado para los datos abiertos y accesibles al público, compañías y organizaciones que los pueden utilizar para lanzar nuevos productos o servicios, analizar patrones, tomar decisiones, etc. La estrategia Open Data nació el año 2009 en Washington y se refiere a la posibilidad de que el ciudadano acceda a los datos del gobierno, que antes solo eran analizados en el interior de las Administraciones públicas. Actualmente, el concepto se ha extendido a los países europeos a través de la Agenda Digital Europea y también a algunos países de Iberoamérica, como Argentina, Chile, Colombia y Perú.

En el modelo Open Data, los datos deben ser accesibles a cualquier persona y se han de facilitar de modo que permitan su utilización con fines comerciales o no comerciales. Estos datos han de ser accesibles de forma gratuita o a un coste mínimo. Y esto es así porque entienden que en nuestra sociedad de redes y bajo el gobierno de la información, el derecho a acceder a la información pública se erige como un derecho humano fundamental, en virtud del cual las personas pueden tomar conocimiento de la información que elaboran o poseen los órganos del Estado. Se basa esto, y lo reafirma a la vez, en el aporte relevante que puede generar esta información al conocimiento, expresión, reflexión y debate público de las ideas.

De ahí que, la información que se publique no debe ser definitiva, en virtud de que puede contener diversos estudios, informes, etc., que han servido como base para la prestación de un servicio por parte de la entidad pública. De esta forma, la imagen de la Administración pública de cara a la sociedad será percibida de manera distinta y no como un ente cerrado y opaco.
Open Data no solo se ha de referir a los datos de los gobiernos, también podría abrirse por parte de empresas de transporte, bibliotecas, universidades, museos, arte y cultura, consumo energético, geología, astronomía, temas de educación, etc., y se han de facilitar en un formato electrónico normalizado.

El uso avanzado de información de la Administración se ha de construir sobre una base que permita, no solo mejorar la transparencia, eficiencia y eficacia de las Administraciones públicas, sino también, garantizar los derechos y garantías jurídicas de los ciudadanos. Producto de la ejecución de una política pública previamente diseñada, las legislaciones deben contener disposiciones para garantizar, fortalecer e incentivar la transparencia y publicidad de la información pública que permitan erradicar las asimetrías de información entre el Estado y los ciudadanos existentes bajo la cultura de la opacidad.

Por este motivo, es importante revisar y adaptar la normativa jurídica vigente, teniendo en cuenta las características específicas de cada materia o archivo (datos históricos, datos de salud, antecedentes penales, etc.) y redefinir las relaciones con los ciudadanos y empresas y sus derechos.

Hay que tener en cuenta que, aunque la información relativa a una persona identificada o identificable esté a disposición del público, debe seguir estando protegida por la legislación sobre protección de datos, garantizando los derechos, libertades y dignidad de las personas interesadas.

A la hora de determinar en cada caso si la información se facilita, la entidad pública deberá:

- No incluir datos personales, por ejemplo, facilitando datos estadísticos, lo cual excluiría limitaciones referentes a la normativa de protección de datos, como la necesidad de consentimiento, finalidad determinada, proporcionalidad, etc.

- Anonimizar, en este caso, se deberá garantizar que se han empleado las técnicas y evaluaciones necesarias para evitar que estos datos puedan ser reidentificados. Se deberá evaluar y realizar pruebas sobre el riesgo de reidentificación. Si el resultado de estas valoraciones no es positivo, la autoridad competente debería establecer limitaciones, de acuerdo con el apartado siguiente o bloquear su publicación.

- En el supuesto de incluir datos personales, las garantías de protección de datos e intimidad de las personas resultan plenamente aplicables y por tanto se requerirá:

  - O que la publicación de estos datos sea compatible con las finalidades determinadas en el momento de su recogida (evitar finalidades incompatibles, por ejemplo, mensajes comerciales no solicitados, etc.).

  - O deberá existir una base jurídica sólida para la publicación (basada en el consentimiento del afectado o en el complimiento de una ley claramente definida con un objetivo legítimo).

  - O la divulgación de estos datos ha de ser siempre necesaria y proporcionada al objetivo legítimo perseguido por la normativa.

  - O establecer condiciones específicas y salvaguardas para su utilización.

La Administración deberá aplicar un criterio de prudencia antes de decidir cómo publicará la información ya que, una vez los datos se han puesto a disposición del público y son accesibles a través de Internet, es muy difícil limitar su uso y garantizar el cumplimiento de las normas sobre protección de datos.

También convendrá revisar las normativas sectoriales y específicas, con el fin de evitar resultados incompatibilidades o contradicciones. Por ejemplo, que al relacionar datos publicados por la Administración con otros datos accesibles a través de Internet, pueda resultar en finalidades incompatibles.

La limitación de la finalidad ha de estar siempre presente en el modelo de Open Data, para garantizar un tratamiento compatible con la recogida inicial.

Para la evaluación del tratamiento ulterior de los datos se tendrá en consideración:

- La relación entre los fines para los que se recogieron los datos personales inicialmente y los fines de su tratamiento ulterior.
- El contexto en el que se recogieron estos datos y expectativas razonables de los interesados de su posterior uso.

- Naturaleza de los datos personales e impacto del tratamiento ulterior en los interesados.

- Medidas de salvaguardia para garantizar un tratamiento leal y evitar repercusiones indebidas al interesado.
-

Deberá aplicarse un principio de proporcionalidad y de minimización de datos, solo publicar los datos estrictamente necesarios para cumplir con una finalidad concreta y determinada.

También se deberá de tener en cuenta cómo se accede a estos datos y garantizar que los datos personales de los afectados queden protegidos, incluso si se trasladan a otros Estados o países. Para ello deberán establecerse garantías adecuadas.

En lo que respecta a la conveniencia de realizar de manera previa una evaluación e impacto de la protección de datos, antes de que la Administración pública decida abrir determinados archivos o información al público en base al concepto de Open Data podría entenderse como una buena práctica, ya que serviría para:

- Evaluar los riesgos derivados de la apertura de esta información e impacto en la intimidad de los afectados, especialmente teniendo en cuenta que la información, incluso si se publica de forma anónima, puede llegar a identificar a una persona si se relaciona con otra información pública o disponible en Internet.

- Aplicar los principios de privacidad por diseño y por defecto.

- Determinar en qué condiciones y garantías se puede permitir su utilización. Valorar el establecimiento de una licencia de uso que determine limitaciones en la utilización, así como responsabilidades y sanciones en caso de incumplimiento.
- Fijar una base jurídica para su divulgación que establezca finalidades determinadas y actuaciones prohibidas.

- Aplicar los principios básicos de protección de datos: limitación de la finalidad, proporcionalidad, calidad, minimización de datos.
- Escuchar a todas las partes interesadas y tenerlas en consideración, para poder equilibrar los riesgos en juego, antes de decidir la publicación de estos datos (autoridad pública titular de los datos, entidades privadas que interesa acceder a dichos datos y representantes del colectivo de personas afectadas).

- Contar con el soporte y consejo de las autoridades de protección de datos.

También es importante que se fomente la cooperación entre diferentes organizaciones públicas con el fin de que se compartan buenas prácticas y códigos de conducta relativos a la apertura de datos entre las diferentes entidades públicas, a nivel estatal, provincial o local.

En lo que respecta al uso de tecnologías de Big Data por parte de las Administraciones públicas, al poderse procesar no solo información obrante en varias Administraciones públicas, otras empresas o terceros sino también, información disponible en Internet (por ejemplo, redes sociales, blogs, foros, webs), estos tratamientos pueden tener una especial relevancia en las actuaciones inspectoras de la Administración, actuaciones policiales, en el control de subvenciones, prestaciones por bajas médicas, subsidios de desempleo, etc.

En un contexto internacional, países como Estados Unidos han declarado la utilización del Big Data en la Administración pública como una prioridad gubernamental, particularmente por la reducción de costo y tiempo que implica el procesamiento de la información. Esto, a través de diversas iniciativas: DoD USA (2011), D2D Data to Decission y la Iniciativa Big Data de la Casa Blanca (2012).

La Comisión Económica de las Naciones Unidas para Europa (UNECE) también ha incluido el aprovechamiento estadístico de los Big Data entre sus temas de interés estratégico para este año.

Actualmente, algunas instituciones y Administraciones iberoamericanas han declarado que utilizarán los beneficios del Big Data para la obtención de indicadores que permitirán tomar decisiones de política pública, y es justo en este punto en donde se centra el desarrollo de la presente opinión.

El Big Data utilizado por las Administraciones públicas será suministrado de información particularmente sensible: datos de todos los ciudadanos, que concentrado en una sola plataforma de información resulta peligroso, particularmente, en relación a la privacidad y la protección de datos personales de los ciudadanos.

Por todo ello, el uso del Big Data en el ámbito de la Administración ha de configurarse sobre un principio de transparencia más elevado, pues mucha información que se obtenga podrá provenir de terceros o sin el conocimiento del afectado.

En el tratamiento de esta información es importante tener presentes los derechos básicos del ciudadano en materia de protección de datos basados en el consentimiento para el tratamiento de datos, el principio de finalidad y en los derechos de acceso, rectificación, cancelación u oposición. Y todo ello, sin olvidar un derecho de indemnización a favor del afectado en caso de que la actuación de la Administración haya vulnerado dichos principios, y con ello haya causado daños y perjuicios que deban ser reparados.

El derecho de los ciudadanos a resarcirse de los daños y perjuicios causados por un defectuoso tratamiento o vulneración de los procedimientos y garantías básicas por parte de la Administración puede ayudar a conseguir un mejor equilibrio y funcionamiento del sistema, en el sentido de que la Administración no se verá tentada a tratar información de forma indiscriminada y a basar sus decisiones estrictamente en un tratamiento automatizado. No obstante, para su efectividad es necesario que el acceso de los ciudadanos a este resarcimiento no se vea desnaturalizado por procedimientos demasiado burocráticos y costosos.

Si la Administración pública desea adoptar decisiones basadas en información que no ha sido facilitada por el propio usuario, hay que preguntarse dónde se sitúan los límites, ya que esta información podría traer graves consecuencias contra el usuario (por ejemplo, inicio de una actuación inspectora) y estas consecuencias podrían tener su origen en información falsa, incorrecta u obsoleta.

En este sentido, se podría valorar un sistema que estableciera una serie de garantías, tales como:

- Limitación en las finalidades, esta información solamente se puede utilizar por determinados sujetos y para finalidades concretas “numerus clausus”.

- En relación a datos de salud (o datos sensibles en general) exigir la adopción de medidas más estrictas, consentimiento reforzado y relevancia para su tratamiento.

- Calidad en los datos (completos, actualizados y exactos), no se pueden recabar datos de forma indiscriminada, sino los que son relevantes para la concreta finalidad que han de cumplir.

- Un importante derecho de acceso y rectificación, incluyendo un procedimiento para permitir al usuario poner en duda la información de que dispone la entidad cuando no es correcta, y permitir rectificarla. Todo ello, con carácter previo a que se pueda utilizar esta información para evaluar al sujeto. Igualmente, el afectado ha de disponer de un derecho de acceso a obtener esta información siempre que lo interese, de forma fácil y accesible. Este derecho de acceso debería permitir conocer el origen de la información para facilitar un mejor control sobre los propios datos. En el caso de las Administraciones públicas, el derecho de acceso debería facilitarse de forma gratuita.

- Igualmente, las Administraciones deberían hacer accesibles los criterios en base a los cuales adoptan decisiones basadas en esta información.

- Transparencia y "accountability": la actuación de las Administraciones públicas deberá estar gobernada por un principio de transparencia y sujetas a una obligación de responsabilidad de sus actuaciones y debiendo rendir cuentas frente a los ciudadanos.

El respeto a los derechos de privacidad e intimidad de las personas, a la libertad de expresión y el derecho a la legítima defensa no deben verse mermados por la utilización del Big Data en la Administración pública, puesto que su finalidad es servir a sus ciudadanos, regular y mejorar el buen funcionamiento de la sociedad, no convertirse en un estado policial o en un Big Brother.

En lo que respecta al uso del Big Data y su contribución al desarrollo de "Smart Cities" (ciudades inteligentes), basadas en un modelo de sostenibilidad y eficiencia, respondiendo a las necesidades básicas de sus habitantes, instituciones y empresas:

- Contribuye a una gestión más eficiente y sostenible de los recursos naturales, creando patrones de consumo que permitan mejorar la planificación y utilización de las energías alternativas, promoviendo la sostenibilidad y el ahorro. Por ejemplo, con una gestión eficiente del alumbrado público, solo en las horas que no hay luz natural.

- Fomenta la participación ciudadana para conocer sus necesidades y mejorar los servicios. También para permitir valorar los servicios o denunciar situaciones de forma fácil y ágil, a través de Internet o mediante aplicaciones móviles y de este modo, poder obtener una solución más rápida y eficaz a través de la denominada Administración electrónica.

- Contribuye en una planificación más eficaz del transporte público a partir de múltiples sensores ubicados estratégicamente y de dispositivos móviles de los ciudadanos, para, por ejemplo, mejorar la gestión de aparcamientos, evitar retenciones o mejorar la circulación.

- las redes de telecomunicaciones garantizando su continuidad y calidad.

- Utiliza sensores en los trenes para detectar actividad sísmica y, en caso de advertir una actividad inusual, enviar un mensaje para desactivar los trenes. Este sistema ya se está utilizando en los trenes de alta velocidad de Japón.

- Mejora la calidad de vida y medio ambiente mediante sensores de polución (mejora la calidad del aire con reducción de emisiones de CO2, del agua, ruido, residuos, espacios públicos, etc.).

- Mejora la eficiencia energética en edificios públicos y privados (organizaciones públicas, universidades, escuelas, etc.).

- Optimiza los recursos destinados a la salud pública: Muchos mejora y optimiza seguimientos de pacientes podrían realizarse sin que éste acudiera físicamente al centro médico, ayudando de este modo a descongestionar las consultas.

- Gestiona de manera eficiente los residuos y reduce emisiones, contaminantes, etc.

- Desarrolla redes inteligentes (smart grid) que permiten el control del consumo energético, lectura de datos en tiempo real (mediante "smart meters" o medidores inteligentes), facturación automática y fácil acceso a los ciudadanos de aquella información que pueda servir para el ahorro, eficiencia y mejora (facilitando el acceso al ciudadano sobre los datos de su consumo energético, permitiendo que los pueda gestionar, visualizar por Internet, ver estadísticas sobre su consumo y solicitar cambios de consumos y tarifas; reduciendo el tiempo de solución de averías y reclamaciones).

La información, tal como se ha indicado, no solamente ha de ser accesible y gestionada por las Administraciones públicas sino que es importante mejorar y fortalecer el concepto de "open government" ya que, de otro modo, se produciría un desequilibrio, pues muchos de estos datos provienen justamente de los mismos ciudadanos. Por ello, el uso de estos dispositivos debe adecuarse a las medidas garantistas mencionadas con anterioridad.

BIG DATA Y SANIDAD

El aprovechamiento de los grandes volúmenes de información que se recaban en las instituciones de salud como resultado de la consulta, tratamiento y hospitalización de pacientes para la atención de enfermedades y padecimientos, bajo un esquema de análisis y disociación adecuado, constituye un material que permite asegurar la mejora constante de los servicios de salud.

La incorporación de una estrategia de Big Data para administrar los grandes volúmenes de datos estructurados y no estructurados, combinado con la posibilidad de aplicar algoritmos que permitan correlacionar datos provenientes de diferentes fuentes para apoyar la investigación y desarrollo de respuestas que favorezcan un mayor acceso a los servicios de salud, es una de las alternativas que las tecnologías de la información ofrecen para fortalecer la investigación científica en materia de salud.

Los avances en la investigación científica relacionada con la salud y bienestar humano ofrecen la posibilidad de contar con nuevos esquemas de tratamiento para atender enfermedades

y mitigar sus efectos, esta innovación se fundamenta en gran medida por la capacidad tecnológica disponible para comprender la biología de la enfermedad, que además permita el desarrollo de nuevos medicamentos, diagnósticos y servicios preventivos de sanidad.

Esta visión contrasta con los métodos tradicionales utilizados por las compañías farmacéuticas, que pueden implicar plazos de hasta 10 años para desarrollar e introducir un nuevo producto al mercado.

El esquema considerado para disminuir el proceso de desarrollo e introducción de productos incluye compartir esfuerzos mediante esquemas de alianzas con otras empresas farmacéuticas o con las instituciones de salud administradas por los Estados, para la consolidación de un sistema de sanidad más eficiente que permita trasladar los resultados de la investigación científica en aplicaciones de salud, resultado de compartir recursos y conocimientos entre los participantes.

En este contexto, se identifica que un recurso valioso para apoyar la investigación científica está referido a la posibilidad de aprovechar la información que se recaba de los pacientes atendidos en el sector salud como parte de una estrategia para obtener conocimiento útil en la detección de enfermedades y su curación.

Las características de la información de salud existentes en los sistemas de información y las condiciones en que se busca su aprovechamiento posicionan a Big Data como una estrategia tecnológica adecuada para los fines de investigación científica, pues satisface las condiciones de las cinco V:

- Volumen. Sin duda los datos de salud son un buen ejemplo de cantidad incremental de información, tanto estructurada como no estructurada, y que además se produce por la intervención humana y por el uso de diferentes dispositivos que la recolectan.

- Velocidad. Como se ha expuesto, el aprovechamiento de la información contenida en los sistemas de salud es una alternativa para disminuir el tiempo dedicado a la investigación y desarrollo de nuevos productos que mitiguen o alivien las enfermedades.
- Variedad. La información de salud tiene además la particularidad de recabarse en diferentes procesos y formatos.

- Verificación. Por el impacto potencial que representa a la salud general esta cualidad es crítica en su aplicación para fines científicos de sanidad.

- Valor. El resultado esperado de la aplicación de una estrategia de Big Data es la contribución general al bienestar poblacional en materia de salud.

Si bien las consideraciones anteriores abonan en favor de la aplicación del Big Data, no debe omitirse que la titularidad de los datos contenidos en los sistemas de información de salud

pertenece a los pacientes y está sujeta a los principios reconocidos para su tratamiento, incluyendo la condición de excepción de su aprovechamiento por el Estado, aduciendo situaciones de salud general y el tratamiento para fines científicos, considerando la aplicación de un proceso de disociación.

Esta necesidad de aprovechar la información en posesión de los Estados para fines científicos de salud puede confluir en conflicto de interés entre la protección del derecho del titular de los datos personales y el establecimiento de esfuerzos de colaboración con las empresas farmacéuticas, para la aplicación del conocimiento científico en la investigación del que se derivarán nuevos productos médicos, cuyo beneficio económico directo recaerá en ellas.

Un segundo riesgo entre privacidad y datos disociados para fines científicos se tiene entre los datos sensibles que incluyen la información genética de los pacientes y las investigaciones que se realizan en el genoma humano como parte de los avances médico-biológicos, siendo que la consideración de la información genética resulta necesaria para profundizar en el estudio de la biología humana y sus enfermedades, considerando inclusive patrones hereditarios para el desarrollo de tratamientos médicos específicos.

El aprovechamiento colectivo que ofrece una estrategia de Big Data dirigida al sector salud no limita la consideración del beneficio individual, principalmente en situaciones que hacen necesario que un paciente reciba un trato personalizado, y pueda vincularse electrónicamente con otras fuentes de información para recibir atención médica, realizando intercambio de información con otros prestadores de servicios de salud.

Desde la perspectiva del interés general, es importante salvaguardar el derecho de los titulares a la protección de sus datos personales, para hacerlos accesibles a la colectividad, bajo la tutela del Estado, que en ejercicio de sus obligaciones de proteger los derechos individuales deberá tener la capacidad y habilidad de administrar la información confiada en forma responsable, estableciendo los mecanismos y políticas que aseguren la protección y aprovechamiento responsable de la información contenida en los sistemas de salud, para la investigación científica en el área de salud.

BIG DATA Y ENTIDADES FINANCIERAS

Sabido es que la ingeniería aplicada para perfilamiento y conocimiento de clientes se utiliza en el sector analizado desde hace mucho tiempo, incluso antes de considerarse algún tipo de protección a los datos personales. Tampoco tenía esta actividad un nombre apetecible para una época tan tecnologizada como la actual, era simplemente la labor de analistas de información de muy diversas fuentes para el ofrecimiento de determinados productos para determinados clientes y una pretensión de calificación de riesgo, considerando los antecedentes de cumplimiento de las obligaciones económicas de las personas en general.

Otra condición era que la información o datos que se analizaban se encontraban dispersos en muy diversas fuentes, tanto privadas como públicas, y ciertamente ninguna de ellas contaba con las autorizaciones que los titulares hoy, en términos generales, deben dar a conocer a quienes las manipulan, como es el caso de las llamadas "sociedades de información crediticia", entidades que –refiriéndome al caso mexicano que es muy representativo de los países en los que existe– tienen por objeto fundamental el recopilar y manejar datos bancarios, financieros y otros relativos al historial crediticio y otras operaciones de naturaleza análoga de personas y empresas, mantenerlo y acrecerlo con aquellos datos que les proveen sus propios participantes (bancos, operadores financieros, casas comerciales y autoridades), así como información de operaciones crediticias fraudulentas, con objeto que los mismos sean entregados a los participantes y usados por éstos para llevar a cabo distintas actividades, la mayoría vinculada a explotación mediante el análisis del conocimiento de quienes ahí aparecen.

Al respecto del tema, consideremos al Big Data como tendencia y consecuencia en el avance de la tecnología, es la fórmula perfecta para el análisis de una gran cantidad de información para su posterior explotación por aquellos que la realizan y contar con una herramienta científica para la toma de decisiones. Dicho conocimiento puede poner en jaque la privacidad, la honra, la reputación y, por supuesto, el derecho a la protección de los datos personales, ya que todos tenemos información y datos por evidente consecuencia del desarrollo, actas de nacimiento, registros escolares, antecedentes laborales, historia social, bancaria y financiera.

El derecho a la protección de datos personales viene garantizando un principio de calidad de los datos y el ejercicio de derechos ARCO, que no es más que la garantía de que la información inadecuada, incompleta o excesiva que se contenga en medios sea eliminada o rectificada.

Precisamente en el ejercicio de este derecho radica una disposición creada dentro del sector y circunscrita en las sociedades de información crediticia. En el caso mexicano –y en otros, como el español–, transcurridos seis años en términos generales aplicamos un "reseteo" de aquellos incumplimientos o desviaciones que se hubieran realizado para el cumplimiento de obligaciones y, en consecuencia, aquellos análisis que se realicen contendrán una historia parcial de la realidad en el cumplimiento y perfilamiento que se realice con el Big Data.
De lo anterior surge la inquietud de que ocurre en países donde la legislación no contempla estas figuras y se producen tratamientos relativos a solvencia patrimonial y crédito mediante técnicas de Big Data, pudiendo aparecer información sobre insolvencias crediticias o impagos con una antigüedad sin límite.

BIG DATA Y LA PUBLICIDAD COMPORTAMENTAL

El GT29, a través de su Dictamen 2/2010 sobre publicidad comportamental en línea, la identifica como aquella actividad que "implica la identificación de los usuarios que navegan por Internet y la creación gradual de perfiles que después sirven para enviarles publicidad que corresponde a sus intereses".

Conforme a lo anterior, para este Grupo de Trabajo los siguientes elementos definitorios de este tipo de publicidad son:

- Permite la identificación de "usuarios" (personas físicas, titulares de datos personales).
- La identificación de éstos se efectúa a partir de su navegación por Internet.
- Esta identificación permite, a su vez, la creación gradual de perfiles (profiling).
- La creación de estos perfiles tiene por objeto el envío de publicidad que correspondería "a los intereses" de los usuarios.

Claramente, nos encontramos frente a una actividad especializada que hace uso de Big Data; sin embargo, cabría analizar si, dentro de esta definición, el interés de los usuarios por recibir este tipo de publicidad constituye en sí mismo un elemento que la defina o si, por el contrario y como puede también deducirse, "el interés" radica en aquellos que generan publicidad comportamental.

Esta observación no pasa inadvertida para el GT29, que "no cuestiona los beneficios económicos que la publicidad comportamental pueda aportar a los que la practican" a la vez que establece claramente que esta práctica "no debe realizarse a expensas de los derechos a la intimidad y a la protección de datos de las personas". Consideramos que la misma posición debe ser adoptada por las diferentes autoridades nacionales y difundida entre responsables y titulares.

Por otro lado, es necesario tomar en cuenta que el uso de medios electrónicos para la definición de perfiles (tecnologías de rastreo) como elemento esencial de este tipo de publicidad, se ha convertido en un elemento diferenciador entre las diversas legislaciones que regulan su uso. Existen aquellas que requieren que el uso de dichas tecnologías sea informado a los usuarios y que éstos puedan aceptarlas de forma previa a su instalación en sus propios equipos, con opción a su rechazo; otras requieren de información previa y obligatoria para los usuarios, que les permita rechazar (a posteriori) la instalación de este tipo de tecnologías. Otras simplemente exigen que se proporcione información a los usuarios, sin que necesariamente deba ser previa o accesible antes de su instalación.

En todo caso, es necesario establecer qué legislaciones cuentan con las disposiciones necesarias para salvaguardar los derechos de los titulares de datos personales que pueden ser objeto de publicidad comportamental, así como su expectativa razonable de privacidad.
Identificamos como esencial el cumplimiento del principio de información, que en relación con las finalidades de mercadotecnia, publicidad y prospección comercial, deben encontrarse expresamente recogidos en los Aviso de Privacidad, de forma que aquellos responsables que traten datos personales para dichas finalidades, deban comunicarlo expresamente a los afectados, dando opción a su negativa cuando esta finalidad no resulta necesaria para la relación jurídica existente entre ambas partes.

El uso de tecnologías de rastreo también está expresamente regulado por alguna normativa nacional. En este sentido, es necesario recordar que bajo la rúbrica "Política de cookies, web beacons u otras tecnologías similares", las normativas nacionales aludidas disponen (de manera análoga a la mexicana) que cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento deberá informar al titular, a través de una comunicación o advertencia colocada en un lugar visible, sobre el uso de esas tecnologías y sobre el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos.

Por lo anterior, en el contexto de Big Data y la publicidad comportamental, se hace necesario emprender acciones de formación y concienciación sobre el uso de las tecnologías de rastreo que la normativa vigente ya regula, pero que su propia novedad parece alejar de su cumplimiento integral.

En esencia, se considera que la especialidad de actividades de Big Data (como la publicidad comportamental) debe dar lugar a su identificación, estudio y definición de actividades de cumplimiento, para que cada una de ellas se desarrolle con respeto de los derechos fundamentales de las personas, en relación con el tratamiento de sus datos personales y de su privacidad.

BIG DATA Y EDUCACIÓN

Hoy en día existe una cantidad ingente de información que está chocando en nuestra sociedad y que en la mayoría de las ocasiones es imposible o insostenible de tratar o analizar con herramientas de base de datos, consolidando un entorno donde es común la proliferación de webs, apps de imagen y sonido, redes sociales, dispositivos móviles, sensores.

Por eso, debemos de ser conscientes de la realidad en la cual vivimos e irnos adaptando a ella. Para lo cual es bueno conocer y comprender las tendencias actuales y futuras sobre modelos

basados en Big Data. De esta forma se ayudará a que las instituciones educativas puedan adaptarse e identificar a estudiantes en riesgo, de forma que puedan intervenir con el fin de reducir la deserción y aumentar las tasas de graduación de los alumnos/as.

Este tipo de medidas dentro del ámbito académico se pueden abarcar desde dos perspectivas: una centrada en la propia institución, y otra, en el aprendizaje. Siendo mucho más efectiva la primera, ya que propone modelos educativos centrados en Big Data que optimizan la deserción en el ámbito educativo (centro e instituciones), así como también realiza un seguimiento más exhaustivo de los alumnos/as.

Una forma de logarlo es mediante el análisis y comprensión de la información disponible en la web, como son: redes sociales, sistemas educativos, webs institucionales.

Esta innovación educativa está en auge actualmente, gracias a los conocidos MOOC (Massive Online Open Courses), cursos de formación abiertos, masivos y gratuitos. Nacieron en el año 2008 y tenían como iniciativa el acercamiento de conocimiento de nivel superior a todos los internautas, sin tener que ser estudiantes de universidad. Es una formación globalizada e internacional que busca un público más amplio, con el objetivo de liberar conocimiento. Cuenta con un sistema de evaluación propio, que valorar a cada uno de los estudiantes en función de los conocimientos adquiridos.

Además, este tipo de enseñanza no solo ayuda en la lucha de la brecha digital; sino que también proporciona una serie masiva de información (Big Data) muy importante para la mejora de la enseñanza en todos los niveles educativos: social, cognitivo y emocional, a nivel individual, grupal e institucional. Al mismo tiempo que facilita y mejora el apoyo que se ofrece en tiempo real a cada uno de los alumnos/as de estos cursos.

Toda esa información recogida tiene un gran valor educativo para las instituciones, ya que ayudará a mejorar el diseño curricular de muchas de las materias adaptándose, aún si cabe, a las necesidades reales de los alumnos/as. De esta forma se podrán solucionar algunas de las necesidades que se requieren en las universidades, como son: módulos más adaptados, módulos actualizados, plantear tareas, recoger el feedback y diseñar una formación más relevante que constituya un aprendizaje más efectivo y mejore la enseñanza.

Por último y sin menor relevancia, un punto a considerar dentro de esta problemática son los aspectos éticos, morales y legales de dicho uso de la información. Un elemento crucial en la privacidad de datos. Las herramientas analizadas a lo largo de la presente Declaración (como la evaluación de impacto) se manifiestan imprescindibles a la hora de realizar este tipo de tratamientos, sobre todo si son de menores.

El concepto de portabilidad de los datos e interoperabilidad

En una época en donde la migración de servicios hacia soluciones de Cloud Computing y aplicaciones es cada vez más común, la protección de datos se vuelve fundamental, pero también la posibilidad de estandarizar los procesos de portabilidad de los datos de usuarios asociados a diversos servicios de Cloud Computing.

Se debe implementar una política de portabilidad e interoperabilidad como política de contratación. La portabilidad de datos representa el mayor riesgo operativo para los usuarios del Cloud Computing, ya que ante la ausencia de regulación que establezca los formatos, parámetros, términos y condiciones bajo los cuales un proveedor de Cloud Computing portará los datos a otro en caso de terminación del contrato del primero, como ha ocurrido en el caso de los servicios telefónicos, la posibilidad de hacer efectivo este derecho radica en la inclusión de una cláusula contractual que precisamente se encargue de lidiar con este tema.

Desafortunadamente para el crecimiento de la industria de servicios de Cloud Computing, la obligación de permitir la portabilidad del dato es una cláusula que el cliente o usuario debe buscar incluir en el contrato, y es que no solamente se trata de hacer que el proveedor del servicio entregue un soporte magnético u óptico que contenga la información del usuario, sino que además el cliente debe buscar garantía de que esos datos entregados puedan ser leídos y procesados por su nuevo proveedor, y que la información en poder del proveedor primigenio sea destruida dentro del plazo legal aplicable. Dicho proceso debe ser verificable, en el entendido que no debe existir ninguna información adicional o derivada de la información original que pueda ser utilizada o considerada propia por el proveedor.

Es importante hacer notar que la creciente configuración de nubes pone en peligro el principio de neutralidad de la Red, ya que el hecho de que un cliente o usuario de servicios en nube no pueda portar sus datos entre uno u otro proveedor pone en entredicho la libertad de contratación, el derecho de protección y uso de sus datos, razón por la cual diversos expertos ya han comenzado a elaborar el concepto denominado cloud neutrality, señalando la necesidad de establecer la portabilidad de los datos como un derecho legalmente previsto en los contratos en cuestión, y aceptado por el proveedor, mismo que deberá sujetarse a reglas básicas que permitan portar los datos y supervisar la debida realización de los mismos.

Por lo anterior, es muy importante establecer que en la actualidad dentro de las diversas opciones que ofrecen los proveedores de Cloud Computing se pueden encontrar soluciones abiertas a la portabilidad de datos y soluciones sin portabilidad.

Aunque, como se ha señalado anteriormente, la idea es que se generen en un futuro parámetros internacionales que permitan a los usuarios de soluciones de Cloud Computing requerir y exigir

a los proveedores las mismas reglas de portabilidad de datos sin restricciones, actualmente los usuarios deben buscar solución abierta a la portabilidad, en el entendido que las mismas permiten con mayor facilidad transferir todos sus datos y aplicaciones del usuario desde un proveedor de Cloud Computing a otro (o a los sistemas propiedad del cliente), garantizando la disponibilidad de los datos y la continuidad del servicio.

Es vital tener en cuenta que los contratos de Cloud Computing pueden terminarse no solo en el caso de rescisión de contrato por parte del cliente, sino por otras circunstancias ajenas al mismo, como podría ser el fin de la prestación de algún tipo de servicio por parte del proveedor, el cambio de su política comercial o cambios en el marco regulatorio existente, razón por la cual, el usuario debe tener en cuenta qué tipo de contrato tiene firmado, ya que entre más restringido esté el derecho de portar sus datos, mayor será la dificultad de transferir sus datos.

Es fundamental que los usuarios de soluciones de Cloud Computing celebren acuerdos con proveedores reconocidos por su calidad en el servicio y que reconozcan los derechos de portación de los datos y apliquen la legislación local de protección de datos. El usuario de soluciones de Cloud Computing debe tener la opción de exigir a su proveedor la portabilidad de la información a sus propios sistemas de información o a un nuevo prestador de Cloud Computing, lo anterior, siempre de acuerdo con las condiciones y términos acordados para tal efecto.

La portabilidad de datos debe también generarse y adecuarse para resolver los casos de transferencias internacionales, que podrían generar afectaciones de derechos y conflictos entre legislaciones, en el entendido que dicha situación pudiera dar lugar a transferencias de datos a proveedores situados en jurisdicciones con menos medidas de protección a los datos personales de los usuarios y requerir, en su caso, autorización previa de la Autoridad de Control.

El debido establecimiento de los procedimientos de portabilidad de datos, y la subsecuente entrega de información a un nuevo proveedor hará más sencillo el proceso de migración de bases de datos, sin afectar, dañar o impedir dicha migración, resguardando la integridad de los datos. El proveedor debe garantizar por escrito dicha obligación de portar de manera adecuada e íntegra la información y detallar los procedimientos aplicables. No obstante lo anterior, la determinación de normas y parámetros técnicos aplicables respecto a la migración y recepción de bases de datos entre proveedores de soluciones de Cloud Computing son necesarias para generar interoperabilidad entre los mismos y sus sistemas para asegurar la portabilidad de datos de los usuarios.

Las partes deben establecer procedimientos, con la finalidad de que una vez concluida la portabilidad, el proveedor anterior garantice al usuario el borrado seguro de los datos entregados bajo el contrato anterior. Dichos procesos de borrado seguro pueden ser realizados y/o validados por terceros designados previamente en el contrato.

La interoperabilidad debe en todo momento aligerar la carga del cumplimiento de las funciones básicas de las soluciones de Cloud Computing, al asignar el quién, qué y dónde para mantener organizados los datos no estructurados. Estas tareas deben ser ejecutadas sobre servidores que formen parte de las soluciones de Cloud Computing como una tarea en segundo plano, virtualmente invisible para los usuarios, manejando archivos sin interrumpir el flujo de trabajo.

La interoperabilidad de redes debe permitir a los proveedores desarrollar una interacción segura y fluida entre centros de datos de la nube y crear centros de datos mucho más sencillos con una infraestructura más ágil que mejore los procesos de gestión.

Por lo anterior, la interoperabilidad debe ayudar a alcanzar la eficiencia global del Cloud Computing mediante las mejores prácticas de la infraestructura. Para facilitar lo descrito, los proveedores deben proporcionar y estandarizar las mejores prácticas, modelos de uso, diseños de referencia y sólidas herramientas para planificar e implantar estrategias de la nube garantizando la interoperabilidad de las redes y soluciones utilizadas. La creación de estándares para soluciones de interoperabilidad en Cloud Computing debe incluir elementos relacionados con las redes definidas por el software, innovaciones en almacenamiento y avances en arquitectura de redes utilizadas.

Para finalizar, se deben tener en cuenta alguna de las responsabilidades que los proveedores de servicio deberían asumir:

- Responsabilidad por daños por interrupción en el servicio. Independientemente de establecer los parámetros mínimos de servicios, los proveedores deben reconocer expresamente en los contratos que contengan soluciones los niveles de responsabilidad directa por la interrupción que afecten los servicios. Es cierto que el cómputo en la nube establece un problema práctico para determinar la responsabilidad de los proveedores de servicios por fallas en los mismos, ya que el cómputo en la nube consiste en la mezcla de recursos e infraestructuras para poder brindar a los usuarios movilidad, disponibilidad y funcionalidad; por tanto, es importante que los proveedores de Cloud Computing determinen y delimiten las partes de su red e infraestructura en las cuales aceptan control y responsabilidad ante el usuario por fallas en los servicios prestados. Determinado lo anterior, es muy importante establecer no solamente procesos de falla, sino procesos de aceptación de responsabilidad y las penalidades aplicables por dichas fallas.

- Acuerdo de Niveles de Servicios. Ya antes hemos hablado de la importancia de un acuerdo de niveles de servicio o SLA (Service Level Agreement), por lo que en este punto vale la pena recordar que el contrato de Cloud Computing debe contener un anexo que detalle de manera eficiente los parámetros, niveles y términos de servicios que permitan

la funcionalidad, de acuerdo con lo requerido por el cliente, dentro de dicho acuerdo de niveles de servicio se deben incluir por lo menos los siguientes elementos:

i) Disponibilidad Mínima de los Servicios e Infraestructura.
ii) Tabla de penalidades por incumplimiento en la disponibilidad.
iii) Detalle de los parámetros técnicos a medir durante la prestación de los servicios.
iv) Tipos y periodicidad para la entrega de reportes.
v) Tiempos máximos para reparación de fallas.
vi) Procesos de escalamiento.
vii) Detalle sobre los procesos de seguridad aplicables.
viii) Detalle de monitoreo.

Es muy importante señalar que una de las obligaciones claves del cómputo en la nube es la funcionalidad de servicios en tiempo real y la garantía de protección y resguardo eficiente de la información, transmitida, intercambiada y/o almacenada a través de recursos de cómputo en la nube.

No basta agregar niveles de servicios, ya que si estos no garantizan la disponibilidad y funcionalidad de los mismos, no puede garantizarse que los servicios de cómputo en la nueve sean prestados de forma eficiente, ni que otorguen las ventajas ofrecidas al usuario de manera efectiva.

- Responsabilidad de garantizar la disponibilidad del dato. Es indispensable que los proveedores de Cloud Computing garanticen la disponibilidad y seguridad del dato almacenado, transmitido e intercambiado, ya que más allá de la forma en que pueda funcionar o estar conformada la infraestructura utilizada o el servicio prestado, la capacidad del usuario de recuperar, modificar o eliminar su información en tiempo real no puede ser limitada. La capacidad para utilizar los datos almacenados, en tiempo real y en cualquier dispositivo, debe ser la premisa del prestador de servicios de cómputo en la nube. Adicionalmente a lo antes referido, la responsabilidad por afectar la disponibilidad en el acceso a los datos de usuario debe ser una responsabilidad que el proveedor reconozca en los contratos en cuestión.

- Localización del dato. Este punto en particular puede generar muchas confusiones y discusiones entre los especialistas, ya que, si bien es cierto que la posibilidad de resguardar un solo dato o bases de datos en diferentes lugares de forma simultánea es una de las características principales del cómputo en la nube, los proveedores defienden la idea de mantener en secreto los diversos lugares en donde se guarda la información, siempre por cuestiones de seguridad y protección del usuario y el proveedor. Uno de los problemas que puede generar la ubicuidad de los datos es, sin duda, la determinación de la jurisdicción aplicable para el caso de un conflicto entre las partes o que se provoque una transferencia internacional de datos.

Si bien es cierto que el secreto de los datos es importante por temas de seguridad, también lo es que debe existir compromiso expreso del proveedor de señalar al usuario el lugar físico principal en donde se guardará la información, además de borrar y hacer constar la eliminación de datos de cualquier registro y lugar del proveedor al finalizar el contrato.

Conclusiones

Por lo anteriormente expuesto entendemos:

Que siendo los datos personales la moneda de oro de la economía digital y el motor de la economía del siglo XXI, los datos son el negocio de los negocios.

Que como quiera que los datos personales son un activo y generan valor para las organizaciones y el Estado, no cesarán los esfuerzos para, de una parte, flexibilizar su uso, especialmente frente a regulaciones que siguen, en buena medida, el modelo europeo sobre tratamiento de datos personales, y de otra parte, exigir el debido tratamiento de esa información para evitar la eventual vulneración de los derechos de las personas cuando su información es tratada indebidamente.

Que los beneficios o maleficios del Big Data dependerán del uso ético y responsable que haga quien posee enormes cantidades de datos sobre diversos aspectos de millones de personas alrededor del mundo.

Que debido a que con la tecnología se puede hacer casi todo, la pregunta que surge es la siguiente: ¿todo lo tecnológicamente posible es social y humanamente deseable?

Que ante el desarrollo de estas tecnologías que indudablemente tienen consecuencias altamente positivas para la humanidad, con grandes posibilidades en sectores como la sanidad, los diferentes Estados, las entidades y las empresas se deben implicar para que estas tecnologías no se utilicen con fines invasivos de la privacidad de las personas.

Que corresponde a los Estados adaptar las legislaciones y unificarlas, desarrollando nuevas herramientas que mejoren la privacidad de los individuos cuando se usan estos sistemas, y corresponde a las empresas y entidades implementarlos.

Que estos sistemas, herramientas y garantías deben ir encaminados a los principios de transparencia, objeción al tratamiento, inocuidad para el afectado, calidad de los datos, minimización de los mismos y responsabilidad en lo que respecta a las relaciones con los individuos, debiendo obligar las diferentes legislaciones a la implantación de medidas de índole técnica y organizativa que prevean la evaluación de impacto en privacidad, el privacy by design, la adopción de medidas de seguridad, la anonimización de los datos, el ejercicio

de derechos de acceso, rectificación, cancelación y oposición y la disponibilidad, integridad y confidencialidad de la información.

Que hay que preguntarse en qué clase de sociedad queremos vivir, qué tipo de información estamos dispuestos a que se recabe diariamente sobre lo que hacemos, dónde vamos, sobre cómo nos comportamos y durante cuánto tiempo ha de ser analizada y accesible.

Que la tecnología y la información no son por sí solas el problema. Todo radica en su uso. Si se puede hacer algo con la información, alguien lo va a hacer (o lo está haciendo): ¿hacia dónde vamos a seguir? Y, ¿adónde vamos a parar?

Que es bienvenida la innovación y es bienvenido el Big Data, pero también bienvenida la reflexión crítica sobre los riesgos del big data. No podemos ser espectadores ingenuos y ciegamente maravillados por lo que nos dicen sobre el Big Data. Como todo en la vida, no es positiva la "tecnofobia" ni la "tecnofascinación", pero sí la tecnoreflexión y sobre todo, la ética.

DECLARACIÓN DE SAN JOSÉ, HACIA LA IMPLANTACIÓN DE UN SELLO SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN IBEROAMÉRICA[9]

Introducción

Si bien existe un consenso unánime en la validez y vigencia de los principios de Protección de Datos Personales, también hay coincidencia generalizada en la necesidad de revisar su contenido para hacerlo más acorde con las exigencias que la globalización y el desarrollo de las tecnologías de la información y la comunicación plantean.

La dimensión transnacional es en la actualidad uno de los principales retos de la protección de datos.

Es conveniente tener en cuenta que la evolución de las tecnologías de la información define un nuevo escenario con características específicas:

a) Se trata de un escenario global, trasnacional, que supera la esfera local.

b) Las redes sociales, los dispositivos móviles inteligentes, y en el futuro inmediato desarrollos como el "Big Data" o el "Internet de las cosas", plantean nuevos problemas para la protección de la privacidad: análisis del comportamiento de los internautas, marketing viral o de geolocalización por solo citar algunos ejemplos.

c) El individuo se convierte en un agente activo "colgando" datos e informaciones de terceros.

d) La capacidad de control de internautas, generalmente desinformados o poco informados, es nula y tampoco se encuentran convenientemente concienciados.

e) Determinados colectivos, singularmente los menores, se encuentran en riesgo.

f) Necesidad de continuar afianzando el derecho a la portabilidad de los datos.

9. La Declaración de San José, hacia la implantación de un Sello sobre el tratamiento de datos personales en Iberoamérica, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, presentada en la ciudad de San José (Costa Rica), el 15 de marzo de 2016, por Mauricio Paris y Daniel López Carballo, en el transcurso de II Privacy Data Protection Forum. La Declaración fue elaborada por Romina Florencia Cabrera, María Paulina Casares Subía, Camilo Alfonso Escobar Mora, Joel Gómez Treviño, Alonso Hurtado Bueno, Lorena Higareda Magaña, Lilibeth Alvarez, Dulcemaría Martínez Ruíz, Sara Molina Pérez-Tomé, Eduardo Lagarón Martín, Mauricio París, Romina Garrido, Jessica Matus, Héctor Guzmán Rodríguez, Ramón Miralles López, Milagros Olivos Celis, María Julia Giorgelli, Agustina Callegari, Javier Raimo, María Eugenia Cafiero, Lainiver Mendoza Munar, Laura Vivet Tañà, Matías Jackson, Cynthia Tellez Gutierrez, Patricia Reyes Olmedo y Yarina Amoroso Fernández, coordinados por Daniel López Carballo y Francisco Ramón González-Calero Manzanares.

Por ello la protección de datos personales debe superar cada día más la barrera nacional.

Durante una primera etapa, que podríamos situar en la década iniciada en el año 2000, la comunidad internacional de protección de datos orientó sus esfuerzos a promover la elaboración de textos que pudieran constituir una especie de "carta internacional de la protección de datos", con principios, derechos y garantías básicos que pudieran ser asumidos por todas las regiones y entornos culturales y jurídicos. El resultado más acabado de estos esfuerzos fue la Resolución sobre "Estándares de Privacidad en relación con el tratamiento de Datos de Carácter Personal", aprobadas en Madrid por la 31 Conferencia Internacional de Autoridades de Protección de datos y Privacidad.

Teniendo plena conciencia, se trabaja en instituir mecanismos de certificación en materia de protección de datos y de sellos y marcados de protección de datos que permitan a los interesados evaluar rápidamente el nivel de protección de datos que ofrecen los responsables y los encargados del tratamiento.

El "Sello Europeo de Protección de Datos" tiene un objetivo principal: "crear confianza entre los interesados", y facilitar las transferencias internacionales de datos, por tanto, podemos considerarlo un argumento de valor competitivo, en el contexto del mercado único digital europeo, que no solo interesa a las empresas europeas, también a las de fuera de Europa, en tanto dirijan su oferta de servicios y productos a los europeos. En este sentido cobra interés para Iberoamérica.

El Reglamento General de Protección de Datos de la Unión Europea dispone que las certificaciones y códigos de conducta se encuentran entre los mecanismos que consideran una transferencia internacional de datos con garantías adecuadas.

Como toda solución también trae aparejado nuevos retos, tales como:

a. Incentivar que las autoridades de Protección de Datos cooperen para garantizar mecanismos de certificación armonizados.

b. Propiciar que las tasas también sean armonizadas.

c. Precisar el objeto de la certificación.

d. Garantizar la transparencia del proceso de certificación y basado en proceso de auditoría.

e. Registro de certificados.

Alcanzar un sello de Protección de Datos supone, además, asumir un reto desde la ingeniería de Software toda vez que hay cuestiones que deben ser asumidas por diseño de las aplicaciones y servicios que se instrumenten, tales como los que realizan los servidores y buscadores. Otro tanto puede lograrse desde el diseño de las Bases de Datos. También es importante incluir estos requerimientos desde la evaluación de calidad y certificación de soluciones digitales.

¿Qué es un Sello de Protección de Datos?

El Reglamento General de Protección de Datos considera una transferencia internacional de datos con garantías suficientes cuando existe una adhesión a Códigos de Conducta y Certificaciones.

En lo que respecta a la regulación de las certificaciones, los Estados Miembros, las autoridades de control, el Consejo Europeo de Protección de Datos y la Comisión deberán promover modelos de certificación, sellos o marcas que sirvan para demostrar cumplimiento con el RGPD. Las específicas necesidades de las microempresas y las PYMES deberán ser tenidas en cuenta.

Será de carácter voluntario y no reducirá la responsabilidad del cumplimiento con el RGPD por parte de controladores y procesadores de datos.

Serán otorgadas por entidades de certificación o por las autoridades de control. De otorgarla el Consejo Europeo de Protección de Datos, se denominará como certificación tipo "Sello Europeo de Protección de Datos". Se otorgará por periodos máximos de 3 años, pudiendo ser renovada si se cumplen los requisitos para ello. El Consejo Europeo de Protección de Datos llevará un registro público con todas las certificaciones, sellos y marcas otorgados.

En relación con la entidad de certificación que emite y renueva los certificados, sellos o marcas, después de informar a la autoridad de control, deberá contar con un nivel adecuado de expertise en protección de datos. Cada Estado decidirá quién otorga la acreditación a estas entidades de certificación, pudiendo ser:

- La autoridad de control competente.

- La Entidad Nacional de Acreditación denominado en acuerdo con el Reglamento (CE) No 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos, sin perjuicio de las competencias de la autoridad de control.

Quedan igualmente detallados los requisitos mediante los cuales se obtiene la condición de entidad de certificación y su renovación como máximo por periodos de 5 años. En el caso de incumplimiento por parte de la entidad de certificación, la acreditación podrá ser revocada.

Por ello el Sello Iberoamericano de Protección de Datos debidamente aprobado por el Consejo Europeo de Protección de Datos sería un instrumento que facilitaría las transferencias internacionales de datos hacia Iberoamérica y aportaría confianza en el consumidor al igual que los conocidos "sellos de confianza".

Los sellos de confianza nacen hace casi 20 años para resolver una necesidad concreta: fomentar la confianza de los consumidores al hacer transacciones por Internet, buscando fortalecer principalmente al comercio electrónico "business to consumer" (negocio a consumidor).

En aquella época se buscaba resolver principalmente tres situaciones que incomodaban a muchos usuarios de Internet:

- Conocer quién estaba detrás de una página web (la identidad legal del negocio);
- Que el sitio web contaba con mecanismos de seguridad mínimos que protegieran la información bancaria y datos de los consumidores durante su tránsito entre la computadora del comprador y el servidor del vendedor; y
- En caso de que el consumidor tuviera alguna inconformidad o queja hacia el negocio respecto de la prestación del servicio o bien entregado, ésta fuera atendida de manera expedita y profesional.

Con el paso de los años la privacidad, particularmente en entornos digitales, ha tomado cada vez mayor relevancia a nivel mundial. Es por ello que muchos "sellos de confianza" también han buscado certificar a sitios web que cuenten con "buenas prácticas" en materia de privacidad.

¿Cómo funcionan los sellos de confianza?

Los sellos de confianza usualmente son operados por empresas independientes creadas para tal efecto, o por organizaciones industriales o asociaciones de empresas que buscan otorgar un beneficio particular a sus afiliados.

Para ser acreedor o estar autorizado a usar un sello de confianza, usualmente se requiere que el negocio, entidad o individuo:

- Presente la solicitud correspondiente en el portal de la empresa o asociación administradora del sello.
- Usualmente la solicitud va acompañada de una serie de documentos que buscan acreditar, entre otras cosas, lo siguiente:

- la identidad legal del solicitante,
- las medidas de seguridad tecnológicas,
- las políticas de privacidad, y
- las políticas de solución de quejas.

- Pague la cuota correspondiente.

- Se someta al escrutinio correspondiente por parte de la empresa o asociación que administre el sello de confianza, para determinar si los parámetros o criterios necesarios para la obtención del sello son satisfechos por el solicitante.

No uniformidad legislativa: países con legislación en protección de datos y sin legislación en protección de datos.

El término respecto a si los países "cuentan con un nivel adecuado de protección" se encuentra íntimamente relacionado con el desarrollo de la protección de datos personales en el ámbito europeo, específicamente, a la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en la que se tomó en consideración que pueden existir diferencias en cuanto a los niveles de protección debido a la disparidad de las legislaciones de los Estados miembros y de los países terceros; en virtud de esto, por mandato del artículo 29 se creó el grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual entre otras cosas se encarga de analizar los instrumentos jurídicos para catalogarlos como normas generales o sectoriales.

Artículo 30

1. El Grupo tendrá por cometido:

a) Estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) Emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) Asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así

como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) Emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.

3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.

4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.[10]

En este sentido, para el desarrollo de este apartado se considera que la Directiva 95/46 adquiere relevancia, puesto que el desarrollo de la protección de datos en Iberoamérica se encuentra relacionada con la disparidad o no uniformidad de la legislación, ya que hay países que cuentan con legislación específica en la materia y hay otros en donde la regulación se ha realizado de manera sectorial.

Pedro Dubie justifica la existencia de estas normas con base en criterios de "verticalidad u horizontalidad"[11]. Esta clasificación sirve para establecer si un país cuenta o no con un nivel de protección adecuado como lo exige la Unión Europea. Así, se tiene que una ley vertical es una norma que regula una sola categoría de datos en forma específica, entre las virtudes que presenta esta estructura jurídica se encuentran dos: la primera es que la ley vertical permite regular muchas de las características que distinguen a una categoría de datos, por ejemplo,

10. Directiva 95/46/CE Del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

11. La protección de datos en Latinoamérica y el interés de España por un nivel de protección adecuado. Entrevista realizada a Pedro Dubie por Pablo Rui Pérez García, en el marco del Programa Revista de Informática, en la Universidad Nacional de Educación a Distancia (UNED) el 11 de enero de 2003.

es muy habitual observar que los datos crediticios tienen un problema que no tienen los datos de salud, y que los datos del marketing directo son muy diferentes de los datos de seguridad pública, que no es lo mismo tratar datos sensibles que tratar datos que provienen de una fuente de acceso público o restringida; y la otra ventaja es de carácter histórico, pues el legislador se aboca a regular solo lo que la sociedad le reclama y no involucra todo el tratamiento de datos.

Por el contrario, una ley horizontal es una norma que regula todas las categorías de datos de una sola vez; es una norma que abarca todo el universo de datos existentes y a todos ellos les aplica un régimen único con algunas salvedades respecto a determinadas categorías de datos, como por ejemplo, datos de seguridad pública. La ventaja que presenta es que de una vez para siempre quedan sometidos en una sola ley todos los datos personales y bajo el imperio de una sola autoridad; es decir, son leyes que luego necesitan de leyes posteriores que regulen en específico cada categoría de datos; el beneficio interesante que conlleva es que se produzca un orden normativo, ya que toda ley especial posterior de datos específicos estará siempre referenciada a la ley general y horizontal.

Además, la reciente sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015, en el asunto C-362/14 Maximillian Schrems vs Data Protection Commissioner con la intervención de Digital Rights Ireland Ltd. ha declarado nula la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, entre otros argumentos por la falta de revisión y seguimiento por parte de la Comisión Europea y la imposibilidad de control por parte de las autoridades nacionales de control, circunstancias (revisión, seguimiento, auditoría, revocación o renovación) que sí se dan en los mecanismos de certificación.

Para poder entender mejor el estado en el que se encuentra la legislación en materia de protección de datos en Iberoamérica, realizaremos un análisis para determinar los países que cuentan con legislación específica y los países que cuentan con legislación sectorial. Para ello, se analizará desde el reconocimiento constitucional de la protección de datos como derecho fundamental, el sector al que es aplicable la legislación y si existe una autoridad de control encargada de garantizar a las personas la protección de sus datos personales.

Países con legislación específica en Protección de Datos.

PAÍS	CONSTITUCIÓN	NOMBRE DE LA LEY
Andorra	Artículo 14. Se garantiza el derecho a la intimidad, al honor y a la propia imagen. Toda persona tiene derecho a ser protegida por las leyes contra las intromisiones ilegítimas en su vida privada y familiar.	Ley 15/2003 cualificada, de 18 de diciembre, de protección de datos personales "Qualificada de protecció de dades personales".
Argentina	Artículo 43. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.	Ley 25326 del 2 de noviembre del 2000. Ley 1845 de Protección de Datos Personales, Ciudad Autónoma de Buenos Aires.
Colombia	Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.	Ley Estatutaria 1581 del 17 de octubre de 2012 por el cual se dictan disposiciones generales para la protección de datos personales. Ley Estatutaria 1266 del 31 de diciembre de 2008 por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales.

Costa Rica	Artículo 23. - El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley. Artículo 24. - Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.	Ley 8968 de 7 de julio de 2011 "Protección de la persona frente al tratamiento de sus datos personales".
Chile	Artículo 19.4 La constitución asegura a todas las personas: El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.	Ley 19628, del 28 de agosto de 1999, sobre Protección de la Vida Privada.
España	Artículo 18.4: La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos	Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personal.

México	Artículo 6. - [...] La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Artículo 16.- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. Toda persona tiene derecho a la protección de sus datos personales, 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.	Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010.
Nicaragua	Artículo 26. - Toda persona tiene derecho: A su vida privada y la de su familia; A la Inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo; […] A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información	Ley 787 de Protección de Datos Personales.

Perú	Artículo 2. - Toda persona tiene derecho a: 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal […]Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. Artículo 161 y 162. - Defensa de los derechos fundamentales de la persona y de la comunidad. Artículo 200: Garantías constitucionales: 3.- La Acción de Hábeas Data, que la Procede contra el hecho u omisión, Parte de cualquier autoridad funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2, inciso 5) y 6) de la Constitución	Ley 29733, de 3 de julio de 2011, de Protección de Datos Personales.
Portugal	Artículo 35. Utilización de la informática. 1. Derechos de los ciudadanos 2. La ley define el concepto de datos personales, y las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección por medio de un órgano administrativo independiente. 3. Límites utilización de la informática.	Ley 67/98 de Protección de Datos Personales del 26 de octubre.

República Dominicana	Artículo 44.2 Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos; Artículo 70. Hábeas data. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística.	Ley Orgánica de Protección de Datos de Carácter Personal, Ley 172-13.

Andorra: Legislación aplicable a entidades privadas y públicas, cuenta con una autoridad específica en materia de protección de datos, constituida por un organismo público con personalidad jurídica propia, independiente de las Administraciones públicas y con plena capacidad de obrar (Agència Andorrana de Protecció de Dades, APDA).

Argentina: Se reconoce a nivel constitucional la acción de Habeas Data junto con el amparo y Habeas Corpus, su legislación en materia de protección de datos es aplicable al sector público y privado, cuenta con un órgano de control, descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación (Dirección Nacional de Protección de Datos de Argentina).

Se destaca la Ley CABA 1845/2006, emitida por la Legislatura de la Ciudad Autónoma de Buenos Aires, la cual tiene por objeto regular, dentro del ámbito de la Ciudad de Buenos Aires, el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a

ser asentados en archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa; asimismo, se reconoce como organismo de control a la Defensoría del Pueblo de la Ciudad de Buenos Aires.

Colombia: Legislación aplicable a entidades públicas y privadas, contempla como autoridad en protección de datos a la Superintendencia de Industria y Comercio a través de una Delegatura para la protección de datos personales, quien ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos y garantías previstos en la Ley[12].

Costa Rica: Legislación aplicable a los datos personales que figuren en bases de datos automatizadas o manuales de organismos públicos y privados, como autoridad de control contempla a la Agencia de Protección de Datos de los Habitantes (Prodhab), órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz que goza de personalidad jurídica instrumental propia en el desempeño de sus funciones, en la administración de sus recursos y presupuesto, así como para suscribir contratos y convenios que requiera para el cumplimiento de sus funciones[13].

Chile: Legislación aplicable al tratamiento de datos de carácter personal en registros o bancos de datos de organismos públicos y por particulares, no contempla una autoridad de control o única encargada de garantizar la protección de datos, ya que únicamente se señala la obligación para el Servicio de Registro Civil e identificación de llevar el registro de los bancosde datos en poder de organismos públicos[14].

España: Legislación aplicable a los sectores público y privado. La autoridad de Control es la Agencia Española de Protección de Datos, que es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones[15].

México: Legislación aplicable al sector privado, la autoridad de control es el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) antes (Instituto Federal de Acceso a la Información y Protección de Datos Personales (IFAI), quien a raíz de la reforma constitucional en materia de transparencia del año 2014, se le otorgó autonomía constitucional. La construcción del derecho a la protección de datos personales en México es sui géneris, su nacimiento se encuentra vinculado al derecho de acceso a la información pública previsto en el artículo 6 constitucional, ya que a raíz de la reforma de 2007 se establecieron las primeras menciones constitucionales limitantes al ejercicio del derecho de acceso a la información,

12. Artículos 19 y 20 de la Ley Estatutaria 1581 por el cual se dictan disposiciones generales para la protección de datos personales.
13.. Artículo 15 de la Ley 8968, protección de la persona frente al tratamiento de sus datos personales.
14. Artículo 1 y 22 de la ley No. 19.628 sobre Protección de la Vida Privada.
15. Artículos 2 y 35 de la Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personales.

relativas a la vida privada y los datos personales, en este sentido, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), que entró en vigor desde 2002, se contemplaba ya un apartado específico pero muy limitado en su

Capítulo IV, relativo a la protección de datos personales aplicable al sector público, ya que fue hasta 2009 que se reconoció la protección de datos como un derecho humano y fundamental independiente del acceso a la información pública.
Como consecuencia de las reformas constitucionales que poco a poco han ido reconociendo la protección de datos personales como un derecho independiente, se tiene contemplada la expedición de la Ley General de Protección de Datos Personales aplicable al sector público, no obstante, en tanto no se expida dicha ley, la protección de datos en dicho sector será regulada a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que se encuentra en vigor[16].

Nicaragua: Legislación aplicable al sector público y privado. La autoridad de control es la Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público, que contará con un director designado por la máxima autoridad administrativa de dicho ministerio, y que tiene por objeto el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada[17].

Perú: Legislación aplicable a la Administración pública y privada. La Autoridad Nacional de Protección de Datos Personales es el Ministerio de Justicia, a través de la Dirección Nacional de Justicia, misma que ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras[18].

Portugal: Legislación que traspone la Directiva 95/46 del Consejo de Europa, la autoridad de control es la "Comissão Nacional de Protecção de Dados", que es una entidad administrativa independiente con funciones de autoridad, que opera junto a la Asamblea de la República[19].

República Dominicana: Legislación aplicable al sector público, el órgano de control es la Superintendencia de Bancos, pero únicamente respecto a los bancos de datos públicos y privados destinados a proveer informes crediticios[20].

Uruguay: Legislación aplicable al ámbito público y privado, el órgano de control es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), que se encuentra dotada de autonomía técnica, la Unidad Reguladora y de Control de Datos Personales estará dirigida por un consejo integrado por tres miembros; asimismo, se destaca

16. Ley Federal de Protección de Datos Personales en Posesión de Particulares.
17. Artículos 2 y 28 de la Ley 787 de Protección de Datos Personales.
18. Artículos 3 y 32 de la Ley Ley 29733, de Protección de Datos Personales.
19.. Artículo 21 de la Ley 67/98 de Protección de Datos Personales del 26 de octubre.
20. Artículos 1 y 29 de la Ley Orgánica de Protección de Datos de Carácter Personal, Ley 172-13.

Países sin legislación en protección de datos o que cuentan con alguna norma de carácter sectorial.

PAÍS	CONSTITUCIÓN	NOMBRE DE LA LEY
Brasil	Artículo 5. LXXII se concederá "habeas data": a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. LXXVII son gratuitas las acciones de "habeas corpus" y "habeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.	ey 9296, del 24/6/1996, por la que se reglamenta la interceptación de comunicaciones telefónicas (Artículos 1 al 10). Ley 9507, del 12/11/1997. Derecho de Acceso a la Información y reglamenta el "habeas data" (Artículo 1). Código Penal: violación del domicilio, de correspondencia; de comunicación telefónica, divulgación de secreto; violación de secreto profesional. Ley Complementaria 105. Secreto de las operaciones de instituciones financieras. Ley 8078/90. Código de Protección y defensa del Consumidor.
Bolivia	Artículo 21.2. Las bolivianas y los bolivianos tienen los siguientes derechos: a la privacidad, intimidad, honra, propia imagen y dignidad. Artículo 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida	Código Penal. Modificado por la Ley 1768, de 10 de marzo de 1997 (Artículos 363 Bis y 363 ter). Delitos Informáticos. Ley 28168, de 18 de mayo de 2005. Acceso a la Información del Poder

de conocer, objetar la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa. Artículo 131. I. La acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo ConstitucionalII. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ellos se suspenda la ejecución. IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la Ley.

Ejecutivo (Artículo 19: Petición de Hábeas Data).

Ley 018, de 16 de junio de 2010, del Órgano Electoral Plurinacional. Artículos 72 (obligaciones); 74 (Registro y actualización de datos); 76 (Padrón Electoral); 77 (Lista de habilitados e inhabilitados), y 79 (acceso a información del Padrón Electoral).

Ley 164, de 8 de agosto de 2011, General de comunicaciones, Tecnologías de la Información y Comunicación. Artículos 54 (derechos de los usuarios); 56 (inviolabilidad y secreto de las comunicaciones); 59 (obligaciones de los operadores y proveedores); 84 (reglamentación); 89 (correo electrónico personal); 90 (correo electrónico laboral), y 91 (comunicaciones comerciales publicitarias por correo electrónico o medios electrónicos).

Decreto Supremo 1793, de 13 de noviembre de 2013. Reglamento de la Ley 164. Artículos 3 (definiciones); 4 (principios), 40 (funciones de la Agencia de Registro); 54 (derechos del titular del certificado); 56 (Protección

		de datos personales), y 57 (comunicaciones comerciales publicitarias).
Ecuador	Número 9: Determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución, lo cual implica la obligación estatal de adecuar formal y materialmente, las leyes y normas de inferior jerarquía a la Constitución y los instrumentos internacionales, e implementar las normas que sean necesarias para garantizar la dignidad del ser humano. Artículo 66. Número 19: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. Número 20: El derecho a la intimidad personal y familiar. Número 21: El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.	Ley 162, de 31 de marzo de 2010, del Sistema Nacional de Registro de Datos Públicos. Ley 13, de 18 de octubre de 2005, de Burós de Información Crediticia (arts. 5 a 10). Ley 67, de 17 de abril de 2002 de Comercio Electrónico, Firmas y Mensajes de Datos (Artículo 9). Ley Orgánica de Transparencia y Acceso a la Información Pública, de 18 de mayo de 2004. Ley 184, de 10 de agosto de 1992 Especial de Telecomunicaciones (Arts. 1, 14 y 39). Ley 13, de 18 de octubre de 2005. Burós de Información Crediticia (Arts. 5 a 10). Ley Orgánica de Transparencia y Acceso a la Información (LOTAIP), de 18 de mayo de 2004.

República de El Salvador	Artículo 2. Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.	Decreto 534, de 30 de marzo de 2011. Ley de Acceso a la Información Pública (en especial, su Título III, dedicado a la Protección de Datos Personales). Decreto 136, de 1 de septiembre de 2012. Reglamento de la Ley de Acceso a la Información Pública. Decreto Legislativo 695, de 27 de julio de 2011. Ley de regulación de los Servicios de Información sobre el Historial de Crédito de las Personas. Decreto Legislativo 166, de 8 de septiembre de 2005. Ley Protección al Consumidor. Decreto Legislativo 142, de 6 de noviembre de 1997 (Reformada oct. 2008). Ley Telecomunicaciones y Energía. Decreto Legislativo 1030, de 26 de abril de 1997. Código Penal. Delitos relativos a la intimidad. Ha sufrido diversas reformas parciales, la última en diciembre de 2013. Reglamento General de Ley Penitenciaria. Establece algunas disposiciones sobre privacidad de datos del interno.

Guatemala

Artículo 24. Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Artículo 30. - Publicidad de los actos administrativos.

Artículo 31. Acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos.

Ley de Acceso a la Información Pública (en especial, el art. 9). Decreto 57-2008 del Congreso de la República.

Ley de Protección al Consumidor y Usuario. Decreto 006-2003 del Congreso de la República.

Ley para el reconocimiento de las Comunicaciones y Firmas Electrónicas.

Decreto 47-2008 del Congreso de la República.

Código Penal. Decreto 17-73 del Congreso de la República. En el artículo 274, inciso D) se establece como un delito informático la creación de registros prohibidos, regulando que se impondrá prisión de 6 meses a 4 años y multa de Q.200 a Q.1,000, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Ley de Derecho de Autor y Derechos Conexos. Decreto 33-98 del Congreso de la República.

Honduras	Artículo 76. - Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.	Ley de Transparencia y Acceso a la Información Pública. Decreto 170-2006.
	Decreto Legislativo 381-2005. Se reformó el Capítulo I, del Título IV de la Constitución de la República, donde el Estado de Honduras reconoce la garantía del HABEAS DATA: Que toda persona tiene el derecho a acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y /o enmendarla.	Artículo 23: HÁBEAS DATA Artículo 24: Sistematización archivos personales y su acceso. Artículo 25: Prohibición entrega de información.
Panamá	Artículo 29. La correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales. […] se guardará reserva sobre los asuntos ajenos al objeto de la ocupación o del examen. Igualmente, las comunicaciones telefónicas privadas son inviolables y no podrán ser interceptadas.	Ley 6 del 22 de enero de 2002, Transparencia y Acceso Información Pública. Establece acción de Habeas Data (Artículos 3, 13 y 17). Ley 24 del 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito (Artículos 23 y 30).
	Artículo 42 a 44. Derecho Acceso de Información y Habeas Data.	Ley 3 del 5 de enero de 2000, Ley General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida (Artículos 34 y 37).

Paraguay

Artículo 33 - Del Derecho a la Intimidad. La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

Artículo 135 - Del Hábeas Data. Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

Ley 3440, de 16 de julio de 2008, que modifica varias disposiciones de la Ley 1160/97, Código Penal.

Ley 4439, de 3 de octubre de 2011, que modifica y amplia varias artículos de la

Ley 1160/97, Código Penal. Artículos 146 b; 146 c; 146 d; 174; 174 b; 175; 175 b y 188.

Ley 1682, de 16 de enero de 2001, que reglamenta la información de carácter privado.

Ley 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley 1682. Ley 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley 1682.

Ley 4017, de 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico.

Ley 4610/2012, que modifica y amplía la Ley 4017/10.

		Decreto Nº 7369, de 23 de septiembre de 2011, por el que se aprueba el Reglamento de la Ley Nº 4017/10. Ley 4868, de 26 de febrero de 2013, de Comercio electrónico. Decreto 1165, de 27 de enero de 2014, por el que se aprueba el Reglamento de la Ley 4868, de Comercio electrónico. Ley 4989, de 9 de agosto de 2013, que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATIC).
Venezuela	Artículo 28. Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados […] conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas […].	Ley de registro de antecedentes penales del 3 de agosto de 1979 (Artículos del 6 al 8). Ley sobre Protección a la Privacidad de las Comunicaciones del 16 de diciembre de 1991. Ley Orgánica para la Protección del Niño y del Adolescente del 10 de febrero de 1998 (Artículos 65 al 68).

	Artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática. Artículo 281. Son atribuciones del Defensor o Defensora del Pueblo: 3. Interponer las acciones de inconstitucionalidad, amparo, habeas corpus, habeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los ordinales anteriores, cuando fuere procedente de conformidad con la ley.	Ley Especial contra Delitos Informáticos del 30 de octubre de 2001 (Artículos 20 al 30).

que dicho consejo estará asistido por un Consejo Consultivo integrado por 5 miembros[21].

Como puede observarse, la situación en la que se encuentra el ordenamiento jurídico en el sistema iberoamericano resulta contradictoria, puesto que en la mayoría de los países existe un reconocimiento de carácter fundamental del derecho a la protección de datos personales y un marco jurídico que establece los mínimos para su desarrollo, por lo tanto, a nuestro parecer, hasta el momento resulta insuficiente, situación que ha generado que el nivel de protección de los datos personales no sea el adecuado, de acuerdo con los estándares internacionales, específicamente nos referimos a la Directiva 95/46/CE.

El hecho de que la mayoría de los países de Iberoamérica no cuenten con un nivel adecuado de protección genera una consecuencia específica que se refiere a la imposibilidad de que se puedan realizar transferencias de datos personales desde el ámbito europeo, salvo que se cuente con una autorización especial; en este sentido, resalta la legislación de Argentina, Uruguay y Andorra, las cuales se considera que cuentan con un nivel adecuado de protección de acuerdo con los estándares internacionales, por lo que cabe resaltar que cuentan con una legislación específica aplicable al sector público y privado y existe una autoridad de control.

De otra parte, podemos resaltar el caso de México en donde la normativa de protección de datos se ha realizado de manera sectorial; decimos que es sectorial porque hasta el momento se han regulado los datos personales por categorías o por sectores; es decir, se cuenta con una ley que regula la protección de datos en el sector privado y otra en el sector público, en materia de transparencia y acceso a la información; así también se ha sectorizado en función

21. Artículos 3 y 31 de la Ley 18.331, de 11 de noviembre de 2008.

de las competencias y atribuciones entre dos niveles de gobierno: el Federal y el Estatal, es decir, existen entidades federativas que cuentan con leyes en materia de protección de datos aplicables al sector público y otras no, por lo que existe una diferencia a nivel nacional respecto a los principios, derechos y, en general, a la regulación en la materia, a diferencia de los países que cuentan con legislación específica en la materia, ya que estos mediante una sola ley regulan los dos sectores, el público y el privado.

Así también destacan otros países con legislación sectorial, es decir que no cuentan con una ley específica en la materia, y que contienen ciertas disposiciones que regulan la protección de datos en otras legislaciones, como es el caso de Brasil, Honduras y Guatemala, entre otras.

Asimismo, otro aspecto importante que debe tomarse en cuenta respecto a la legislación en materia de protección de datos en Iberoamérica es la existencia de autoridades de control independientes encargadas de garantizar a las personas su derecho fundamental, toda vez que en diversos países dichas autoridades no gozan de autonomía plena e independencia en sus decisiones, pues pertenecen a dependencias específicas del Gobierno, y esto adquiere relevancia porque la intervención de las autoridades de control es un elemento primordial para el "sello de protección de datos", si tomamos en cuenta que se tiene previsto en el modelo europeo que el sello podrá ser obtenido tanto por responsables como por encargados del tratamiento de datos, y que podrán solicitar la certificación ante "cualquier autoridad de control de la Unión", siendo este sello un elemento que considera la transferencia internacional de datos con garantías a tenor del futuro Reglamento General de Protección de Datos.

Aunado a lo anterior, en la Directiva 95/46 también se hace referencia a la independencia de las autoridades de control al establecer en su artículo 28: "Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia".

Finalmente, consideramos que para que se pueda dar una protección efectiva de los datos personales en Iberoamérica y, por consiguiente, el sello de protección de datos se implemente de una manera adecuada, es preciso que se replantee la legislación en la materia, por lo que se considera que se debe adoptar el modelo europeo; de esa manera se evitarían vacíos legales, se contaría con un esquema de protección adecuado a nivel internacional, y se tendría en Iberoamérica uniformidad legislativa, lo que facilitaría la certificación, puesto que es necesario que en principio las legislaciones en los países de Iberoamérica garanticen un nivel adecuado de protección.

El sello de protección de datos como una buena praxis de Privacy by Design

Relacionar la obtención y la conservación de un sello de protección de datos con la Privacidad por Diseño (Privacy by Design) requiere del conocimiento e "interiorización" de este concepto, por parte de cualquier responsable interesado en la distinción.
Los orígenes de la Privacidad por Diseño (en adelante PbD, por sus siglas en inglés) se remontan a los años 90[22], y pasan necesariamente por la identificación y aplicación de siete principios[23], cuyo cumplimiento permitiría, por un lado, que los ciudadanos vean asegurado el control de su información personal y, por el otro, que las organizaciones obtengan una ventaja competitiva.

La adopción de PbD requiere de modificaciones en las políticas y procedimientos de los responsables, que algunos pueden calificar como un verdadero cambio de filosofía corporativa, puesto que la protección de la privacidad no deriva en exclusiva del cumplimiento de la normativa sobre la materia, sino que pasa a convertirse en un modo de operación predeterminado en la organización, en el que el respeto a la privacidad se constituye como una práctica natural del responsable, y así se refleja tanto en el exterior como el interior de la entidad.
Para adquirir y mantener un nivel de protección como el que persigue el modelo de PbD, es necesario conocer los siete principios antes aludidos, con un punto de vista práctico:

1. Los responsables deben ser proactivos y preventivos, en oposición a reactivos y correctivos. La organización que ostenta un "sello de protección de datos" no espera a que los incidentes sucedan para corregirlos; analiza, valora y adopta medidas preventivas que pueden evitar infracciones a la organización, pero sobre todo, que disminuyen riesgos para la privacidad de los titulares de los datos personales.

2. La privacidad debe existir "por defecto" (privacy by default), no debe tratarse de un elemento optativo o adicional a los sistemas de información del responsable o a sus prácticas de negocio, de tal forma que no es necesario elegir entre opciones con menor o mayor grado de protección a la privacidad, dado que ésta ha sido considerada desde que el sistema, el servicio o la práctica del negocio fueron concebidos.

3. La privacidad deberá estar integrada en el diseño y arquitectura de los sistemas de tecnologías de la información y en las prácticas del negocio del responsable, de forma que ésta se constituya como un elemento esencial de la funcionalidad de unos u otros.

22. Ver, por ejemplo, la información disponible la web del Comisionado de la Información y de la Protección de la Privacidad de Ontario.
23. Los siete principios de PbD fueron internacionalmente reconocidos como un estándar en la 32ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos, en el año 2010.

Esta integración permitirá que, posteriormente, no sea necesario corregir o modificar sistemas o prácticas que no integraron la privacidad desde que fueron diseñados.

4. La PbD busca que los intereses de todos los involucrados estén reconciliados, se persigue una funcionalidad total, una suma positiva. En este sentido, en una

   organización compleja, la funcionalidad total podrá alcanzarse si un proyecto, un servicio o un sistema, desde su concepción, cuenta con la participación de todos los interesados para que, en defensa de sus intereses y objetivos legítimos (obtener ganancias, generar reputación, respetar la ley, entre otros) estos puedan ser conciliados para evitar que alguno "pierda" en "beneficio" de otro.

5. Cuando se ha implementado la PbD, se asegura la protección punto-a-punto durante todo el ciclo de vida de los datos. En este estado de organización, un responsable que desea obtener o mantener un sello de protección de datos, garantiza que la obtención, procesamiento, consulta, comunicación, conservación, bloqueo y destrucción de los datos, se realizará con garantías de seguridad desde el inicio y hasta el final del ciclo de vida de cualesquiera datos personales que trate.

6. La visibilidad y la transparencia son inherentes a la PbD, y las tecnologías o prácticas de negocios del responsable pueden ser sujetos a una verificación o revisión independiente, en los que los componentes y operaciones permanecen visibles tanto para los usuarios como para cualquier tipo de proveedor. En la práctica, la tenencia de un sello de protección de datos trae aparejado el acceso expedito a información como las finalidades y tipos de datos que son tratados por el responsable; la existencia de comunicaciones de datos y los derechos que los titulares pueden hacer valer ante dicho responsable, mediante procedimientos igualmente claros y transparentes.

7. Finalmente, debe considerarse que el modelo de PbD mantiene un enfoque centrado en el usuario, en el que el respeto a su privacidad ostenta una posición prioritaria, ofreciendo por medios adecuados la comunicación de incidencias, cambios en la política de privacidad del responsable o la adopción de medidas de seguridad, así como accesos, información y opciones "amigables".

En el contexto de los principios aludidos, un sello de protección de datos no constituye un fin en sí mismo, sino el resultado de prácticas alineadas con aquéllos, que distinguirán al responsable frente a otros que no han incorporado la protección de la privacidad en el diseño de sus servicios y procesos corporativos.

Ventajas de los Sellos de Protección de Datos

Los Sellos de Protección de Datos derivan de los procesos de certificación o autorregulación contemplados en algunas normas de protección de datos personales, siendo este sello parte del proceso de certificación.

Dicha certificación se puede ver como un proceso que equilibra los vacíos existentes entre las normas de protección de datos que tienen carácter obligatorio y los instrumentos de autorregulación. Sobre todo, porque estos últimos ofrecen flexibilidad para que los responsables y encargados del tratamiento puedan establecer modelos o esquemas de protección adecuados a su modelo de negocio, modelos que pueden establecerse incluso desde el diseño del producto o servicio.

Una de las formas para impulsar la autorregulación y el cumplimiento normativo en la materia es reconociendo el esfuerzo, costos e interés que los responsables y encargados del tratamiento invierten al implementar las medidas necesarias para garantizar la protección de los datos personales que manejen, reconocimiento que se realiza mediante la Certificación de Protección de Datos Personales, la cual sirve además como estímulo para que los responsables o encargados se adhieran a la misma.

Además del incentivo de tener una certificación que indique que se cumple con las obligaciones sobre protección de datos, tal certificación ayuda a los responsables del tratamiento a posicionarse en el mercado y ante sus clientes, ya la misma se convierte en una garantía de seguridad y confianza ante los usuarios y, en un instrumento que les permite diferenciarse de otros productos o servicios similares en el mercado, con lo que se favorece y robustece la marca y los productos asociados a la misma.

Para que los usuarios o titulares de los datos personales puedan conocer cuáles proveedores establecen medidas, procesos y estándares de seguridad adecuados para la protección de sus datos, es conveniente que mediante el principio de transparencia se les dé a conocer de manera estándar quiénes cumplen con tales medidas, para ello es que existe la Certificación de Datos Personales, lo cual no solo es importante desde el punto de vista de transparencia, sino que ayuda a romper con el problema de asimetría de información que generalmente existe entre los proveedores y los titulares de los datos personales, ya que estos últimos en diversas ocasiones no logran entender o conocer todos los alcances y usos que el responsable realiza con sus datos personales.

Si la identificación de la Certificación de Datos Personales por parte de su titular es rápida y sencilla, se facilitará el entendimiento y conocimiento por parte de este último respecto de quiénes garantizarán la protección de sus datos personales. Lo anterior se cumplirá con la emisión del Sello de Protección de Datos Personales, ya que visualmente ayudará al usuario

a identificar rápidamente quién cuenta o no con la certificación. Y en caso de que quieran entrar en más detalles respecto del sello o simplemente revisar si el mismo efectivamente fue otorgado, los titulares podrán consultar si el mismo es válido y/o vigente en los Registros o Bases de Datos Públicas que al efecto se publiquen por la Autoridad Reguladora o por los terceros certificadores.

A su vez, el Sello de Protección de Datos Personales podrá ser utilizado por los responsables como un instrumento para promocionar sus productos o servicios, permitiéndole diferenciarse de otros como un elemento adicional de calidad.
Promoción de negocios ayudará a facilitar los negocios no solo a nivel local, sino también internacional cuando sean solicitados productos o servicios para otro país, ya que se incrementa la confianza en la transacción.

Finalmente, como se viene recogiendo a lo largo de la presente Declaración, la obtención del sello implica, a tenor del futuro Reglamento General de Protección de Datos, que las transferencias internacionales de datos realizadas a al amparo de una certificación gozan de la calificación de realizadas con garantías suficientes, lo que redundará en una mejora de la fluidez y seguridad jurídica de las operaciones comerciales.

Como se ha analizado, los sellos suponen varias ventajas y facilitan el comercio de productos y servicios a nivel local o a nivel Unión Europea, según se trate. Sin embargo, para facilitar el comercio internacional sería conveniente contar con un sello que fuera reconocido en los países iberoamericanos. Sobre todo, aprovechando el hecho de la similitud que existe entre los principios y normas de Protección de Datos Personales de los países iberoamericanos, ya que en su mayoría han tomado como base o ejemplo la legislación europea en la materia.

Si bien es cierto que se requiere una reforma en las legislaciones de protección de datos de estos países y/o la creación de un organismo internacional que pueda emitir certificaciones y, por lo tanto, sellos que permitan un libre flujo de datos personales entre titulares y responsables, la misma se puede lograr. Sobre todo, pensando en el beneficio que implicaría para el comercio internacional entre los países de Iberoamérica, así como el beneficio que traería para los titulares de datos el conocer de una manera fácil y rápida quién tiene el sello y, además, teniendo la posibilidad de corroborar su veracidad y vigencia en un Registro Iberoamericano en donde se encuentre información pública respecto de estos sellos y sus titulares.

La protección de datos como indicador de calidad

Tenemos que entender que la sociedad evoluciona de una manera vertiginosa hacia sistemas de exigencia y garantía mayores, por lo que hoy en día las empresas y otras personas jurídicas deben pensar en un modelo de gestión diferente y, por ende, del tratamiento de los datos personales que se manejan.

Uno de los principales problemas en la sociedad de la información es la falta de confianza en los productos y servicios tecnológicos. Los ciudadanos, e incluso, los propios empresarios, demandan una mayor protección de su privacidad cuando utilizan estos productos y servicios.

En la actualidad es necesaria una mayor transparencia a la hora de conocer las garantías que respecto a la privacidad ofrecen los anteriormente citados productos y servicios tecnológicos.

La necesidad de implementar una política de privacidad de datos por medio del Sello Iberoamericano no debe tratarse de un imperativo legal únicamente, sino que también debemos entenderlo como un KPI (Key Performances Indicators) o indicador necesario de calidad.

Los indicadores de calidad son medidas estadísticas basadas en cifras o ratios que se utilizan como criterio para juzgar y evaluar el desempeño de una organización, un sistema o un proceso.

La satisfacción del cliente y la generación de su confianza es uno de los principales indicadores de la calidad de un servicio en base a la relación entre percepciones y expectativas esperadas acerca de su privacidad y el tratamiento que se dará a sus datos personales.

Por medio del sello se podrá establecer un procedimiento de certificación de aquellos productos y servicios tecnológicos que cumplan con la legislación de privacidad, protección de datos y seguridad. Por tanto, la adaptación a los parámetros de protección de datos, además de crear confianza, supone también un fundamental argumento de valor competitivo a nivel empresarial, ya que en palabras de Javier Hernando "la información y los sistemas informáticos que la soportan conforman un activo importante en cualquier organización, que contribuye a garantizar su funcionamiento y continuidad".

Toda empresa debe enfocar su estrategia orientándola al cliente, entendiendo sus expectativas y respetando su privacidad, ya que los datos que manejamos les identifican de alguna manera.

El hecho de que una empresa no los proteja hace que el usuario pierda la confianza y vea vulnerada su privacidad. Así por ejemplo, el cliente puede ver vulnerada su privacidad si no controlamos las "fugas de información", el phishing o aquellos incidentes que ponen en poder de una persona ajena a la organización, información confidencial y que solo debería estar disponible para integrantes de la misma.

Por ello, el Sello Iberoamericano en Protección de Datos es imprescindible para poder calificar la excelencia empresarial, en cuanto a que por medio de él:

- Se transmite a la sociedad que se posee las capacidades técnicas y funcionales para la excelente prestación de nuestros servicios, así como los procedimientos internos que aseguran su adecuada prestación.

- Aumenta la satisfacción y la confianza de los usuarios, ya que implicará que la empresa tiene un sistema de gestión que incorpora las buenas prácticas y la transparencia.

En este mismo sentido, Daniel López Carballo afirmaba en su artículo para el CGAE:

> (…) correcta adecuación (…) conlleva una serie de beneficios para las empresas, tanto en el ámbito de la responsabilidad en el tratamiento de los datos como en la trazabilidad de la información y la correcta asignación de recursos para lograr un seguimiento adecuado. Mayor seguridad implica confianza, limita riesgos y, por tanto, genera beneficios.
>
> Este planteamiento en positivo y el entendimiento de que dichas acciones no son un trabajo baldío, muestra una concepción de la normativa de protección de datos como motor de negocio, generador de beneficios y de confianza, en definitiva, como un activo empresarial.

El tratamiento de los datos personales implica hacer una apuesta por la ética empresarial, en cuanto a la cultura de la organización en su conjunto para que el proyecto perdure en el largo plazo. Por este motivo, el sello permite evaluar el nivel de protección de datos que ofrecen los responsables y los encargados del tratamiento de las empresas como un indicador de calidad y seguridad para el cliente.

El objetivo principal del Sello Iberoamericano es crear confianza, lo que supondrá una mejora de la imagen corporativa y una mayor garantía para los afectados en lo que se refiere al tratamiento de sus datos personales. En definitiva, dotar a la organización de parámetros de calidad y excelencia.

Mantenimiento del Sello. Auditoría y renovación

El Sello Iberoamericano de Protección de Datos se propone como un mecanismo voluntario de certificación o marca de protección de datos, que permitirá a los interesados reconocer rápidamente el nivel de protección de datos que ofrecen los responsables y encargados del tratamiento sobre sus productos y servicios y otorgar la categoría de transferencia internacional con garantías a aquellas entidades adheridas. Hoy en día los flujos de información transfronterizos plantean retos relacionados con Internet y mayores riesgos de menoscabar la privacidad de las personas. El sello permite, por tanto, evaluar rápidamente los niveles de protección que se consideran adecuados.

El mantenimiento del sello de protección de datos debe establecerse como prioridad por parte de las empresas, ya que como toda certificación debe ser renovada y puede ser revocada. El

cumplimiento de la normativa de protección de datos en lo que respecta al tratamiento de datos personales en los distintos sistemas de información, no dependerá solo de la evaluación que se realice en un momento inicial, sino también de las acciones previstas para que el grado de cumplimiento perdure a lo largo del tiempo.

A este respecto, resulta necesario el establecimiento de mecanismos que consigan la confianza necesaria para el resto de los operadores del mercado y, en particular, en lo relacionado con las operaciones comerciales que impliquen el tratamiento de bases de datos de carácter personal. Este Sello Iberoamericano de Protección de Datos se constituye así como elemento fundamental y su mantenimiento aporta un valor añadido a la seguridad jurídica, no solo entre empresas iberoamericanas sino también a las relaciones de éstas con las empresas europeas.

Auditoría

A fin de mantener y renovar el sello, cobra especial relevancia la realización de una auditoría y/o adecuación de los nuevos sistemas de información que en una empresa se implanten y que supongan un tratamiento de datos de carácter personal. La auditoría del sello responde a una revisión de la organización en cuanto a detectar si se cumple con todas las medidas que se consideraron para la entrega y mantención del Sello Iberoamericano de protección de datos.

¿En qué consiste?

Es una inspección de las medidas que se implantaron en el momento de concesión del sello y aquellas mejoras que se consideraron como vinculantes de manera de corregir prácticas o implementar otras nuevas. También se analiza en el momento en que se realiza si se han producido cambios en la organización, tanto de sistemas, procesos, seguridad, que requieran mejoras relacionadas con la implementación del sello.

Como toda auditoría, esta debe hacerse por personal profesional debidamente cualificado, independiente, imparcial y objetivo. La independencia tiene relación con la actividad de tratamiento, es decir, no puede hacerse por el responsable del tratamiento o de seguridad o el encargado. La auditoría del sello es una oportunidad para las organizaciones de generar y mantener confianza y promover buenas prácticas en la relación con usuarios y/o clientes.

Renovación

Como parte fundamental para mantenimiento del sello y en consonancia con el nuevo Reglamento Europeo de Protección de Datos, éste deberá ser renovado cada cinco años en las mismas condiciones y, para ello, el responsable o encargado del tratamiento deberá realizar la correspondiente auditoría orientada a su renovación, teniendo en consideración lo anteriormente expuesto.

Por último, en lo que se refiere al agente interviniente en la certificación, sobra decir que los organismos de certificación debidamente acreditados deberán tener entre sus funciones no solo la expedición de la certificación, sino también la revisión periódica y la retirada de sellos y marcados de protección de datos.

Certificaciones y Sellos de Protección de Datos: el papel de las Autoridades de control

Los "sellos de protección de datos" como instrumentos eficaces y confiables para un escenario global.

En los entornos digitales donde las fronteras pierden cada vez más relevancia, y se apuesta por la creación de un mercado digital único; la confianza de los consumidores es un elemento esencial para su despliegue. Hoy, los productos y servicios tecnológicos desafían con mayor intensidad los límites de la privacidad, haciendo que los usuarios, y hasta los mismos empresarios, hagan mayores demandas para proteger su privacidad.

Desde inicios de 2012, la Comisión Europea propuso regular certificaciones relacionadas con el nivel de protección de los datos personales ofrecido por los responsables y encargados del tratamiento, invitando a la creación de mecanismos para la certificación en materia de protección de datos y de sellos que permitan a los interesados evaluar rápidamente el nivel de protección que ofrecen los responsables y los encargados de los tratamientos[24].

La finalidad de dicha propuesta radicaba en crear un signo distintivo como mecanismo de confianza para que las personas afectadas por los tratamientos de sus datos personales puedan valorar, cuando se exhiba este distintivo, que sus datos están siendo objeto de un tratamiento legítimo y respetuoso de las normas que defienden la privacidad. En este sentido se busca crear un modelo de certificación que cumpla con la normativa de protección de datos personales. En la versión final del texto de compromiso alcanzado, incluso, se otorga la consideración de transferencia internacional de datos con garantías a aquellas que se realicen bajo el paraguas de una certificación.

Para tales fines, es indispensable que los mecanismos de obtención de este "sello" sean eficaces y, por tanto, que no se defrauden las expectativas de confianza que lógicamente debe generar un instrumento de esta naturaleza.

24. En esta misma línea, el Parlamento Europeo, en sus enmiendas a la propuesta de reglamento de la Comisión Europea, aprobadas en marzo de 2015, entraba con más detalle en esas "certificaciones", al hacer una referencia concreta al Sello Europeo de Protección de Datos".

Definición de las condiciones para la acreditación y certificación

La experiencia europea ha puesto de manifiesto el importante rol de las Autoridades de Control, las cuales se han constituido como una verdadera garantía institucional de la protección de ese derecho y a través de las cuales se desarrolla el núcleo de la efectiva protección de los individuos, en relación al tratamiento de los datos personales.

Este papel debe mantenerse y potenciarse en relación a la propuesta de una certificación o sello sobre el cumplimiento de la normativa de protección de datos personales, que a la vez deba ser considerada como un modelo de aplicación global, respetando las particularidades de cada ordenamiento.
Para la concreción de estos fines, deberá considerarse también que la obtención de este sello

sea voluntaria; y que conectada con el régimen sancionador que se prevé, su obtención suponga algunas ventajas adicionales; ya que si se dispone del mencionado "sello", por ejemplo, la sanción económica por incumplimiento de las obligaciones previstas en la normativa de protección de datos podrá reducirse.

Los elementos esenciales de cualquier esquema de certificación implican, en primer lugar, garantizar la independencia e imparcialidad en la evaluación de los tratamientos de datos personales de conformidad con los principios, obligaciones y derechos que pueda prever el marco jurídico y de autorregulación aplicable a responsables y encargados de los tratamientos sometidos a evaluación. Esta independencia e imparcialidad deberá alcanzar, no solo a los organismos certificadores como tales, sino también a los profesionales acreditados a su servicio, que deberán estar suficientemente cualificados y libres de conflictos de intereses.

Las instituciones europeas hacen referencia a la existencia de organismos o entidades certificadoras específicas que expidan la certificación o sello, aunque con la posibilidad de que sean las propias autoridades de control competentes las que puedan llevar a cabo las tareas de certificación.

Tal como en su momento se aceptó en el escenario europeo, la expedición de la certificación deberá ser sobre la base de criterios aprobados directamente por la autoridad de control competente, o en su caso, por el Consejo Europeo de Protección de Datos, institución creada por la propuesta de Reglamento, como evolución del actual grupo del artículo 29. En cualquier caso, el organismo de certificación deberá estar acreditado en cuanto a su capacidad y pericia en materia del derecho a la protección de los datos de carácter personal, específicamente, respecto de la regulación que sea aplicable al responsable o encargado de tratamiento, y a los propios tratamientos. En caso que la autoridad de control decida llevar a cabo la función de organismo certificador, esa capacidad y pericia estaría acreditada por las competencias y funciones que le atribuye el ordenamiento jurídico.

En el supuesto de que se opte por un modelo donde la verificación de los requisitos para obtener el sello sea llevada a cabo por otras entidades, sean públicas o privadas, la autoridad de control debería adoptar el papel de organismo de acreditación; es decir, determinará las condiciones y requisitos para que efectivamente ese organismo certificador pueda valorar la adecuación de los tratamientos y, en consecuencia, pueda informar favorablemente respecto de la expedición del sello. En todo caso, esta última función debería estar reservada a las autoridades de control, una vez recibidos los informes pertinentes, elaborados en base a los criterios de verificación establecidos por la autoridad de control competente.

En este sentido, la definición de las condiciones de las entidades certificadoras, y de los profesionales a su servicio que lleven a cabo las tareas de verificación, deberán ser elaboradas y aprobadas por la autoridad de control competente, manteniendo en todo caso un adecuado nivel de neutralidad, especialmente en los aspectos tecnológicos.

Esta reserva en la función de expedición del sello resulta de especial relevancia en el caso del Reglamento Europeo, si tenemos en cuenta que entre las propuestas de las instituciones europeas se encuentra la posibilidad de que estar en posesión del sello de protección de datos llegue a impedir la imposición de una sanción económica, siempre que no se trate de un incumplimiento intencionado o negligente o, en otro orden de cuestiones, que se facilite la transferencia internacional de datos, considerando el sello otorgado a un responsable o encargado de tratamiento como una garantía apropiada para llevar a cabo la exportación de datos personales.

Entre esas condiciones deberían concretarse tanto los supuestos de retirada y mantenimiento del sello, como de renovación y revocación de la acreditación, funciones que deberían llevarse a cabo directamente por la autoridad de control competente. Consecuentemente, el conjunto de condiciones y requisitos relacionados con las certificaciones y acreditaciones deberán ser hechos públicos, y actualizados, por las autoridades de control.

En los territorios donde exista más de una autoridad de control, sin modificar las respectivas competencias, sería aconsejable que las diferentes autoridades de control establecieran un marco común de certificación y acreditación.

Consideraciones finales, un especial llamado para los países de América Latina

Uno de los principales desafíos que enfrenta la implementación de certificaciones de esta naturaleza con el alcance global que se pretende, radica en la uniformidad de legislaciones e independencia formal de las autoridades de control que existe en Latinoamérica. A modo de ejemplo, se puede citar el caso de Colombia y Perú, países de los cuales, si bien se puede predicar la imparcialidad de su gestión, estructuralmente dependen de otros organismos estatales.

América Latina inició hace algunos años el desarrollo del camino de la protección de datos personales, y aunque con pasos significativos, su progreso todavía es inicial. Por tanto, reconociendo la importancia de estas certificaciones y el alcance global que se busca alcanzar; es necesario tomar conciencia de las condiciones para la acreditación y certificación respecto de los tratamientos de los datos personales, e implementar las modificaciones estructurales y legislativas que sean necesarias.

Hoy se apuesta por la implementación de certificaciones y sellos que permitan adecuarse a los actuales mercados digitales en los que el derecho a la protección de datos personales quede garantizado en términos de eficiencia y eficacia; pero para ello será necesario que, desde la posición en la que nos encontremos, especialmente desde las Autoridades de Control, se desarrollen las acciones que se requieran para tales fines.

Autoridad de expedición. Consultores acreditados para auditar en nombre de la autoridad

Cada país deberá crear una autoridad de expedición de certificados, la cual a su vez capacitará consultores para auditar en nombre de la autoridad las bases de datos de usuarios para cada país, donde ante todo se vigilará que:

1. Se respeten los principios de información, transparencia y consentimiento.

2. Los responsables del tratamiento estén debidamente identificados.

3. Se respete el principio de calidad de los datos.

4. Cada administrador de datos tenga su propio esquema de seguridad.

5. Se realizan auditorías y revisiones periódicas.

6. Se garanticen los derechos de los afectados.

Por su parte, los consultores deberán acreditar conocimientos de experto en protección de datos tanto a nivel teórico como de práctica profesional. Una vez capacitados, deberán renovarla periódicamente.

Por ello, se plantea que la autoridad de cada país debe expedir unos certificados por medio de consultores. La autoridad de emisión del sello de protección de datos personales debe ser una autoridad establecida por los países miembros, que pueda avalar estándares técnicos y jurídicos de certificación, que pueden ser llamadas a emitir este tipo de certificaciones, ya que serán entidades reguladas y vigiladas. En el caso iberoamericano, son los países miembros

quienes deben designar una entidad de emisión nacional o en conjunto para estos temas, donde el Consejo Europeo de Protección de Datos, una vez homologado, las incluirá en un registro público creado para tal efecto por el Reglamento General de Protección de Datos, que permitirá conocer tanto los certificados válidos como aquellos que hayan sido inválidos, en este caso, referentes a cada Estado miembro.

La coordinación entre Estados se hace fundamental, puesto que el Consejo Europeo de Protección de Datos deberá reconocer a las autoridades nacionales de expedición de los países iberoamericanos y homologar su procedimiento de homologación de consultores.

Reconocimiento mutuo entre países iberoamericanos y firma de acuerdos de convalidación con la Unión Europea y terceros Estados

La implementación del Sello Europeo de Protección de Datos tendría su ámbito de aplicación a todas las empresas y entidades ubicadas en América Latina, con la finalidad de ser reconocidos por los países de la Unión Europea como destinos que garantizan transferencias internacionales con garantías suficientes. En este sentido, el sello puede constituir una herramienta más para facilitar las transferencias internacionales de datos.

A pesar de que algunos países como Argentina y Uruguay ya fueron reconocidos mediante decisiones de la Comisión Europea como países que ofrecían una protección adecuada conforme la Directiva 95/46/UE (Decisión 2003/490/CE, 30 junio y Decisión 2012/484/UE, de 21 agosto respectivamente), a la vista de los cambios que hay previstos en el nuevo Reglamento de Protección de Datos y de la sentencia del Tribunal de Justicia de la Unión Europea invalidando el acuerdo de Safe Harbor con Estados Unidos, es posible que este reconocimiento necesite ser nuevamente evaluado. Por esta razón, el sello puede servir a estos países para facilitarles otras herramientas e igualmente dotar al resto de países de Latinoamérica de un mecanismo que ofrezca cierta uniformidad para facilitar el intercambio de datos con Europa y con el resto de países latinoamericanos.

Para la correcta efectividad del sello, resulta imprescindible que en cada país se cuente, por un lado, con una estructura mínima que permita la ejecución de las medidas y garantías que ofrece el sello y, por otra, se ha de poder garantizar la tutela de los derechos de los afectados.

En cuanto a la estructura, conviene que cada país latinoamericano cuente con una autoridad independiente dotada de facultades suficientes de control, investigación y ejecución, con potestades sancionadoras. Estas autoridades de control pueden ser clave en la cooperación con las autoridades de protección de datos europeas y también para facilitar el ejercicio de derechos de los ciudadanos.

A pesar de que la Decisión 2000/520 de la Comisión Europea que permitía el intercambio de datos con empresas Americanas adheridas al programa Safe Harbor ha sido declarado inválido recientemente por sentencia del Tribunal de Justicia de la UE de 6 octubre 2015, y sin perjuicio de que resurja con nuevas garantías, hay que tener en cuenta que algunos de los aspectos que lo configuraban eran realmente funcionales.

Por ejemplo, la publicación del listado de empresas adheridas al programa, que era accesible a través de la página web del Departamento de Comercio de EEUU, siendo necesario validarlo anualmente. Requisito que igualmente podría aplicarse al Sello Europeo de Protección de Datos; también el hecho de que las empresas adheridas debían hacer público su compromiso, quedando sometidas a la jurisdicción de la Federal Trade Commission o de otros organismos públicos que garanticen el cumplimiento efectivo de los principios. Es decir que el control se ejercía por autoridades preexistentes, no propiamente autoridades de protección de datos, pero dirigidas a proteger los derechos de los consumidores.

Este punto puede ser interesante, teniendo en cuenta la falta de recursos que existe en algunos países de América Latina, situación que puede dificultar la creación de una institución desde cero dedicada exclusivamente a la protección de datos personales.

Igualmente, y teniendo en cuenta la citada sentencia del Tribunal de Justicia, se ponen de relieve dos aspectos fundamentales a considerar: en primer lugar, el hecho de que para poder valorar el nivel adecuado de protección de un país o de un programa, sello o mecanismo similar, las normas y leyes del país de destino no se pueden ignorar y, en segundo lugar, las autoridades de control europeas han de poder mantener intactas sus facultades de impugnación de dichos mecanismos, si hay razones para pensar que su eficacia se ha visto afectada por algún motivo.

Para poder superar algunos obstáculos referentes a las normas y leyes del país de destino, la utilización de mecanismos como la encriptación de datos en tránsito y en destino pueden ser de gran utilidad en algunos casos, aunque no en todos. Asimismo, el exportador debería ser informado previamente de si el importador ha recibido una solicitud de acceso a los datos por parte de una entidad gubernamental. Además, se ha de poder garantizar que la solicitud de acceso por parte de órganos públicos nunca se va a autorizar si se incumplen los requisitos de legitimidad y proporcionalidad.

En cuanto a la tutela de derechos de los afectados, deberían potenciarse mecanismos que refuercen la seguridad en el sistema, generando conciencia en la importancia del sello. Para ello es necesario impulsar soluciones alternativas a la justicia ordinaria, que complementen y acerquen a los ciudadanos maneras ágiles de proteger sus derechos. El uso de mecanismos de resolución de conflictos en línea, más ágiles o los listados actualizados de empresas que cuentan con la aprobación son ejemplos de estas medidas que favorecerán no solo a los responsables de ficheros, sino también a los titulares de los datos y a las autoridades de control.

Tampoco se pueden ignorar las ventajas que el sello convalidado puede suponer para países comunitarios y extracomunitarios en materia de inversiones y flujo de capitales entre mercados. En momentos en que las garantías ofrecidas por el Safe Harbor son cuestionadas, la creación de sellos debidamente autorizados y controlados periódicamente parece una solución razonable, con la cual las empresas podrían dar a conocer su cumplimiento y mantener sus operaciones sin mayores dificultades.

Sello de Protección de Datos como instrumento eximente de la obtención de autorización previa a transferencia internacional

Las normas que tratan la protección de datos personales por sí solas no protegen a las personas, si es que estas no son puestas en práctica y se cuenta con la implementación de un proceso que garantice la eficacia de estas nomas, para ello distintas legislaciones a nivel internacional han establecido un procedimiento para velar no solo por el cumplimiento de la norma dentro de su competencia territorial sino también asegurar al menos un estándar de protección cuando los datos personales salgan de su territorio.

Así encontramos mecanismos en materia de transferencias internacionales de datos personales que constatan que dicha operación cumpla con los niveles de protección adoptados en el país emisor, constatación que se ha uniformizado y unificado en algunas regiones, como la europea, que brindan un "sello" de protección adecuado a aquellos países que no son miembros de su comunidad, a fin de agilizar y asegurar los flujos transfronterizos.

Dicho sello no es un modelo nuevo, sino que instituciones internacionales como la Unión Europea ha establecido reconocimientos de "nivel adecuado". Para mayor información véase el "Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE"; la OCDE a través de la emisión de "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980)", que suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal; la ONU mediante su Resolución 45/95 de 14 de diciembre de 1990 establece los "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales" para brindar las bases de las garantías mínimas en las legislaciones en la materia. En la experiencia iberoamericana contamos con las "Directrices de Armonización de la Red Iberoamericana" (2007), además de grupos de trabajos como el "Marco de Privacidad" (1999) de APEC. Procesos que deben cumplir un estándar de transparencia en el procedimiento donde el sujeto a evaluar debe estar inscrito y reconocido legalmente en su país de procedencia, brindar la información necesaria al organismo designado para el procedimiento de acreditación; dando cumplimiento de requisitos ya normalizados, lo cual acompañado de un informe al alcance de los miembros será un mecanismo fundamental para hacer transparente la aprobación o rechazo de la autorización.

La emisión de este sello para los flujos transfronterizos entre los países miembros de la región iberoamericana y con países terceros, como manifestación de que el proceso es conforme con las condiciones establemente enumeradas será aquel instrumento que tendría por finalidad acreditar una certificación mediante este sello. De hecho el texto de compromiso del futuro Reglamento General de Protección de datos otorga a los códigos de conducta y a las certificaciones la categoría de transferencias realizadas con garantías adecuadas de protección.

Este sello de calidad será el instrumento oficial eximente de realizar los procesos de adecuaciones que se debería llevar a cabo en cada país iberoamericano y en cada operación de transferencia, que además de significar costos de tiempo en algunos casos también lo es de tasas, asesorías legales y otros económicos, siendo simplificado en un solo proceso, previa evaluación y constatación de las exigencias estipuladas por este sello regional que va respaldar la certificación de cumplimiento.

Instrumento, el sello, que se reviste de un proceso transparente al tener las normas previamente uniformizadas y acordadas entre todos los países miembros y que facilitaría sobre todo las transacciones comerciales en la industria de los datos personales, industria que cuente con un sello y lo muestre como un producto confiable, al estar estandarizado, por todos los involucrados en la emisión y recepción de los datos, e incluso el titular de estos datos personales.

Este sello como eximente para obtención de autorización previa a transferencia internacional en los procesos posteriores a la dación de este certificado debe tener un perfil que asegure esencialmente una calidad internacionalmente aceptada, que como se ha mencionado, resulta de la aplicación de estándares establecidos normativamente de manera oficial, el cual debe cumplir con características que aseguren no solo un sello de calidad sino un lenguaje común para los involucrados, mecanismo indispensable para la resolución de conflictos derivados del proceso de transferencia, valores de calidad básicos para establecer una situación real de seguridad jurídica en el mercado.

Conclusiones

Tras el análisis realizado por los colaboradores de la iniciativa del Observatorio Iberoamericano de Protección de Datos, a modo de conclusiones podemos destacar las siguientes:

- Implementar mecanismos más seguros de certificación en materia de protección de datos permitirá al titular realizar una evaluación rápida en relación al nivel de protección que los encargados del tratamiento de sus datos le están ofreciendo. Facilitará igualmente las transferencias internacionales de datos, puesto que las realizadas bajo su paraguas se entenderán realizadas con suficientes garantías de protección.

- El principal objetivo del Sello Europeo será el de crear confianza entre los interesados, lo que traería consigo una notable mejora en la imagen corporativa de la empresa, así como una garantía mucho más fuerte para los posibles afectados por el inadecuado tratamiento de sus datos personales. Es por esto que lo más importante será brindar calidad y excelencia.

- Lograr llegar a la meta de alcanzar un sello de Protección de Datos supone además asumir un reto desde la ingeniería de Sw, ya que como bien sostiene la doctora Amoroso, hay cuestiones que deben ser asumidas por diseño de las aplicaciones y servicios que se instrumenten, tales como los que realizan los servidores y buscadores, y adicionalmente a ellos, es también incluir requerimientos desde la evaluación de calidad y certificación de soluciones digitales.

- La situación actual del ordenamiento jurídico en Iberoamérica resulta contradictoria, puesto que, si bien gran parte de los países cuentan con un reconocimiento de carácter fundamental del derecho a la protección de datos personales y un marco jurídico que establece los mínimos para su desarrollo, el nivel de protección de los datos personales no es el adecuado de acuerdo con los estándares internacionales.

- Para que se pueda dar una protección efectiva de los datos personales en Iberoamérica y por consiguiente el sello de protección de datos, es necesario que se implemente y replantee de una manera adecuada legislación en la materia, quizás adoptando el modelo europeo que ha venido siendo trabajado durante largo tiempo y que facilitaría la certificación.

- Por otro lado la adopción de PbD trae consigo la necesidad de modificar políticas y procedimientos de los responsables, dado que la protección de la privacidad no deriva en exclusiva del cumplimiento de la normativa sobre la materia, sino que pasa

a convertirse en un modo de operación predeterminado en la organización, en el que el respeto a la privacidad se constituye como una práctica natural del responsable, y así se refleja tanto en el exterior como el interior de la entidad.

- Los Sellos de Protección de Datos derivan de los procesos de certificación o autorregulación contemplados en algunas normas de protección de datos personales, siendo este sello parte del proceso de certificación.

- Es importante destacar que la sociedad evoluciona de una manera vertiginosa hacia sistemas de exigencias y garantías mayores, por lo que hoy en día las empresas y otras personas jurídicas deben pensar en un modelo de gestión diferente, y por ende, del tratamiento de los datos personales que se manejan.

- Al establecer el sello, romperíamos uno de los principales problemas que presenta la sociedad de la información: la falta de confianza en los productos y servicios tecnológicos.

- El Sello Iberoamericano de Protección de Datos, se propone como un mecanismo voluntario de certificación o marca de protección de datos, que permitirá a los interesados reconocer rápidamente el nivel de protección de datos que ofrecen los responsables y encargados del tratamiento sobre sus productos y servicios.

Autores

En la elaboración de las diferentes Declaraciones que se compilan en la presente obra han intervenido diferentes profesionales de reconocido prestigio de quince nacionalidades.

ARGENTINA
Adela Goberna
Agustina Callegari
Analía Aspis
Dolores Dozo
Ernesto Liceda
Ezequiel Passeron
Inés Tornabene
J. León Unger
Javier Raimo
Lucía Fainboim
María Eugenia Cafiero
María Julia Giorgelli
Matilde Martínez
Noemí Olivera
Romina Florencia Cabrera

BOLIVIA
Edgar David Oliva Terán

CHILE
Claudio Magliona
Jessica Matus
Patricia Reyes Olmedo
Pedro Huichalaf Roa
Romina Garrido

COLOMBIA
Alexander García Díaz
Camilo Alfonso Escobar Mora
Heidy Balanta
Iván Darío Marrugo Jiménez
Lainiver Mendoza Munar
Nelson Remolina Angarita

COSTA RICA
Mauricio Paris Cruz

CUBA
Yarina Amoroso Fernández

ECUADOR
Alexander Cuenca Espinosa
Carlos Vera Quintana
Damián Armijo Álvarez
María Paulina Casares Subía

ESPAÑA
Alberto Cuesta Ureña
Alonso Hurtado Bueno
Andrés Blázquez García
Daniel López Carballo
Diego Pérez Gutiérrez
Eduardo Lagarón Martín
Emilio Suñé Llinás
Francisco Ramón González-Calero Manzanares
Javier Sempere Samaniego
Javier Villegas Flores
José Luis Colom Planas
José María Fernández-Varela Villamor
Laura Vivet Tañà
Lorenzo Martínez Rodríguez
Marta Sánchez Valdeón
Noemí Brito Izquierdo
Óscar Costa Román
Ramón Miralles López
Ruth Benito Martín
Sara Molina Pérez-Tomé
Violeta Guerra Ramos

GUATEMALA
José R. Leonett

MÉXICO

Aristeo García González
Dulcemaría Martínez Ruíz
Edgar Tomas Quiñonez Ríos
Federico César Lefranc Weegan
Héctor E. Guzmán Rodríguez
Horacio Gutiérrez Gutiérrez
Joab Andrés Mora
Joel Gómez Treviño
Jorge Moreno Loza
Lilibeth Álvarez
Lorena Higareda Magaña
Olivia Andrea Mendoza Enríquez
Philipe Bienvenue Martin del Campo

PANAMÁ

Lía P. Hernández Pérez
Alberto Martín Hernández

PERÚ

Braddy Leonardo Alave Apaza
Cynthia Téllez Gutiérrez
José Reynaldo López Viera
Milagros Olivos Celis

PORTUGAL

João Ferreira Pinto

REPÚBLICA DOMINICANA

Santa Matilde Reyes Valenzuela

URUGUAY

Matías Jackson

Índice

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

0800 999 3722 | ATENCIÓN AL VECINO AV. BELGRANO 673 | DEFENSORIA.ORG.AR