REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

NÚMERO 2 - agosto, 2017

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

SUMARIO

PRÓLOGO

Cuando aún se escuchan las voces y los ecos de la edición anterior, la Unidad Reguladora y de Control de Datos Personales publica, con gran satisfacción, el segundo número de la Revista Uruguaya de Protección de Datos.

Sin embargo, es importante puntualizar que la revista no es un fin en sí mismo, sino que es un instrumento pensado para alimentar la discusión necesaria de temas relevantes acerca de la protección de datos personales y temas vinculados, como la privacidad y la seguridad.

La revista es la excusa para convocar a expertos nacionales e internacionales a reflexionar sobre una realidad cambiante desde perspectivas distintas, quienes aportan sus conocimientos, experiencias y puntos de vista a fin de compartirlos con la comunidad y enriquecernos.

La realidad es cambiante, pero no por mérito exclusivo de la tecnología; tal sería una visión reduccionista de una situación en la que hay múltiples factores. Si bien el dinamismo tecnológico es uno de ellos, no pueden soslayarse aquellos cambios que operan a nivel de la cultura, la sociedad, la economía y la política y que afectan la ética que nos rige.

La revista es un ámbito público donde abordar estas cuestiones y analizar su impacto en la protección de datos personales.

En la presentación del número inaugural, el Dr. Felipe Rotondo señala la publicación como el principio de un camino. Me permito retomar esa metáfora para destacar la importancia del camino y su sentido, que no es otro que la defensa de la dignidad humana, por mandato constitucional, legal y de conciencia.

Sin más preámbulos y con la satisfacción del reencuentro: ¡buena lectura!

Mag. Federico Monteverde

Presidente

Consejo Ejecutivo – URCDP

DOCTRINA


ROBERTO
BALAGUER


MARCELO
BAUZÁ


ARELI
CANO GUADIANA


ANN
CAVOUKIAN


LAURA
SCHERTEL
MENDES
DANILO
DONEDA


JOHN
EDWARDS


SOPHIE
KWASNY


ÁLVARO
SÁNCHEZ BRAVO

¿CÓMO REGULAMOS LA INTELIGENCIA APLICADA A LOS DATOS?

Hansel y Gretel en el siglo XXI

ROBERTO
BALAGUER

Psicólogo por la Facultad de Psicología de la Universidad de la República. Magister en Educación por la Universidad ORT, Uruguay. Posgraduado en Psicología en la Universidad de Minnesota, Estados Unidos, así como en Psicoterapia Psicoanalítica de Niños y Adolescentes y en Psicoterapia Psicoanalítica de Adultos en Clínica UNO, de Uruguay. Experto en TICS y Discapacidad por Fundación Free/Universidad Católica del Uruguay/Universidad de Córdoba, España. Ex Docente universitario en Facultad de Psicología de la Universidad de la República. Docente universitario en posgrados de Educación – Diploma y Maestría en Orientación Educativa – en la Universidad Católica del Uruguay. Docente universitario en la Maestría en Tecnología Educativa en el Centro de Economía Humana. Consultor en distintas temáticas vinculadas con Tecnología, Educación y juventud. Con veinte años de experiencia en instituciones educativas, se desempeña desde 2008 como Director del Programa Link.spc (TICs y Educación) en St. Patrick's College, de Montevideo.

SUMARIO

RESUMEN

El presente trabajo busca echar luz sobre algunos aspectos vinculados a los jóvenes y el uso constante de las redes, la protección o falta de protección de los datos, la identidad digital y cierta ausencia de consciencia por parte de los jóvenes al respecto de su importancia a futuro. El nuevo contexto de conexión 24/7/365 permite que los datos estén disponibles y sean vendidos por las empresas y posteriormente agrupados en perfiles. Por último, abordamos los riesgos de los usos algorítmicos de esos datos y las implicancias éticas que trae consigo ese uso.

EL CONTEXTO DE HIPERCONEXIÓN JUVENIL

¨Si el servicio es gratis, tus datos son el producto¨

J. Sander

La generación de adultos, hoy padres y profesionales, estaba acostumbrada a existir, por defecto, en dos estados: en desconexión y en privado. Las personas debían moverse físicamente o sino trasladarse o hacer una llamada para establecer contacto entre sí y conectarse. A su vez, debían buscar un medio masivo y acceder a él para poder hacer algo público. No era sencillo lograr esto. Hoy, los jóvenes están conectados con sus grupos de pares, por defecto, lo que, en otros términos, significa que sus vínculos son constantes a través de las redes sociales, salvo en aquellos momentos que se les pide que se desconecten. Esto ocurre generalmente en las instituciones educativas al menos, hasta el nivel secundario. Para los jóvenes, muchas de las experiencias que llevan a cabo con los medios digitales es su forma de estar en contacto entre sí (HarrisInteractive, 2008) y esas experiencias son por defecto, públicas. Así tanto ha cambiado el escenario global de las relaciones en los últimos años. Más allá de lo que nos guste o desagrade, así está el mundo y desde allí deberíamos intentar explicarlo.

Cuando uno observa los datos de conexión a nivel mundial, estos son crecientes. En el ámbito local esto también se repite, por lo que se entiende que no se trata de un fenómeno pasajero, ni de una moda. La hiperconexión ha llegado para quedarse. La alternancia entre el mundo material y el virtual es cada vez más permanente. El perfil del internauta uruguayo que elabora periódicamente el grupo Radar (2016) con su crecimiento de la conexión constante a lo largo de los años, ratifica esa impresión que todos tenemos.

Cuando en jornadas especificas hablamos de la necesidad de generar instancias de desconexión, observamos la creciente influencia del acontecer conectado en la vida de los jóvenes. A medida que disminuye la edad, las horas en línea crecen hasta llegar a la conexión constante en un cuarto de los casos, según nuestras propias cifras (Balaguer, en prensa). En definitiva, se trata de un contexto de hiperconexión que ya vislumbrábamos hace ya varios años atrás (Balaguer y Canoura, 2010).

Estamos insertos en una nueva matriz cultural (Balaguer, 2012) en la cual los datos crecen exponencialmente, especialmente aquellos vinculados a la telefonía celular y los materiales multimedia (música y videos). La cantidad de celulares en el mundo y en el Uruguay según datos de INE (2013) alcanza más del 90% de la población y no hay quintil que quede por fuera de esta realidad. Según el grupo Radar (2016) más de 8 de cada 10 usuarios de internet se conecta desde su móvil. La llegada del Plan Ceibal en Uruguay (Balaguer, 2009) significó un aumento del uso de lo digital y el acortamiento de la brecha digital de acceso.

LOS CELULARES COMO PUERTAS DE ENTRADA Y COMO SALIDA DE DATOS

Debemos entender que los celulares son desde hace mucho tiempo mucho más que teléfonos móviles. Venimos estudiando ya desde hace una década los tipos de vínculos que se establecen con los celulares de forma tal de comprender los fenómenos de hiperconexión tan presentes hoy. En otro lugar hemos delineado al menos cinco tipos distintos de usos de celulares (Balaguer, 2012, 2016). La conexión a través de Internet y los celulares, conforma una suerte de malla omnipresente que penetra cada casa, cada rincón material y que deja a los jóvenes de hoy en un estado de permanente conexión entre pares, o como solemos decir: en conexión, por defecto. La relación con esa malla puede ser llevada a cabo de distintas maneras. Los celulares son usados muchas veces como objetos transicionales (como el trapito o la almohadita del infante) que ayudan a andar por el mundo sintiéndose acompañados y seguros (Balaguer, 2012). Otras veces son utilizados como objetos para modificar el humor o el talante, para escapar de ambiente o para sentirse vivo, entre otros posibles usos en los que no entraremos en detalle aquí, pero que hemos descripto anteriormente (Balaguer, 2012, 2016). Las relaciones que se establecen con los celulares y con la conexión y esos tipos de vínculos se relacionan con los perfiles de personalidad de los usuarios. Si bien la tecnología está diseñada de

forma cada vez más inteligente, los tipos de uso tienen que ver más con el tipo de personalidad del usuario. En este sentido, las dificultades en el control de los impulsos suele estar asociada a un mayor uso y dependencia de los aparatos (Wilmer, 2016).

Por eso es importante conocer cómo se sienten sin el celular chicas y varones. Lo viven de distinta manera según el género también. El tipo de vínculo con sus dispositivos es diferente. De hecho, la desconexión para uno y otro género también es diferente (Balaguer, en prensa).

Hay que comprender que el drama juvenil de gestionar y negociar la identidad se ha trasladado al mundo virtual. En ese contexto de redes sociales "amigos, *followers, selfies*, Me Gusta, fueguitos y RT" son las monedas de cambio corrientes. No es sencillo para los jóvenes la socialización a través de las redes ya que queda en pantalla todo el acontecer vivido frente a la potencial mirada de miles de personas. No ser muy popular en estos tiempos de alta visibilidad es algo no deseado. Los likes, los Me gusta, en definitiva, todo lo que muestra cómo va su vida social, aparece allí en pantalla, como una suerte de cotización en bolsa.

NUEVOS PARADIGMAS DE LO PRIVADO

Nos encontramos frente a un nuevo paradigma en la concepción de la privacidad. En otro lado (Balaguer, 2008) hemos denominado *outimidad* a esto que predomina en las redes. Es desde lo público, desde la desconexión, que se encuentra la manera de hacer algo privado, ponerlo a resguardo, contraviniendo el movimiento cultural, casi automático de compartir. Hacer algo privado es el movimiento equivalente a hacer algo público en el pasado. Cuidar los datos, significa desprenderse de las redes sociales virtuales. Por eso, la pregunta que se hacen los usuarios de redes es ahora: ¿qué hago privado? en lugar de: ¿qué hago público?

Por definición, en las redes que habitamos, todo se vuelve público a no ser que se busque filtrar la audiencia para acotar la masividad de la llegada. Y en ese devenir público los jóvenes están permanentemente brindando datos de sí mismos, sin una conciencia total de la magnitud de ese tema.

El ingreso a las redes, la vida en ellas, representa un cambio importantísimo, ya que los niveles de influencia de los nodos mutan constantemente. En esa posible constante conexión con los otros, el territorio de las redes es inmensamente más cambiante que el de la modernidad sólida (Castells, 1997; Bauman, 2000) y ese es el telón donde se desenvuelve la vida juvenil, bastante más complicada en la medida que todo queda en las redes sin contexto explicativo. Los aproximadamente siete millones de likes por minuto en Facebook y los 6 millones y medios de videos vistos en Snapchat son algunas de las cifras que nos muestran el alcance de Internet hoy y que permanecerán mañana dando cuenta de nuestro tránsito por Internet.

LA IDENTIDAD DIGITAL

Los jóvenes brindan datos sobre ellos mismos 24/7/365. El intercambio, la formación de espacios que ayudan a delinear identidades son clave en esta etapa de la vida y las nuevas tecnologías permiten desarrollar toda esa cuestión social a través de diversas herramientas. Todo aquello que escriben, suben o comentan en las redes, páginas personales o institucionales, blogs, conforman la identidad digital.

Si además incluimos todas las apps que brindan datos de salud, ejercicio, sueño, el panorama es aún más complejo. El mundo actual es un mundo de cámaras omnipresentes, en algunos casos incluso cargadas con software de reconocimiento facial. Vivimos en un mundo donde la gente brinda datos a las aplicaciones y las aplicaciones generan datos a las empresas que en un mundo de *Big Data* y *Machine Learning* pueden generar conocimiento.

Cada cosa que escribimos, subimos, comentamos, etiquetamos en las páginas personales o institucionales, blogs, redes sociales va conformando la identidad digital, esa identificación que nos acompaña en nuestro accionar por la web. Esta consta de dos partes bien distinguibles: una deseada, fomentada y creada a partir de las intervenciones que hacemos y otra, que se desprende de la forma en que intervenimos en la Red, es decir aquello que dejamos entrever de nosotros casi sin quererlo. Hay datos explícitos y otros implícitos A su vez, los datos que brindamos a veces son estructurados y otras tantas veces, son interpretables a partir de algoritmos. Las trazas de navegación de los sitios en los que se ingresa también son rastreables además de las trazas declarativas, es decir todo lo que decimos en las redes, expresamos y mostramos en palabras.

LA FALTA DE CONSCIENCIA POR PARTE DE LOS JÓVENES AL RESPECTO DE SU IMPORTANCIA A FUTURO

Según Web World Stats el 61 % del total de los internautas uruguayos (1.855.000) tiene su perfil en Facebook. Facebook como plataforma digital

integra buena parte de la identidad digital. Los jóvenes por lo general intentan minimizar el hecho de que su accionar en la red deja rastros digitales. Negar los peligros o riesgos es propio de esa etapa de la vida signada por el riesgo. Para ellos, las cosas "les pasan a los otros". Los chicos admiten que suelen tomar recaudos y protegerse en relación con los demás pero no siempre con ellos mismos. Nuestros hijos piensan que nadie presta demasiada atención a su presencia y a sus dichos y que su accionar queda restringido a su grupo de amigos. Amparados en esa fantasía pueden actuar de formas de las cuales luego podrán arrepentirse. La otra fantasía que uno observa es que sus publicaciones van a ser vistas solamente por aquellos que ellos quieren efectivamente que las vean. Es una forma de pensamiento mágico harto común en esas edades.

UNA INVISIBILIDAD FICTICIA

Lo que sucede en el ámbito de internet y sus distintos entornos queda para muchos adultos por fuera del univer¬so, no solo visible, sino también —y eso representa una enorme pérdi¬da— cognoscible. Buena parte de lo que acontece con y entre los jóvenes se da en los entornos virtuales, en pantalla. Esto genera cierto grado de invisibilidad no solo en los padres, sino también en los docentes y profesiona¬les «analógicos» —si se me permite el término— que quedan por fuera de varios de los códigos y entor¬nos juveniles (Balaguer, 2012). Cu¬riosamente, eso es, en parte, lo que los jóvenes desean: cierto grado de invisibilidad que pretenden que así permanezca. Mientras las redes son para los jóvenes lugares de encuentro, para muchos adultos se vuelven, en un inicio, redes de reencuentro (Balaguer, 2012) con vínculos pasados.

LOS RIESGOS DE LOS USOS ALGORÍTMICOS DE ESOS DATOS

Cada cosa que se escribe cuando se está en Internet —incluso un aparente inocuo "me gusta" de Facebook — se transforma en una radiografía instantánea de la persona. El estudio Kosinski (2013) es una muestra de ello. Tuvo un fuerte impacto mediático ya que solo tomando en consideración los Me gusta de Facebook el estudio mostró que es posible predecir con un alto porcentaje de acierto la raza, edad, orientación sexual y tendencia política de cada usuario. Ese estudio llevado a cabo entre 58.000 personas alertó a los internautas sobre el rastro digital que dejan a su paso. Los "me gusta" de Facebook permitieron saber con alta precisión si el usuario era hombre o mujer (88% de aciertos) si votaba al partido demócrata o al republicano (85%). Tuvo un porcentaje de acierto de 82% al determinar si el voluntario era cristiano o musulmán y supieron con un grado de precisión entre el 65 y el 75% si era o no consumidor de droga.

Sobre finales de marzo de 2017 el Congreso de los EEUU aprobó una ley que le permite a las compañías proveedoras de internet seguir y vender la actividad personal de las personas a terceros. Esto representa una fuerte amenaza a la privacidad de las personas. Cuando todo se vuelve transparente, la única forma de luchar contra ellos es distraer. En ese sentido, la comunidad comienza a hacer surgir herramientas para despistaje. Una de ellas es Internet noise (ruido en Internet), una aplicación que cumple con ese cometido de generar ruido para evitar el seguimiento. La aplicación que se utiliza con el navegador Chrome, carga aleatoriamente sitios aleatorios en las pestañas del navegador. Llena las bases de datos con el ruido como una forma de protesta contra el seguimiento y el perfilamiento, ese Gran Hermano que parece haberse instalado entre nosotros sin que a la mayoría le genere ningún ruido, valga la paradoja.

BIBLIOGRAFÍA

1. Balaguer, R. (2009) (compil.) "Los ojos del mundo en el Plan Ceibal" *en Plan Ceibal. Los ojos del mundo en el primer programa OLPC a escala nacional*, Montevideo: Pearson Ed.
2. Balaguer, R.; Canoura, C. (2010) *Hiperconectados. Guía para la educación de nativos digitales*, Montevideo: Santillana.
3. Balaguer, R (2012). *La Nueva Matriz Cultural. Claves para entender cómo la tecnología moldea nuestras mentes*, Montevideo: Pearson Foundation.
4. Balaguer, R (2016). *La práctica psicoanalítica en el universo digital. Psicoanálisis para un mundo líquido.*
5. Bauman, Z. (2000) *Modernidad Líquida*, México: Fondo de Cultura Económica, 2002
6. Castells, M. (1997) The Power of Identity The Information Age: : *Economy, Society and Culture* Vol. II. Cambridge, MA; Oxford, UK: Blackwell
7. HarrisInteractive, *A generation unplugged*, Research Report September 12, Disponible en: 2008 http://files.ctia.org/pdf/HI_TeenMobileStudy_ResearchReport.pdf
8. Kosinski, M. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academics Science 2013 Apr 9; 110(15): 5802–5805. Published online 2013 Mar 11. 10.1073/pnas Wilmer, H. Chein, J.(2016). Mobile technology habits: patterns of association among device usage, intertemporal preference, impulse control, and reward sensitivity

LA LEY 18.331 Y EL REGLAMENTO (UE) 2016/679

Apuntes para un nuevo alineamiento

MARCELO
BAUZÁ

Doctor en Derecho y Ciencias Sociales (UDELAR-Fac. Derecho-Uruguay). Asesor Letrado de la Agencia para la Gestión del Gobierno Electrónico y la Sociedad de la Información y el Conocimiento – AGESIC y la Unidad Reguladora y de Control de Datos Personales (2008-2014). Actualmente es miembro del Consejo Consultivo de este órgano, en representación del área académica. Profesor Adjunto de Informática Jurídica (UDELAR-Fac. Derecho-Uruguay). Fue Director del Instituto de Derecho Informático, y luego Coordinador del Centro de Derecho Informático de la citada Facultad. Diplomado de Estudios Superiores (D.E.A.) en Informática Jurídica y Derecho de la Informática por la Universidad de Montpellier I, Francia (1989-1990). Premio Lamy "Droit de l´Informatique" por la obra "Le droit de la preuve et l´informatique" en coautoría con el Dr. Audilio González Aguilar (1990). Stage académico de ocho meses en la misma especialidad en Italia con el Profesor Mario Losano, y un mes en España con el Profesor Fernando Galindo (1988). Vicepresidente y Secretario General de la FIADI (Federación Iberoamericana de Asociaciones de Derecho e Informática – www.fiadi.org (1996-2015).

SUMARIO

RESUMEN

Un interesante desafío que se le presenta al Estado uruguayo, como a otros países de la región, es determinar si su normativa de protección de datos personales se adapta al Reglamento (UE) 2016/679, cuya vigencia sobrevendrá a partir del 25 de mayo de 2018, derogando la Directiva 95/46/CE.

Uruguay pertenece a un reducido elenco que se ha hecho acreedor de la "decisión de adecuación" en la materia, por parte de la Unión Europea. Junto con Argentina, los dos únicos de la región. Los otros son Suiza, Israel, Nueva Zelanda, Andorra, Guernsey, Jersey, Isla de Man, Islas Feroe y el sector privado de Canadá. Estados Unidos contaba hasta no hace mucho también con dicha decisión, pero un fallo de la Corte de Justicia UE de 2015 anuló la declaración de adecuado del Safe Harbor.

Se trata de un primer examen, resumido y sin pretensiones de exhaustividad, en el que se pone el acento en las cuestiones que, a juicio del autor, deberían tomarse del Reglamento europeo, para su incorporación a la Ley 18.331 del 11/08/2008, sea por vía de reformas parciales al texto vigente, como ya se ha hecho en otras oportunidades, sea por la aprobación de una nueva ley.

El pasaje de la simple gestión de datos al uso responsable de la información, con nociones no solamente apuntadas sino ampliamente desarrolladas en el RGPD ("responsabilidad proactiva, accountability), se reconoce como el eje central del nuevo modelo, al menos uno de esos ejes. Las "medidas técnicas y organizativas" de cargo de responsables y encargados de tratamientos desplazan el derogado deber general de registro de las bases de datos, y pasan a tener un rol de mayor peso que en el pasado, justamente por el afán de prevenir daños más que repararlos cuando acaecen y pudieron evitarse.

El mismo razonamiento subyace en la incorporación obligatoria de la "privacidad en el diseño y por defecto", herramientas que contribuyen a que los derechos ARCO mantengan plenitud de vigencia. Igual propósito se persigue con la introducción de las evaluaciones de impacto. Estos y otros múltiples ejemplos que se exponen en el texto, muestran que con el RGPD ya no alcanzará con "no incumplir" sino que habrá los responsables y encargados de tratamientos habrán de organizar una completa "gestión del riesgo" a fin de exonerarse si ocurrieran perjuicios.

Otras partes del frondoso articulado del RGPD son igualmente analizadas, atendiendo siempre a aquello que, por novedoso, debería provocar o estimular una actualización del sistema normativo nacional.

El análisis es más detenido en algunos puntos: las transferencias internacionales de datos, su nuevo sistema (que no difiere mucho del anterior en su base, pero sí agrega otras posibilidades, o matices); las autoridades de control, en particular su acentuada caracterización como independientes.

EL NUEVO REGLAMENTO EUROPEO

La protección de datos personales mudará su ropaje jurídico europeo, concretamente a partir del 25 de mayo de 2018 cuando entre en fase de aplicación el nuevo Reglamento (RGPD), que deroga la Directiva 95/46/CE.[1]

No se trata de un cambio menor. La nueva regulación es producto de un largo proceso de reforma que tiene sus motivaciones y arraigos, tendiente a renovar el modelo de protección de datos vigente desde hace más de veinte años, que si bien no altera los principios y fundamentos del edificio hasta ahora construido, de todos modos introduce fuertes novedades.

Con lograda capacidad de resumen, se ha dicho que las legislaciones apoyadas en la Directiva 95/46/CE terminaron por adolecer de las siguientes carencias:

- "Falta claridad en los objetivos que la norma pretende conseguir: busca proteger datos personales pero no se identifica frente a qué o en qué medida.
- Orientada a procesos, se establece lo que hay que hacer pero no por qué, para evitar qué daño o para mejorar qué aspecto de la protección.
- Son obligaciones genéricas aplicables a todos los responsables sin reconocer diversidad o contexto.
- Obligaciones no priorizadas más allá de que pueda deducirse de posibles esquemas sancionatorios."[2]

Expertos en la disciplina han señalado, asimismo, que, "La legislación vigente en materia de protección de datos se remonta a 1995, la Directiva 95/46/CE, … Sus planteamientos siguen siendo válidos, pero se han adoptado hace ya 19 años,

1 *Publicación. oficial: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES*

2 *Ma. Rosario Heras Carrasco, "El nuevo Reglamento Europeo de Protección de datos", pág. 3, en http://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/3100.pdf*

momento en que Internet estaba naciendo para el gran público. En el nuevo y complicado mundo digital estas normas no aportan ni el nivel de armonización requerido, ni son eficaces para garantizar el derecho fundamental a la protección de datos personales en la Unión Europea".[3]

Buscando sintetizar al tiempo que destacar lo más esencial de este cambio, se ha sostenido lo siguiente: "Un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información" calificando y extendiendo esta primera apreciación a renglón seguido cuando se agrega: "Este es seguramente el más profundo cambio que el Reglamento va a imponer y que se aprecia en cuestiones como el principio de *accountability* traducido por ´responsabilidad proactiva´ (art. 5.2 del Reglamento), los principios de privacidad desde el diseño y por defecto, la aproximación a la protección de datos basada en el análisis de riegos, la figura del Delegado de protección de de datos, el fortalecimiento de los códigos de conducta, la exigencia de llevar un registro de las actividades del tratamiento, la regulación de las medidas de seguridad, y un largo etcétera…"[4]

Y finalmente, para redondear esta introducción al tema, no encontramos un marco más adecuado que referir a los cuatro objetivos que, a juicio de Troncoso Reigada, presenta la reforma, a saber:

1. Adaptar la normativa de protección de datos personales a los formidables cambios tecnológicos producidos en estos años (expansión rápida de Internet y lo que ha traído consigo como los buscadores, las redes sociales, la computación en la nube, el Internet de las cosas, el big data, etc.).
2. Garantizar mejor el derecho fundamental frente a la elevación de los riesgos producto de múltiples y variados factores (videovigilancia, biometría, historia clínica electrónica), dándole a la persona herramientas para un mayor control sobre sus datos personales sometidos a tratamiento, y fortaleciendo las garantías de los derechos en juego.
3. Favorecer la creación de un mercado digital, potenciador de la actividad económica y la competitividad de las empresas (todo lo referente a la libre circulación de estos datos).
4. Simplificar los mecanismos de protección, reduciendo cargas administrativas de las empresas, en directa conjunción con el incremento de la "accountability".[5]

SU INCIDENCIA EN LA LEY URUGUAYA

En la región iberoamericana existe preocupación por cuidar la armonía de los regímenes nacionales con la reforma del derecho europeo. No podría ser de otra manera, en tanto las leyes nacionales de la región están inspiradas, y ampliamente conectados, con una misma concepción, y sobre todo que en la práctica muestran y asumen vasos comunicantes con la realidad europea merced a la dupla de defensa del derecho fundamental y el favorecimiento del comercio extra fronterizo. Preocupación que explica, entre otros factores, la reciente aprobación de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos[6].

Uruguay no escapa a esta motivación, máxime atendiendo el hecho de ser uno de los pocos países no europeos (y en el mundo todo), que cuentan con una "decisión de adecuación" al sistema. Adecuación que fue alcanzada bajo el régimen europeo anterior y no revisada hasta el presente (lo cual era facultativo), pero que lo será en el futuro escenario, necesariamente. Bien lo ha expuesto Pérez Assinari, cuando expresa que "La decisión de adecuación no significa un ´cheque en blanco´…" y "con la adopción del nuevo reglamento se produce un cambio importante, ya que la Comisión Europea deberá realizar revisiones periódicas, al menos cada cuatro años, que tengan

3 *Álvaro Sánchez Bravo, "Nuevo marco europeo de protección de datos personales", pág. 256, en Derechos Humanos y Protección de Datos Personales en Siglo XXI. Homenaje a Cinta Castillo Jiménez, AA.VV., obra colectiva dirigida y editada por el propio Sánchez Bravo, 329 págs., Ed. Punto Rojo, España, 2013.*

4 *José Luis Piñar Mañas, "I. Introducción. Hacia un nuevo modelo europeo de protección de datos", pág. 17. En Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, AA.VV., obra colectiva dirigida por el propio Piñar Mañas, 863 págs., Ed. Reus, Madrid 2016.*

5 *Antonio Troncoso Reigada, "XXVI. Autoridades de Control independientes", págs. 462-463. En Reglamento General de Protección de Datos..., obra colectiva cit.*

6 *En el presente examen solamente son mencionados, dado el carácter reciente de su aprobación. Fueron elaborados en el Taller de trabajo llevado a cabo los días 9 a 11-05-2017 en Cartagena de Indias, Colombia, en el marco de la Red Iberoamericana de Protección de Datos, y proclamados en Santiago de Chile en oportunidad del XV Encuentro de la Red, 20 a 22-06-2017. Su texto está publicado, entre otras fuentes, en el sitio web de la Unidad Reguladora y de Control de Datos Personales. Ver:https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/95be7f85-3736-4bb4-9547-4bebf064be10/Estandares_de_proteccion_de_datos_personales_para_los_estados_iberoamericanos.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=95be7f85-3736-4bb4-9547-4bebf064be10*

en cuenta los desarrollos acaecidos en los países declarados adecuados…" pudiendo a consecuencia de tal revisión "repeler, enmendar o suspender la decisión de adecuación".[7]

Por estas circunstancias es del caso pronosticar que en corto plazo deberían producirse algunos alineamientos normativos en nuestro país, en base a un desiderátum que, tarde o temprano, se le impone a todo régimen jurídico, como es el de no perder adaptación a la realidad.

Esa intervención o re-armonización, es obvio predecirlo, será hecha en cualquier caso de la forma que mejor entiendan las autoridades en la materia, ya sea a través del dictado de una nueva ley sustitutiva de la No. 18.331, o mediante reformas parciales al régimen vigente. Personalmente somos partidarios del dictado de una nueva ley, dado el alto número de modificaciones, y algunos fuertes cambios en los paradigmas en juego, lo que alimenta renovaciones conceptuales de buena caladura, no tanto meros ajustes o retoques de la ley vigente. Como sostén de esta convicción nos viene a colación lo siguiente: "Es el ´ser´ más que el ´deber ser´ el que suele exigirle dosis de pragmatismo al Derecho, recordándole la necesidad irrenunciable de intervenir en la compleja realidad de las relaciones humanas mediante fórmulas resueltas y decididas. Fórmulas que no se aparten de su esencialidad y destino."[8]

Son muchas las novedades del nuevo Reglamento europeo. No podremos abordarlas todas. El presente artículo repasa tan solo algunas de ellas y lo hace de un modo resumido. A pesar de estas limitantes, se entiende oportuno, y se espera que útil, repasar conceptos e ítems normativos sobre los que posiblemente fuere conveniente proceder a una actualización de la norma nacional, poniendo la mira en el futuro pero inminente escenario donde la fuente jurídica de consulta, inspiración y hasta adaptación de todo el sistema, ya no será más la Directiva 95/46/CE, sino el Reglamento (UE) 2016/679.

Más allá del expresado propósito central, se aprovechará para exponer también algún posible ajuste que podría merecer la norma nacional con independencia del aludido alineamiento, simplemente a la luz del tiempo y la experiencia recogidos durante el lapso de vigencia que lleva el régimen vernáculo sin otras alteraciones que unas pocas y puntuales, motivadas en ajustes que el devenir de la realidad en este caso nacional, aconsejaron acometer[9].

EL DOBLE ALCANCE DE LA NORMATIVA RELACIONADA CON LA PROTECCIÓN DE DATOS PERSONALES

Si hay algo que está bien claro en las definiciones iniciales y centrales del Derecho de la Protección de Datos Personales (como disciplina jurídica), es su formulación y presencia en el escenario de las relaciones de la sociedad contemporánea, como derecho fundamental. Se trata de un rasgo acentuado, si se quiere, en nuestra ley 18.331, cuyo art. 1 define a este derecho como "inherente a la persona humana", encuadrándolo a texto expreso –por si quedaran dudas- en el art. 72 de la Constitución de la República.

Sin embargo, existe otra dimensión diferente de este mismo Derecho (siempre entendido como disciplina jurídica), que la norma uruguaya no contempla a texto expreso, y es el apareamiento de toda la materia en juego con la necesidad social de resguardar a igual tiempo la libre circulación de los datos.

Parece curioso y hasta tautológico expresarlo, pero contribuye a esclarecer el punto afirmar que la razón de que haya emergido y desenvuelto la protección de datos como un derecho fundamental, no es otra que la necesidad inexorable e históricamente demostrada en la sociedad moderna, de preservar que el tratamiento de dichos datos por agentes externos a su titular tenga su calle de actuación con la mayor amplitud posible. Una preservación comandada por el principio de proporcionalidad, para que la necesidad económica y social no termine por afectar más allá de cierto límite, el plexo de derechos fundamentales del individuo.

7 *María Verónica Pérez Asinari, "Impacto en Uruguay del nuevo Reglamento de la Unión Europea sobre protección de datos personales", publicado en https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/c999a065-4daa-4d1b-8a68-369139d60145/Informe_P%C3%A9rez_Asinari_Mar%C3%ADa_Ver%C3%B3nica_2016+%281%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=c999a065-4daa-4d1b-8a68-369139d60145*

8 *Marcelo Bauzá, "La protección de datos personales y su armonización con otros derechos y las políticas de e-gobierno", pág. 53, en op. cit. Derechos Humanos y Protección de Datos Personales en Siglo XXI. Homenaje a Cinta Castillo Jiménez.*

9 *Entre otras, Ley 18.719 de 27/12/2010, arts. 152 y 156, y Ley 19.355 de 19/12/2015, en ambos casos introduciendo ajustes a la redacción original de los arts. 9 y –por remisión- 17 de la ley madre (principio del previo consentimiento informado, derechos referentes a la comunicación de datos, respectivamente); Ley 18.996 de 07/11/2012, art. 43, que agrega el art. 9 bis a la ley madre, estableciendo una mayor regulación de las "fuentes públicas de información", las que simplemente se mencionaban por su título genérico aglutinador en el art. 9 de la ley madre; Ley 18.719, art. 152, dando nueva redacción inc. 2 del art. 14 de la ley madre en materia de datos de personas fallecidas.*

Si no existiera esta necesidad de hacer lugar a los tratamientos que sirven a la libre circulación de los datos, no habría motivo para considerar y proteger el espacio de libertad individual. Razón suficiente, a nuestro juicio, para que los textos normativos nacionales hagan mención de ello.

De forma expresa, el RGPD contempla *ab initio* esta dimensión de la libre circulación y su equilibrio con el/los derechos fundamentales del individuo (considerandos 2 y 3, art. 1), como por otra parte ya lo hacía la Directiva 96/45/CE (art. 1), y el propio Convenio de Estrasburgo No. 108 (segundo considerando). Incluso el nuevo Reglamento parece reforzar esta línea de inclusión a través de una redacción que deja rotundamente asentado el doble propósito de la disciplina.[10]

Sin embargo, las fuentes de inspiración utilizadas en su momento para dar vida a la Ley 18.331 (fundamentalmente la ley argentina No. 25.326 de 30-10-2000), no incluían la faceta evocativa de este segundo aspecto, de vis trascendentemente –aunque no exclusivamente- comercial, y a la que interpela continuamente la sociedad contemporánea cuando de "datos" se habla: su libertad de circulación.

Por lo dicho, y no obstante estar presente este sesgo en las raíces mismas de la disciplina, así como en su continua sistematización histórica, puede ser ésta una buena oportunidad para que la norma uruguaya introduzca algún tipo de referencia explícita al punto. Nos animaríamos a decir que, a la altura de la realidad actual y sus requeridos componentes (trasnacionalidad de las relaciones humanas en constante aumento y en todos los planos), resulta necesaria esta invocación expresa. Para delimitar con claridad las posibles interpretaciones que, de otro modo, quedan libradas a una multiplicidad de sentidos, rayano por ello en la inseguridad jurídica.

De últimas, de lo que se trata es de buscar el equilibrio entre dos derechos, el de las personas a preservar sus datos, y el de la sociedad lato sensu (incluye empresas pero también otras entidades e intereses que se entiendan legítimos), permitiendo utilizar los datos de esas mismas personas, para fines justificados: el consabido "pacto social" consistente en "te doy mis datos pero preservemos mi control sobre los mismos".[11]

Una armonización de esta naturaleza, presente en los mismos cimientos de la disciplina, requiere que se deje bien claro que también importa el segundo polo, o sea el de asegurar la libre circulación de los datos personales, en orden necesario a la desenvoltura del cuerpo social, pero siempre atendiendo que ello sea compatible con la preservación del derecho fundamental del titular del dato.

Posiblemente fuere hora de establecer un agregado de texto a la norma nacional que pusiera en evidencia tal aspecto, puesto que su actual redacción no contiene esta singular referencia o vinculación.

EL CONSENTIMIENTO DEL INTERESADO

No es del caso insistir sobre la importancia y el rol centrales del consentimiento de los titulares de los datos, dentro del sistema jurídico que hace al tratamiento de datos personales.

Sobre el tema, el art. 4.11 del RGPD introduce modificaciones al texto de la Directiva 95/46/UE, no necesariamente influyentes (al menos no todas ellas) en nuestra Ley 18.331, como veremos a continuación.

La exigencia de *inequívoco* ya estaba contemplada en nuestra norma (art. 4 C de la Ley 18.331). La novedad está en la forma que puede asumir la expresión de ese consentimiento, el que cabe canalizar "mediante una declaración o una clara acción afirmativa".

El considerando 32 del Reglamento especifica que este consentimiento puede asumir la forma de una declaración por escrito, incluyendo medios electrónicos, o incluso una declaración verbal. Como ejemplos concretos se alude al marcado de una casilla en un sitio web, la escogencia de parámetros técnicos relativos a la utilización de servicios, o toda otra declaración o conducta de la que emerja de modo indubitable una aceptación del titular a que se utilicen sus datos.

Otros aspectos que interesan en punto al consentimiento del titular, sin que signifiquen estrictamente una novedad pero sí exigencias establecidas con mayor claridad en el RGPD, son lo relativo a la necesidad de contar con tantos consentimientos como especies de tratamiento se sometan los datos (considerando 32 y art. 7.3 del RGPD), y el carácter revocable sin sanción del mismo (considerando 42 del RGPD).

El art. 7 del RGPD por su parte establece una serie de "condiciones del consentimiento", todas ellas tendientes a poder asegurar y comprobar

10 *"El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos" (art. 1.1. del Reglamento).*

11 *Por toda referencia, "Las leyes de protección de la intimidad deben ser un pacto informático entre el ciudadano y el Estado". Entrevista a Mario G. Losano en Boletín No. 128 de Fundesco, Madrid, abril 1992, págs. 6-7.*

su genuinidad, en las que también vale la pena reparar, a saber:

- Capacidad del responsable en cuanto a poder demostrar la existencia efectiva del consentimiento (una de las tantas exigencias de responsabilidad proactiva o *accountability* que incorpora el nuevo Reglamento).
- Posibilidad de distinguir con claridad y fácil acceso dentro de una sumatoria de consentimientos referidos a varios asuntos diferentes.
- Derecho al retiro fácil del consentimiento en cualquier momento, con previa información al interesado de tal derecho.
- Evaluación de la libertad que goza el titular al otorgar su consentimiento, entre otros aspectos cuando se supedita la ejecución de un contrato y/o prestación de un servicio.

Estas alternativas podrían justificar el acometimiento de algunos ajustes de la norma uruguaya en torno a "consentimiento", tema crucial de todo el sistema. Porque la norma uruguaya es menos explicativa, luciendo como escueta y restrictiva al tenor de las acotadas exigencias de "expreso" y "documentado" (art. 9 de la Ley 18.331). Mientras que la fórmula del RGPD, a la vez que más flexible y detallada, aparece como más garantista justamente por incluir previsiones de mayor variedad y detalle.

EL DERECHO AL OLVIDO

Un tema al que la formidable desenvoltura de la informática de redes y sus buscadores, ha dado mayor y dramático relieve si comparamos con épocas pasadas.

La cuestión ha merecido una muy difundida repristinación, provocando nuevos exámenes, a partir del publicitado "caso Costeja"[12]

Un enfoque más general y también actual lo patentiza la siguiente cita del recientemente desaparecido gran doctrino Stefano Rodotá (traducción libre del autor de este artículo): "¿En qué cosa deviene la vida en el tiempo en el que ´Google recuerda siempre´? La implacable memoria colectiva de Internet, donde la acumulación de cada una de nuestras trazas nos rinde prisioneros de un pasado destinado a no pasar más, desafía la construcción de la personalidad libre del peso de cada recuerdo, impone un continuo escrutinio de parte de una infinita multitud de personas que pueden fácilmente conocer la información sobre los otros."[13]

El mismo autor alude al combate del problema luego de enunciarlo: "Nace de ahí la necesidad de defensas adecuadas, que toman la forma de la demanda de derechos nuevos –el derecho al olvido, el derecho de no saber, de no ser ´trazado´, de ´volver silencioso´ el chip gracias al cual se recogen los datos personales"[14]

La norma uruguaya recoge este concepto pero lo hace desde un plano indirecto y si se quiere extremo, cuando establece que los datos "deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados", reconociendo como excepción su conservación en determinadas hipótesis que la propia norma establece y remite a reglamentación (art. 8 de la Ley 18.331).

El art. 15 de la ley uruguaya también se relaciona con el tema en examen, cuando aborda la serie de derechos del titular del dato, entre ellos la supresión o exclusión del tratamiento de que se trate, pero no abunda sobre los casos en que ello procede.

El RGPD por su parte regula con mucha mayor soltura el mismo asunto, lo que bien puede determinar la conveniencia de una actualización de la normativa uruguaya en este punto.

En efecto, del art. 17.1 del Reglamento se desprende de modo expreso y claro la serie de hipótesis en las que cabe ejercitar el derecho de supresión (que el mismo artículo califica entrecomillado como "derecho al olvido"). Se trata de situaciones variadas, que no se circunscriben al cumplimiento de los fines para los que fueron recogidos o tratados los datos (literal a del citado artículo).

Figuran así, como otras causales de supresión, el retiro del consentimiento por parte del interesado (lit. b); el ejercicio del derecho de oposición en

12 *Sentencia Tribunal de Justicia de la Unión Europea. Asunto C-131/12 (Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González) de 13 de mayo de 2014*

13 *Stefano Rodotá, "Il mondo nella rete. Quali i diritti, quali i vincoli", ed. Laterza, 2014, Roma. La cita original figura en la pág. 41 y es la siguiente: "Che cosa diviene la vita nel tempo in cui ´Google ricorda sempre´? La implacabile memoria colectiva di Internet, dove l´accumularsi d´ogni nostra traccia ci rende prigionieri d´un passato destinato a non pasarse mai, sfida la construzione della personalitá libera dal peso d´ogni ricordo, impone un continuo scrutinio sociale da parte di una infniita schiera di persone que che possono fácilmente conoscere le informazioni sugli altri."*

14 *Op cit., pág. 41. "Nasce da qui il bisogno di difese adeguate, che prende la forma della richiesta di diritti nuovi –il diritto all´ oblio, il diritto di non sapere, di non essere ´tracciato´, di ´rendere silenzioso´il chip grazie al quale si raccolgono i dati personali."*

los términos y contextos de que da cuenta el art. 21 del propio Reglamento (lit. c); el tratamiento ilícito (lit. d); el cumplimiento de una obligación legal de supresión (lit. e); el consentimiento de niños en relación a servicios de la sociedad de la información (lit. f).

Finalmente una adecuada consideración de este mismo tema no debería dejar pasar las situaciones en las que descaece el derecho de supresión u olvido, vale decir los casos en que el dato personal recobra perennidad, y que el propio Reglamento europeo se encarga de presentar en el art. 17.3. Cabe contemplar, así, el ejercicio del derecho a la libertad de expresión e información (lit. a); el cumplimiento de una obligación legal, o una misión de interés público, o el ejercicio de poderes públicos conferidos al responsable (lit. b); razones de interés público en el ámbito de la salud (lit. c); fines de archivo en casos de interés público, investigación científica, etc. (lit. d); formulación, ejercicio o defensa de reclamaciones (lit. e).

EL DERECHO A LA PORTABILIDAD DE LOS DATOS

Se trata de una novedad absoluta, regulada en el art. 20 del RGPD, como tal de necesaria contemplación *ex novo* en cualquier actualización del régimen nacional que fuera del caso encarar.

Se ha señalado como antecedente histórico de este derecho una norma española. El Real Decreto 2296/2004 de 10 de diciembre, que aprobara el reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, consagra un "derecho a la portabilidad numérica" a favor de los abonados al servicio telefónico público, facultativo del titular que solicitare conservar su número aún cambiando de compañía proveedora del servicio.[15]

Asimismo se ha evocado como "principal impulsor del desarrollo de este derecho" el grupo de trabajo creado en EEUU bajo el nombre "Data Portability Project", con el propósito de facilitar el control de los usuarios sobre informaciones proporcionadas a prestadores de servicios, y contar con un punto de encuentro de las compañías del sector digital para facilitar las prácticas atinentes a la portabilidad "de una forma homogénea, sencilla y transparente para el usuario".[16]

Consiste –pues- en el derecho del interesado a recibir los datos de su incumbencia por parte del responsable del tratamiento, en un formato estructurado y con las propiedades necesarias como para ser transmitido a otro responsable sin que lo impida el primero, ya sea por el titular como en forma directa (de responsable a responsable).

Este derecho se ve mitigado o excepcionado en torno a alguna de las causales vinculadas con el derecho al olvido. Tampoco puede afectar negativamente los derechos y libertades de terceros.

EL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

Un nuevo derecho de los titulares de datos personales, que habilita para ciertos casos una solución intermedia entre la prohibición y la autorización al tratamiento de datos personales por parte de los responsables.

La fórmula se agrega al tradicional elenco de derechos ARCO. Su ejercicio no se abre de modo indiferenciado, sino en función de hipótesis o condiciones que indica el art. 18 del Reglamento, a saber:

1. Impugnación de la exactitud de de los datos tratados, durante un plazo que permita al responsable realizar la verificación del caso.
2. Tratamiento ilícito no obstante lo cual el interesado se opone a la supresión y, en lugar de ello, requiere la limitación de uso.
3. Cuando el responsable ya no necesite los datos, pero sí los necesite el interesado para reclamaciones.
4. Oposición al tratamiento por parte del interesado en los casos que especifica la norma remitiendo al art. 21 apartado 1, mientras se verifica la prevalencia de motivos legítimos a favor del responsable.

LA "ACCOUNTABILITY" O RESPONSABILIDAD ACTIVA, Y LA EVALUACIÓN DE IMPACTO

Sobre lo primero (la responsabilidad activa, también denominada –quizás con mayor propiedad "proactiva") aludimos a un concepto tradicional si se quiere reformulado. Subyacente en las regulaciones vigentes hasta hoy día, de todos modos es puesto en vitrina con un énfasis y detalle inusitados, en la nueva normativa europea. Al punto de considerarse el elemento central de la reforma, como pusiéramos de relieve al comienzo de este artículo.

15 *Javier Fernández-Samaniego y Paula Fernández-Longoria, "XVI. El derecho a la portabilidad de los datos", pág. 258. En Reglamento General de Protección de Datos..., obra colectiva cit.*

16 *Op cit. pág. 259.*

Tan importante es este nuevo concepto introducido por el RGPD, que podemos decir que contiene un núcleo duro –el comentado en este apartado- pero también permea en ejemplos numerosos por fuera de este núcleo, previstos en otros segmentos del Reglamento. Con el RGPD se considerará insuficiente el "no incumplir", y se exigirá la prevención de acontecimientos que pudieran conducir a ello, para evitarlos antes de que ocurran. Todo lo que se relacione con este premisa, agrupado bajo la noción de "gestión del riesgo", forma parte del cambio del paradigma vigente. Un cambio bastante radical como ya se ha señalado. Conductas todas que, en conjunto, apuntan a exigir del responsable ciertas y determinadas acciones de tipo previsor, reales y concretas, que el Reglamento no se conforma con aludir de modo genérico sino que elenca de forma concreta, y que deben ir en procura de un mismo fin, anticiparse con medidas efectivas al acaecimiento de daños que encuentren su causa en el incumplimiento del Reglamento, y por ende supongan una claudicación en la protección de los datos personales y sus titulares.

Así es que emergen otro tipo de previsiones que no atienden al tratamiento en sí mismo, pero que de todas formas se anteponen o relacionan con el mismo, exigiendo el proactivismo, la anticipación, del responsable. Pueden considerarse ejemplos de ello, entre otros, de la "privacidad desde el diseño y por defecto", que comentaremos en otra parte de este trabajo.

Como quiera que sea, el foco central sobre responsabilidad proactiva y *accountability*, consiste en exigir del responsable del tratamiento el mayor activismo posible, en aras de acreditar, cuando se le exija, que el tratamiento a su cargo cumple con el Reglamento (art. 24 de éste).

Para ello se le obliga que aplique medidas técnicas y organizativas apropiadas, revisables y actualizables las veces que sea necesario, destacando el rol de los códigos de conducta aprobados, como elemento demostrativo de cumplimiento de este tipo de responsabilidad.

En nuestra opinión, como ya dijimos, se trata del cambio más importante del nuevo sistema, contrapuesto a la experiencia anterior confiada mayormente a otras herramientas que, a la luz de años de experiencia práctica, no resultaron lo eficientes que se esperaba (defección reconocida a texto expreso por el considerando 89 del RGPD).

No se trata de sostener que, bajo el régimen prohijado por la Directiva 95/46/CE, no existiera o se ignorase la responsabilidad de parte de quienes realizan tratamientos (responsables y figuras linderas). La cuestión es otra. La experiencia histórica mostró que los caminos para descubrir y hacer valer esta responsabilidad no pasaban por la violación exclusiva de deberes formales. Y fue ahí que hincó la palanca de cambio el RGPD.

Frente a la mala praxis e incumplimiento de la normativa aplicable, sobre todo aquélla que ponía en jaque los esquemas esenciales del sistema, la normas relativas a responsabilidad siempre estuvieron presentes, como corresponde –por otra parte- a cualquier sistema jurídico que se precie. Sin embargo, en el marco de la Directiva 95/46/CE, dentro del cual fueron sancionadas las principales leyes latinoamericanas (incluyendo la uruguaya), el enfoque controlador reposaba mayormente en, o a partir de, exigencias de tipo formal, especialmente la inscripción de las bases de datos y sus modificaciones en un registro llevado al efecto por la autoridad de control.

Bajo el nuevo régimen, como decíamos, se cambian estos parangones en forma bastante radical. La novedad estriba esencialmente en que se elimina la obligación general de registrar las bases de datos (lo que los europeos denominan "notificación o inscripción de los ficheros" bajo la autoridad de control), y en sustitución de ello se introducen fuertes cargas para el responsable del tratamiento, en cuanto a la adopción de "medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento" (art. 24.1. del Reglamento). Reforzando más aún esta exigencia, a renglón seguido se establece en el mismo artículo: "Dichas medidas se revisarán y actualizarán cuando sea necesario".

El nuevo régimen se completa con otras reglas de igual importancia, todas ellas bajo la impronta de la responsabilidad activa, a saber:

1. La extensión de las aludidas "medidas" a "oportunas políticas de protección de datos (art. 24.2 del RGPD).
2. La consideración como pauta de cumplimiento del régimen, de la existencia de códigos de conducta o mecanismos de certificación, en ambos casos aprobados según reglas específicamente contenidas en el propio RGPD (art. 24.3 alusivo a su vez a los arts. 40 y 42 del mismo Reglamento).
3. Obligación de los responsables y representantes, de llevar un registro de las actividades de tratamiento con las especificaciones e hipótesis que se indican, entre otras cuando la organización cuente con más de 250 personas (art. 30 del RGPD).

4. Cumplir con una serie de exigencias y garantías que el propio RGPD describe en forma que supera lo que podría haber quedado de remanente en una redacción de tipo generalista, relativas a la adopción de medidas de seguridad, así como a la notificación y comunicación de su violación, a la autoridad de control y el interesado respectivamente (arts. 32, 33 y 34 del RGPD).

Aunque podría considerarse un literal más sobre este tipo de exigencias (razón por la que no le abrimos un apartado específico), nos parece que merece atención particular, por su absoluta novedad, la exigencia al responsable del tratamiento de practicar lo que el RGPD denomina una "evaluación de impacto" en ciertos casos.

El punto está regulado en el art. 35 del RGPD, y supone la presencia de tratamientos basados en tecnologías con "alto riesgo para los derechos y libertades de las personas físicas". Como en todos los casos, el RGPD no se detiene en fórmulas o declaraciones generales tampoco en este tema. Apunta, por el contrario y sin taxatividad, a los casos en que procederá esta medida, como son la elaboración de perfiles, los tratamientos a gran escala de datos de tipo "sensible", y la observación sistemática -también a gran escala- de una zona de acceso público (art. 35.2 del RGPD).

Otros aspectos son igualmente contemplados con esmero por el Reglamento, referidos siempre a este aspecto: publicación y gestión de los tipos de operaciones de tratamiento que requieran esta evaluación, y los que no (arts. 35.4 y 35.5); tópicos que debe incluir la evaluación como mínimo (art. 35.7 del RGPD), y otras exigencias que, por su minucia y extensión, resultaría excesivo detenernos a analizar en este momento.

A modo de resumen del cambio normativo operado en torno a la responsabilidad, se concluye que el Reglamento confiere realce al cumplimiento sustantivo (ya no formal) del régimen, a través de exigencias (deberes) superadoras del plafón formalista que imperaba en el sistema próximo a concluir, fundamentalmente dirigidas y a cargo de los responsables de tratamiento de los datos. Ello se refleja en un conjunto de deberes tendientes a "demostrar la debida diligencia y la adopción de políticas de protección, códigos de conducta y mecanismos de certificación".[17]

A renglón siguiente y de consuno con lo afirmado antes, se ha podido sostener que "Lo que se indica en el considerando 76 es francamente importante pues, como se ha dicho, no se trata de la simple observancia normativa, es decir, la actitud que hasta ahora se viene adoptando por la mayor parte de responsables y encargados de tratamiento que consiste en constatar el nivel de riesgo (básico, medio y alto) y adoptar las medidas reglamentariamente establecidas, sino que el nuevo Reglamento establece un parámetro de cumplimiento que obliga a demostrar la existencia de diligencia debida por parte de responsables y encargados, de forma que, si no existe, se estará incumpliendo *de facto* el Reglamento, por más que desde el punto de vista formal sea aparente el cumplimiento normativo. Por tanto, el simple cumplimiento normativo es condición necesaria, pero no suficiente, para entender que el tratamiento no vulnera lo establecido en la norma europea.- La gestión del riesgo identificado resulta el *quid* de la cuestión".[18]

LA PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

La "privacidad desde el diseño" es un concepto desarrollado por la canadiense Anna Cavoukian en los años noventa del siglo pasado, postulando la inclusión de elementos esenciales en la defensa y promoción de ese concepto a partir del mismo pie constructivo de toda tecnología, bajo siete principios fundacionales que no es el caso desarrollar ahora y solo mencionaremos:[19] [20]

1. Protección Preventiva y Proactiva.
2. Privacidad "por Defecto"
3. Privacidad integrada en el Diseño
4. Funcionalidad Plena "Win-Win" en lugar de "Suma cero"
5. Protección durante todo el Ciclo Vital: "End to End"
6. Visibilidad y Transparencia: "Trust but Verify".
7. Respeto y Empoderamiento del Usuario (centralidad), "User-centric".

Por su lado, la "privacidad por defecto", que está bastante asociada a la categoría anteriormente

17 *Luis Felipe López Álvarez, "XVII. La responsabilidad del responsable", pág. 291. En Reglamento General de Protección de Datos... obra colectiva cit.*

18 *Op. cit. pág. 291.*

19 *Ann Cavoukian, "Privacy by Design. The 7 Foundational Principles", en https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf*

20 *Miguel Recio Gayo, "Protección de Datos desde el Diseño: principio y obligación en el RGPD", en http://tecnologia.elderecho.com/tecnologia/privacidad/Proteccion-Datos-Diseno-obligacion-RGPD_11_1057930001.html*

expuesta como acabamos de ver, apunta al mundo de las *apps*, o sea los pequeños programas progresivamente incorporados de modo preferente a los teléfonos celulares (el mundo del e-móvil), que habitualmente utilizan datos de los propios usuarios para desenvolver sus prestaciones. Consiste en un deber del fabricante de la aplicación, de proporcionar alternativas de privacidad al usuario, informándole al tiempo, o sea antes de su instalación, de esas alternativas.

En este caso, se trata, entonces, de permisos informados en el acto de instalación, a efectos que la app del caso, al ser instalada luego, pueda acceder a las cámaras, contactos, locaciones y todo otro dato que, de un modo u otro, pudiere comprometer la privacidad del usuario.

El concepto refiere a una habilitación de inicio y por niveles, a elección y consentimiento del usuario (ejemplo de *opt*-in), que se le exige al fabricante que incluya en la aplicación. Será entonces el usuario interesado en bajar y contar con la manida aplicación, quien de antemano es informado y se le da la opción, para que tenga asegurado su "nivel de privacidad" en la app que instale desde ese momento.

El RGPD incluye estos dos conceptos como exigencias a texto expreso en su art. 25. En el primer caso, o sea la privacidad desde el diseño, la exigencia es matizada a lo que permita el estado de la técnica, costes de aplicación y otros factores individualizados a texto expreso por el propio Reglamento (numeral 1).

En ambos casos se explicita esta exigencia en la adopción de "medidas técnicas y organizativas apropiadas" por parte de los responsables del tratamiento, ya sea en el momento de determinar los medios como en el momento del propio tratamiento. Se ejemplifican aquéllas con la seudonimización, la minimización y todo lo que sume garantías al cumplimiento del Reglamento y la protección de los derechos de los interesados.

Con respecto a la protección de datos "por defecto" (numeral 2 del citado artículo), se pone el acento en el deber de afectar solamente los datos personales necesarios a "cada uno de los fines específicos del tratamiento", obligación que se aplicará a la cantidad de datos recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad. Esta última, la accesibilidad, de especial atención en cuanto a garantizar "por defecto" que no ocurra el acceso a los datos por parte de un número indeterminado de personas físicas, "sin la intervención de la persona" concernida.

Recurrentemente, como en otros puntos también se echa mano a la posibilidad de apelar a los mecanismos de certificación previstos en el art. 42 del RGPD, como refuerzo de mayor efectividad de estas ambas exigencias.

EL DELEGADO DE PROTECCIÓN DE DATOS

Otra novedad que trae el Reglamento de la doctrina o el derecho positivo de algunos países, para extenderlo urbi et orbi (art. 37).

"Se trata de un especialista en materia de protección de datos que trabaja en conjunto con el actual responsable del tratamiento de los datos. A pesar de ser una novedad en España, en otros países de la UE ya tiene recorrido. Hasta ahora, Alemania era uno de los pocos que contaban con él. A partir de 25 de Mayo de 2018, dicha figura será obligatoria para determinadas empresas que a continuación nombraremos. Según traducción no oficial del RGPD, el delegado de protección de datos es *´una persona responsable dentro del responsable o del encargado del tratamiento para supervisar y monitorear de manera independiente la aplicación interna y el cumplimiento de las normas de protección de datos.´* El DPO puede ser tanto un empleado como un consultor externo."[21]

Como de habitual, el RGPD establece contextos específicos donde responsables y encargados deben nombrar este tipo de delegados; atención a las cualidades profesionales, conocimientos y capacidades exigidos para su nombramiento; alternativa de subordinación laboral o contrato de servicios respecto del responsable o encargado; y publicación de los datos de contacto del mismo con comunicación a la autoridad de control (art. 37).

El RGDP asigna relevancia a la "posición" de este delegado, con el propósito que el mismo no se convierta en una figura anodina (art. 38). En tal sentido se le debe garantizar una participación adecuada y tempestiva en todas las cuestiones relativas a la protección de datos de la organización; recursos necesarios para el desempeño de sus funciones acceso a los datos y operaciones de tratamiento, mantenimiento de sus conocimientos especializados, imparcialidad, rendición de cuentas al más alto nivel jerárquico, contacto con los interesados por todo lo atinente al tratamiento de sus datos y ejercicio de sus derechos. Tiene los deberes de secreto y confidencialidad. Podrá desempeñar otras funciones y cometidos, en tanto

21 *Blog FORLOPD, Especializado en L.O.P.D., Seguridad de la Información y Normas ISO. La cita fue extraída de https://www.forlopd.es/web/blog/index.php/delegado-proteccion-de-datos/*

no genere conflicto de intereses, lo que garantizará el responsable o encargado del tratamiento.

Sus funciones están establecidas en el art. 39 del Reglamento, a saber:

1. Información y asesoramiento de las obligaciones relativas a protección de datos, tanto sea al responsable o encargado, como a los empleados que se ocupan del tratamiento;
2. Supervisión del cumplimiento en tal sentido, por responsables y encargados, asignando responsabilidades, concientizando y formando al personal y auditorías intervinientes;
3. Asesorar sobre evaluaciones de impacto que se le soliciten, y supervisar su aplicación;
4. Cooperar con la autoridad de control;
5. Actuar como punto de contacto con la autoridad de control, incluyendo la consulta previa estatuida art. 36, y realizar todo tipo de consultas.

CÓDIGOS DE CONDUCTA, MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS DE PROTECCIÓN DE DATOS

Refiriéndonos a los códigos de conducta, ni que decir que ya estaban previstos en la Directiva 95/46/CE. La novedad estriba, como en muchos otros conceptos y categorías tratados en el RGPD, en la muy mayor y detenida atención que la nueva norma les asigna: toda una Sección junto con la certificación, con largos artículos conteniendo varios numerales cada uno (arts. 40 a 43). Se trata de un "supuesto de autorregulación, corregulación por ser más exactos, que puede servir, por un lado, para demostrar que las entidades que voluntariamente lo hayan suscrito cumplen con las obliga ciones impuestas por el RGPD".[22]

Además de reiterar previsiones de tono general que ya estaban en la Directiva 95/46/CE (la promoción de estos códigos por parte de las autoridades de cada Estado, legitimación de las asociaciones y organismos representativos para su elaboración), el RGPD establece sin carácter taxativo el contenido que cabe incluir en ellos.

Se establece la posibilidad de que existan órganos de supervisión de estos códigos, sin mengua de las funciones y poderes de las autoridades competentes (art. 42 del RGPD).

En cuanto los mecanismos de certificación, sellos y marcas (arts. 42 y 43 del RGPD), se trata de otra novedad. Su objeto es "Demostrar el cumplimiento de lo dispuesto en el Reglamento en las operaciones de tratamiento y permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes".[23]

Tales mecanismos serán de adopción voluntaria, por períodos máximos de tres años renovables, y pasibles de cancelación por incumplimiento. Las autoridades de control competentes tendrán competencia en su otorgamiento, pero al igual que en el caso de los códigos de conducta, está prevista la existencia de organismos con niveles de pericia suficiente que actúen también en la materia. Regirá en el punto la norma ISO/IEC 17065/2012 y requisitos adicionales que establezcan las autoridades de control (nums. 4 a 7 del cit. art.).

UNA REGULACIÓN MÁS DETENIDA EN TORNO A LAS TRANSFERENCIAS INTERNACIONALES

Las transferencias internacionales de datos ha sido tema nuclear en todos los grandes textos europeos que precedieran al RGPD. Basta ver que el Convenio 108 de 1981 contiene un capítulo sobre ello (el Capítulo III, arts.12 a 17) al que se suma el art. 2 del Protocolo Adicional de 2001; y que la Directiva 95/46/CE le dedica también un capítulo (arts. 25 y 26 que se desgrana en varios numerales).

En el RGPD la cuestión asume singular atención como lo demuestra la mayor extensión normativa que se le dedica al tema (arts. 44 a 49). Bien se expresa por ello que "Ya sólo este simple dato indica que el legislador comunitario no sólo es consciente de la importancia de las transferencias internacionales en un mundo global, sino que quiere aportar reglas más claras que las que hasta ahora venían rigiendo la materia".[24]

No es preciso insistir, ya lo expresamos al comienzo del presente estudio, en la importancia mayúscula de este sector regulatorio de la protección de datos personales para los países que no pertenecen a la Unión Europea, en particular aquéllos como el nuestro que forman parte del reducido número que cuenta con una "decisión de adecuación" a preservar.

22 *Alberto Díaz-Romeral Gómez, "XXIII. Los códigos de conducta en el Reglamento General de Protección de Datos", pág. 390. En Reglamento General de Protección de Datos... obra colectiva cit.*

23 *Ma. Rosario Heras Carrasco, "El nuevo Reglamento Europeo..." op. cit. pág. 17*

24 *José Luis Piñar Mañas, "XXV. Transferencias de datos personales a terceros países u organizaciones internacionales", pág. 428. En Reglamento General de Protección de Datos... obra colectiva cit.*

En este sentido trataremos, siempre de modo resumido, de presentar lo novedoso del RGPD respecto del régimen conformado a la luz de la Directiva 95/46/CE, advirtiendo que se trata de un conjunto normativo muy nutrido y extenso, de imposible comentario con pretensiones de exhaustivo, al menos en esta oportunidad.

El principio general en la Directiva 95/46/CE es que la transferencia será legítima si el país garantiza un nivel de protección adecuado, y de lo contrario se entenderá prohibida a no ser que opere alguna de las excepciones igualmente previstas a texto expreso, entre otras que el responsable del tratamiento ofrezca garantías suficientes de protección (arts. 25 y 26 de la Directiva).

En el RGPD se dividen las transferencias en dos grandes grupos que no requieren autorización expresa de ninguna autoridad de control: las basadas en una decisión de adecuación (art. 45), y las que se sustentan en garantías adecuadas (art. 46).

Con relación al primer grupo, se le da particular atención a través de una extensa previsión (art. 45), a la evaluación que hará la Comisión de la adecuación del nivel de protección que goce el tercer país, organización internacional, territorio o aún sectores específicos, en función de parámetros específicos (entre otros el estado de derecho y respeto de los DD.HH y libertades fundamentales vigentes en ese lugar), con las consecuencias, positivas o negativas, que ello supone.

El segundo grupo (el de las "garantías adecuadas") gira alrededor de varios casos que el RGPD acepta también como habilitantes *per se* de la transferencia.

En síntesis se amplían los supuestos legitimantes de regla de las transferencias (vale decir sin necesidad de autorización previa), agregando a la adecuación (art. 45) la posibilidad que el responsable o encargado ofrezcan garantías adecuadas (art.46), y entre estas garantías se incluyen las normas corporativas vinculantes, a las que se dedica un artículo también de mucha enjundia, sobre el cual todo ajuste normativo nacional tendrá que detenerse para su mayor análisis –como en otros tantos segmentos del RGPD- llegado el momento (art. 47).

Entre los numerosos capítulos y artículos dedicados al tema de las transferencias internacionales de datos en el RGPD, aparecen algunas excepciones novedosas que amplían las posibilidades validatorias (art. 49).

Conviene destacar que en ciertos casos, fenómeno que se repite en todo el RGPD, puede no tratarse de una novedad absoluta, pero sí de un matiz, agregado, condición, etc. que convierte lo que parecía prima facie previsto, en algo más circunstanciado y –por ende- novedoso. En punto a lo que venimos tratando, hay por lo menos dos casos de este tenor, a saber:

1. La excepción consistente en que el interesado haya prestado su consentimiento para la transferencia. En la Directiva 95/46/CE esta excepción ya estaba contemplada (art. 26 a), y con ello va su inclusión también en los regímenes europeos y extra europeos que internalizaron o asumieron esta previsión. Sin embargo, mientras que la Directiva califica de modo breve al consentimiento ("inequívoco"), el RGPD (art. 49.1 a) lo reviste de otros agregados imperativos, que convierten de tal suerte a la excepción en norma novedosa a tener presente ("explícito", "informado sobre el riesgo del caso por tratarse de una transferencia en ausencia de decisión de adecuación y garantías adecuadas").
2. La excepción relativa a la salvaguardia de un interés vital del interesado, que la Directiva ya había previsto pero sin caracterización o condicionamiento algunos (art. 26 e), mientras que el RGDP lo hace ampliando los sujetos portadores de tal interés ("interesado u otras personas"), y agregando algo que parece jurídicamente de suyo pero no estaba dicho, como es la supeditación de esta excepción a que "el interesado esté física o jurídicamente incapacitado para dar su consentimiento" (art. 49.1f).

Como novedades totales en este campo de las excepciones que habilitan transferencias pese a no existir decisión ni garantías de adecuación, entre otras tenemos las siguientes: formulación, ejercicio o defensa de reclamaciones en sentido amplio, ya no solo de naturaleza judicial (art. 49 1 e); no repetitividad de la transferencia y afectación a un número limitado de interesados (art. 49.1 segundo párrafo).

En síntesis o conclusión sobre este punto, hacemos nuestras las palabras de Piñar Mañas, cuando manifiesta que "Las decisiones de adecuación siguen siendo pieza esencial en todo el sistema de transferencias internacionales, que se extiende ahora también a las que se hagan a o desde organizaciones internacionales. Pero ahora adquieren también notable protagonismo las garantías adecuadas, y muy especialmente las normas corporativas vinculantes. Esta es, sin duda, una de las más importantes novedades del Reglamento. Novedad, hay que decirlo, no en cuanto al contenido de la regulación, que se basa en gran medida en los documentos,

opiniones y práctica del WP29, sino en cuanto a la incorporación misma de tal regulación al texto del Reglamento".[25]

LAS AUTORIDADES INDEPENDIENTES DE CONTROL

Es otra de las materias donde el RGDP muestra un abordaje de extensión considerable, a través de un amplio articulado (arts. 51 a 59) revelador de la importancia que se le asigna al tema.

A comenzar se pone el acento en la independencia de que deben gozar estas autoridades, lo que queda de manifiesto desde las enunciaciones en los títulos con las que, de un modo si se quiere insistente, se alude a este requisito (vg. "Capítulo VI, Autoridades de control independientes", "Sección 1, Independencia", "Artículo 52, Independencia").

El considerando 117 por su parte destaca este rasgo como "elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal".

Pero más allá de estas primeras evidencias, la exigencia de independencia de estas autoridades en tanto carácter nuclear de todo el régimen, se desprende de múltiples y acumuladas exigencias que práctica el Reglamento al respecto.

En orden meramente secuencial destacamos como pasibles de la mayor atención, por su novedad (relativa o absoluta), las siguientes previsiones garantistas contenidas en el RGPD:

Ajenidad completa de todos los miembros de la autoridad, de toda influencia externa, directa o indirecta (art. 52.2).

Disposición de personal propio, sujeto a la autoridad exclusiva del órgano en cuestión (art. 52.5).

Control financiero que no afecte la independencia, y disposición de un presupuesto anual público e independiente (art. 52.6).

Nombramiento de todos los miembros de las autoridades, por ley y mediante un procedimiento transparente (arts. 53.1 y 54.1.c).

Un conjunto de previsiones que deben ir por ley, dirigidas tanto a los miembros de la autoridad como a su personal, entre otras las obligaciones, prohibiciones, y cese de los mismos (art. 54.1 f).

Una larga lista de "funciones" de la autoridad (art. 57), varias de ellas novedosas por responder directamente a previsiones ex–novo del propio Reglamento como son las relativas a la adopción de cláusulas contractuales tipo (num. 1 j), elaborar y mantener la lista referida al requisito de la evaluación de impacto (num. 1 k), etc.

Refiriendo a las distintas posibilidades permitidas como órgano elector de los miembros de la autoridad (art. 53.1 del RGPD), se ha expresado lo siguiente: "Sin embargo no es indiferente quien sea el órgano que nombra a los miembros de la autoridad de control a los efectos de una mayor o menor independencia de ésta. Parece que un nombramiento por un organismo independiente o por una mayoría cualificada del Parlamento puede favorecer más su independencia –o al menos la ausencia de una única dependencia- que el nombramiento por parte del Gobierno, sin perjuicio de que este elemento no sea el más importante y de que personas nombradas por el Gobierno ejerzan o hayan ejercido sus funciones con plena independencia".[26]

El mismo autor a renglón seguido de la anterior cita pone el acento en lo que a su juicio importa más, glosando el artículo respectivo del propio RGDP: "El Reglamento sí recoge los requisitos para el nombramiento de miembro de la autoridad de control, señalando que ´cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes´ -art. 53-2-" E insiste en ello, cuando expresa "Existen, por tanto, ´unas cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de una autoridad de control´ -art. 54.1.b". Para culminar con la siguiente afirmación: "Evidentemente se trata éste de un ámbito donde existe un amplio margen de discrecionalidad y de apreciación a la hora de valorar si un candidato posee la cualificación y la idoneidad para ser nombrado, lo que limita el control jurisdiccional pero éste debe ejercerse en los supuestos que de manera clara y manifiesta el candidato propuesto no posee la titulación y la experiencia necesaria en el ámbito de la protección de de datos personales, elementos éstos más reglados que la mayor o menor aptitud de un candidato que es siempre difícilmente valorable".[27]

Como se aprecia, la garantía de independencia de la autoridad de control sigue siendo un tema delicado y de primer orden, al cual el RGPD le presta atención mayor que la Directiva 95/46/CE. Por lo cual, sin que con ello queramos decir más que lo dicho, nos parece que es un asunto que debería estar, al menos en alguno de sus pliegues,

25 *Op, cit. pág. 457.*

26 *Antonio Troncoso Reigada, obra colectiva. cit. pág. 477.*

27 *Op. cit. pág. 477.*

en la mesa de reexamen de nuestra ley, llegado el momento. Tanto sea para validar como suficiente el sistema vigente, como para reformarlo en todo o parte de lo que se entienda procedente y oportuno.

MECANISMOS DE COOPERACIÓN Y COHERENCIA

No es que no existieran en el régimen europeo aún vigente. Pero las insuficiencias de lo existente también motivaron el reforzamiento regulatorio sobre el particular.

Como factores de tal insuficiencia se señalan la variedad y desnivel de recursos y competencias al efecto de los distintos Estados miembros, así como la inseguridad jurídica proveniente de la incoherencia y en ocasiones contradicción de las decisiones que adoptan las autoridades de control. En este último aspecto se agrega que la actuación del Grupo de trabajo del artículo 29 no siempre ha conducido a una mayor coherencia en tales aplicaciones.[28]

De todos modos, la ley uruguaya no contiene previsión alguna al respecto, motivo por el cual la ocasión de revisión se presenta como muy pertinente sobre este punto.

El RGPD se pronuncia con claridad por el carácter obligatorio de la cooperación y asistencia mutua, entre autoridades de control, estableciendo procedimientos al respecto (arts. 60 y 61).

Las operaciones conjuntas incluyen investigaciones y medidas de ejecución, con participación de miembros o personal de las autoridades de control de otros Estados miembros (art. 62).

En cuanto al denominado "mecanismo de coherencia", se prevén varias situaciones donde tendrán existencia, a saber: las listas de operaciones de tratamientos supeditadas al requisito de evaluación de impacto (art. 64.1 a), las afectaciones relacionadas con los proyectos de códigos de conducta, sus modificaciones o ampliaciones (art. 64.1. b), etc.

Interesa destacar que las numerosas previsiones de este sector, como en otros segmentos del RGPD que tienen relación con la esfera internacional de la protección de datos, atienden a la competencia específica de un nuevo órgano supranacional, como es el Comité Europeo de Protección de Datos, por lo demás regulado en su organización y funciones, al cual el Reglamento dedica uno de sus más pormenorizados y extensos articulados (Sección 3 del Capítulo VII, arts. 68 a 76).

Cabe preguntarse, pues, como se hará en la región latinoamericana, y por ende en nuestro país, para atender este andamiaje normativo incrementado, en forma adecuada. Ya que no conformamos una Unión como es el caso de los europeos, que habilite de un modo fácil y directo la creación de este tipo de órganos, la interrogante queda planteada.

Atendiendo la complejidad creciente que va asumiendo el sistema global de la protección de datos personales en el mundo del que formamos parte, tarde o temprano habrá que pensar en fórmulas sucedáneas que permitan organizar la cooperación y coherencia entre las autoridades de control de la región y fuera de ella, de una manera aceptable. De lo contrario se pierde pie en la armonización y alineamiento perseguidos.

El desafío es grande, desde el momento que ya no se tratará de un "grupo de trabajo" como lo era en la Directiva 95/46/CE, sino de una estructura orgánica de mayores dimensiones y poderes de actuación que hasta ahora, como es el mencionado Comité.

¿Hasta qué punto los países latinoamericanos deben responder a las decisiones de este Comité sin violentar su soberanía, siendo como es un órgano que dispone de competencias y poderes mucho más fuertes que el Grupo de Trabajo del art. 29 de la Directiva? ¿No será el momento de adoptar cambios también fuertes al respecto en la región latinoamericana, creando alguna estructura similar?

Sin duda que este paso trasciende (pero de todos modos involucra) los ajustes que pudiera merecer nuestra ley nacional. Para dar pie a un cambio de tal porte se requeriría un tratado internacional, cuanto menos entre los Estados de la región, que de momento no existe. Queda planteada simplemente la inquietud.

RÉGIMEN DE RECURSOS, RESPONSABILIDAD Y SANCIONES

Muchos de los aspectos vinculados a los temas del título (Capítulo VIII, arts. 77 a 84 del RGPD) ya estaban desarrollados en la Directiva 95/46/CE, y por ende no representan elementos nuevos a considerar. Como ha sido de orden en todo nuestro examen, nos detendremos solamente -o con preferencia- en aquellas cuestiones nuevas que introduce el RGDP.

Se prevé la remisión obligatoria a los tribunales, del dictamen o decisión emitidos por el Comité en el marco del mecanismo de coherencia (art. 78.4). Nuevamente queda evidenciada la carencia señalada en el apartado anterior para el funcionamiento en forma de todo el sistema, con

28 *Fernando Irurzun Montoro, "XXVII. Cooperación y coherencia entre autoridades de control ", pág. 514. En Reglamento General de Protección de Datos... obra colectiva cit.*

motivo en este caso de la inexistencia del aludido Comité en la región.

Pensamos que, al tenor del art. 79.1 del RGPD, se necesitarán previsiones más específicas que las disponibles hoy día en la ley nacional, acerca de los fueros competenciales de accionamiento judicial contra responsables o encargados del tratamiento. Igual por lo que refiere a la actuación judicial mediante representante (arts. 80.1 y 80.2), punto de difícil armonización con la imperiosa, y muchas veces criticable, exigencia de presencia personal en las audiencias, que contiene el Código General del Proceso.

Si bien facultativas, el RGPD establece una serie de hipótesis de suspensión y hasta inhibición de los procedimientos judiciales donde se estén debatiendo asuntos relativos a tratamientos de datos personales, cuando actúan tribunales competentes de diferentes Estados. La cuestión plantea como mínimo la interrogante de acople a las normas de Derecho Procesal Internacional que rigen el tema en nuestro país, fundamentalmente el Título X, arts. 524 y siguientes del Código General del Proceso, donde también se estatuye la "cooperación judicial internacional" (Capítulos II y III, arts. 526 y siguientes del citado Código).

En punto al "derecho de indemnización" de quienes sufran perjuicio por infracción al Reglamento, no se aprecian cambios sustantivos, más allá del mayor detalle regulatorio del RGPD en comparación con la Directiva 95/46/CE.

En efecto, el Reglamento reitera en este punto un principio ya consagrado en nuestra ley, como es el principio de responsabilidad (art. 12 de la ley 18.331), y otros elementos que forman parte del sistema jurídico general en la materia, emanantes del Código Civil y los amplios desarrollos doctrinario-jurisprudenciales en la materia (ejemplos entre otros, la exención del art. 82.3 RGPD, y el reembolso entre co-responsables del art. 82.5 RGPD).

Sí constituye una novedad, que por lo demás requeriría ley en caso de buscar consagrarla en nuestro sistema jurídico nacional, la solidaridad activa entre responsables y encargados "a fin de garantizar la indemnización efectiva del interesado" (art. 82.4 del RGPD).

Finalmente, con relación a la imposición de multas, el Reglamento ingresa en detalles que no están previstos por nuestra ley (art. 83 del RGPD), aunque sí –en parte- por las Resoluciones 890/2010 y 320/2011 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

Del ejercicio comparativo de estas Resoluciones con las disposiciones del Reglamento europeo, surge la necesidad de una revisión –pensamos que a fondo- del régimen nacional vigente, en la medida que el RGPD organiza el tema sobre bases claramente distintas y más circunstanciadas.

CONCLUSIONES

El presente examen no tiene pretensiones ni de exhaustividad ni de postura segura y unívoca acerca de lo que debería ajustarse en el régimen nacional, fundamentalmente en la Ley 18.331 y las modificaciones que ésta ya experimentara hasta el presente, para adecuarse al Reglamento (UE) 2016/679.

Es claro que esa adecuación se impone en las actuales circunstancias, y que no debería tardar demasiado (recordemos como ya fue dicho, que el Reglamento entra en vigor el 25 de mayo de 2018).

Es claro también, que la "decisión de adecuación" de que goza nuestro país, que le habilita sin otras cortapisas o fórmulas no exentas de incógnita y burocracia, ya no será revisada a título facultativo (por lo demás nunca ejercitado) como lo fuera bajo el régimen de la derogada Directiva 95/46/CE. Por el contrario, habrá revisiones obligatorias cada cuatro años.

Y es claro, finalmente, que el mantenimiento del nivel adecuado respecto de los estándares imperantes, no es asunto de poca monta. Tanto por lo que se precia el país de mantenerse en lo alto del cumplimiento de los derechos fundamentales en toda su gama (la protección de datos personales pertenece a esta gama), como por los pragmáticos pero siempre imperiosos dictados que exige el comercio internacional, donde el respeto de estos baremos es cláusula común en los tratados y documentos afines.

Razones todas para pensar con decisión, cuidado y profesionalidad, sobre una revisión de todo el régimen nacional a la luz del nuevo RGPD. No hay que ser iconoclastas en la hora, no lo somos nosotros mucho menos. Lo construido y existente ya es mucho. Solamente que se requiere más y mejor. Para lograrlo habrá que ser atentos (no condescendientes) y perspicaces (no ramplones), para que el Derecho y la Política (en ese orden) hagan su juego al respecto. El examen realizado no es más que una pequeña e inacabada contribución al servicio de ese objetivo.

PANORAMA DE LA PROTECCIÓN DE DATOS PERSONALES

en el sector público en México

ARELI
CANO GUADIANA

Es Comisionada del INAI y Coordinadora de las Comisiones de Normatividad de Datos Personales y, de Vinculación y Promoción del Derecho en el mismo Instituto. Fue Comisionada Ciudadana del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal y Coordinadora Jurídica en la Conferencia Mexicana de Acceso a la Información Pública (COMAIP). También se desempeñó como Directora de Transparencia, Servicios y Trámites en la Delegación Miguel Hidalgo en la Ciudad de México y como Asesora Jurídica en el Instituto Electoral del Distrito Federal (IEDF). Areli Cano es licenciada en Derecho por la Universidad Nacional Autónoma de México y cuenta con estudios de maestría en Administración Pública por el Instituto Nacional de Administración Pública (INAP). Su actividad se ha centrado especialmente en temas de transparencia, acceso a la información pública, protección de datos personales, archivos y, derecho electoral y partidos políticos, de los cuales ha sido conferencista en diversos foros especializados.

SUMARIO

RESUMEN

En México la protección de datos personales en el ámbito del sector público es un derecho protegido por la Constitución Política y está regulado en la recién promulgada *Ley General de Protección de Datos en Posesión de Sujetos Obligados* (2017), la cual establece las bases generales de carácter legal, institucional y programático para el ejercicio y garantía de dicha prerrogativa en todo el territorio nacional. Este nuevo marco jurídico, se construyó a partir de la experiencia acumulada en la aplicación de la primera ley federal de transparencia del país, que introdujo la salvaguarda de la información personal como un límite al acceso a la información pública. En el presente artículo se estudia la evolución de la regulación en materia de datos personales, que rigió el ámbito gubernamental federal de 2002 a inicios de 2017, asimismo se aborda la trayectoria que en el mismo periodo tuvo el ejercicio de los llamados derechos ARCO. Además, se refiere al contexto en el que la nueva Ley General en la materia ha comenzado a desplegarse, y se señalan los puntos relevantes e innovadores contenidos en ella, y se advierten los retos a enfrentar en su implementación.

EL CONTEXTO

Las instituciones públicas mexicanas, tanto a nivel federal como local, son responsables de atender la prestación de servicios y la administración de los asuntos del Estado, lo que conlleva mantener una relación con cerca de 120 millones de individuos (INEGI, 2015). Para la realización de su quehacer cotidiano y el cumplimiento de sus fines legales, los entes públicos suelen requerir a los gobernados diversos tipos de documentación e información de carácter personal, que es inscrita y resguardada en múltiples soportes físicos y electrónicos: expedientes, bases de datos, padrones, directorios, resoluciones, historiales.

Entre la información captada, por ejemplo, se encuentra la referente a la identidad de las personas (nombre y apellido), a su patrimonio (ingresos y egresos económicos, cuentas bancarias), estado de salud (detección y atención de enfermedades, consumo de estupefacientes), trayectoria académica (calificaciones, certificados, reconocimientos) y laboral (datos sobre ingreso, permanencia y promoción a un cargo o empleo). Instituciones como el Sistema de Administración Tributaria, entidad federal responsable de la captación de impuestos, cuenta con un padrón con poco más de 59 millones de contribuyentes; el Seguro Popular y el Instituto Mexicano del Seguro Social, habilitadas para la seguridad social y prestación de servicios salud, tienen cerca de 55 y 62 millones de afiliados, respectivamente.

Otro de los sectores públicos que atiende a un gran número de personas es el educativo. Tan sólo en el actual ciclo lectivo hay 25 millones de niñas, niños y adolescentes inscritos de educación básica, cantidad a la que se debe sumar a los estudiantes de los niveles medio y superior, por ejemplo, la máxima casa de estudios del país, la Universidad Nacional Autónoma de México, tiene una matrícula vigente de 350 mil alumnos.

También cabe mencionar al padrón electoral, ya que su información es fundamental para la organización y dar certeza a los procesos electivos del todo el territorio nacional. Este cuenta con 86.5 millones de ciudadanos inscritos, quienes tienen la posibilidad de tramitar su credencial para votar con fotografía y, de esta manera, poder ejercer plenamente sus derechos políticos, habilitándolo como elector, pero también como aspirante a un puesto de representación popular. Además, este documento es uno de los principales medios de identificación en el ejercicio de otros derechos o el uso de servicios prestados por particulares.

Desde el enfoque de las políticas públicas, puede mencionarse *PROSPERA Programa de Inclusión Social*, el cual constituye la herramienta más importante de combate a la pobreza de la actual administración, caracterizada principalmente por hacer transferencias monetarias en beneficio de los integrantes de 6.6 millones de familias en dicha situación[1].

Como puede observarse a partir de las cifras anteriores, las instituciones en México hacen un tratamiento amplio de datos personales, el cual, hasta hace apenas algunos lustros se realizaba bajo regulaciones y procedimientos definidos por las propias instancias a partir del criterio de los servidores públicos en turno, en los que podía tener cabida la discrecionalidad y la arbitrariedad. Esto significó la proliferación de tantas maneras para proceder a la recolección y procesamiento de datos personales como entidades integrantes del Estado mexicano.

Tal forma de proceder comenzó a modificarse gracias al reconocimiento de los datos personales como un ámbito de protección, motivado, entre otras circunstancias por un contexto en el que las nuevas tecnologías han cobrado gran importancia en la vida cotidiana, incluida la del sector público, debido a la gran capacidad que tienen para almacenar, procesar, resguardar y transmitir diversos volúmenes de información, los cuales se encuen-

1 *Información actualizada al primer trimestre de 2017.*

tran en potencial riesgo debido no sólo a su gran valor político y social, sino también por el económico intrínseco a ellos. (Murillo de la Cueva y Piñar Mañas, 2009: 58).

Esta realidad demanda el fortalecimiento de las salvaguardas que los individuos tienen al proporcionar su información personal, cuyo flujo es significativo y en torno al cual existe una especial preocupación, como bien lo muestra la reciente *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2016 (ENAID)*[2].

De acuerdo a este documento, el nombre y algún apellido (99.5%), la dirección o domicilio (97.5%), el número de teléfono personal (81.8%), y el estado civil (73.8%), son los aspectos que con mayor frecuencia se suministran a las instituciones públicas. En un nivel intermedio se encuentra el estado de salud (51.4%), el correo electrónico (42%), y el monto del sueldo (25.6%); y en menor medida las creencias religiosas (13.9%); número de cuenta o tarjeta del banco (7.1%) y ;opinión política (4.5%). Si bien la mayoría de los encuestados manifestó tener preocupación respecto al mal uso que pudiera hacerse de este tipo de información, resulta positivo que el 55% manifestó que conoce o ha escuchado sobre la existencia de una ley encargada de garantizar la protección de datos personales.

Estas cifras son significativas porque, además de expresar la percepción que se tienen respecto al tema, revelan que el derecho a la protección de datos personales está permeando en la población, pese a ser de reciente configuración, como se mostrará a continuación, el cual se espera cobre mayor importancia conforme se atiendan los retos que enfrenta la aplicación de la nueva Ley General en la materia.

EL MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS EN MÉXICO

El derecho a la protección de los datos personales, al igual que los denominados de acceso, rectificación, corrección y oposición (ARCO), están previstos en la Constitución Política, así como la obligación de las entidades públicas de su promoción, respeto, protección y garantía. A su vez, establece las bases mínimas de la organización y funcionamiento de los órganos garantes de esta prerrogativa, los principios bajo los cuales se conducirán, mismas que se aterrizan en disposiciones a nivel nacional mediante tres legislaciones:

- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010)**
- **Ley General de Transparencia y Acceso a la Información (2015)**
- **Ley General de Protección de Datos en Posesión de Sujetos Obligados (2017)**

Estas normas son producto de tres reformas constitucionales (2007[3], 2009[4] y 2014[5]), que reconocen el derecho a la protección de datos y establecen las bases generales orientadas a garantizar su ejercicio en todo el país, en condiciones similares. Asimismo, a través de ellas se capitaliza el desarrollo normativo derivado de la aplicación de la ***Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental***[6] (LFTAIPG) aprobada en el año 2002, cinco años antes de la primera mención constitucional de la prerrogativa. Esta norma pionera (abrogada en la actualidad), introdujo la obligación de garantizar la integridad de los datos personales en posesión de las instituciones del ámbito federal, que incluye a los poderes Ejecutivo, Legislativo y Judicial, a los órganos constitucionales autónomos y demás entidades del mismo orden.

2 *Esta encuesta fue realizada por el Instituto Nacional de Estadística y Geografía con el objetivo de conocer el grado de conocimiento, percepciones y actitudes que influyen en el ejercicio de los derechos de acceso a la información y protección de datos personales.*

3 *El artículo sexto fue modificado con la finalidad de homologar el derecho a saber en todo el territorio nacional, y en los distintos órdenes de gobierno. Como parte de esta reforma, se introdujo el imperativo de que la información concerniente a la vida privada y a los datos personales deberá ser protegida; y la facultad de los individuos de acceder a los mismos y solicitar su rectificación.*

4 *Se reconoce de manera expresa en el artículo 16, el derecho a la protección de datos personales, al igual que las prerrogativas de acceso, rectificación, cancelación y oposición en la materia, también conocidos como derechos ARCO; ello a efecto de "dotar al gobernado de un poder de disposición y control" sobre la información personal que le concierne, conocido también como autodeterminación informativa. A su vez, se precisa que la seguridad nacional, las disposiciones de orden público, la seguridad y salud públicas o la protección de derechos de terceros, son las causas que podrán invocarse para restringir esta prerrogativa.*

5 *Reforma en materia de transparencia que amplió las bases generales que rigen el ámbito del acceso a la información, mediante el establecimiento de instancias, instrumentos y procedimientos de alcance nacional, a fin de garantizar el ejercicio de este derecho de manera homogénea en todo el país. Asimismo, se crea el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), como máxima autoridad en la materia, al cual se le dota de autonomía al igual que al conjunto de organismos garantes análogos estatales; e incorpora a nuevos sujetos obligados: partidos políticos, sindicatos y particulares que reciban y ejerzan recursos públicos o realicen actos de autoridad.*

6 *Esta legislación fue abrogada por la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación, publicada el 9 de mayo de 2016 en el Diario Oficial de la Federación. Las disposiciones relativas a la protección de datos personales, estuvieron vigentes hasta la publicación de la Ley General de Protección de Datos personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017 en el Diario Oficial de la Federación.*

Desde la formulación de la Ley de Transparencia, la protección de los datos personales era concebida como un límite al derecho de acceso a la información. En la exposición de motivos de la iniciativa de ley[7], se precisa que la publicidad de la información debía respetar el derecho a la privacidad correspondiente a los datos personales de cualquier individuo, y en tanto se emitiera la ley de la materia, se proponía su regulación en un mismo cuerpo jurídico.

La LFTAIPG definió por primera vez a los datos personales como los concernientes a una persona física, identificada o identificable, lo que incluye aquella información que afecte su intimidad. Adicionalmente, prescribió las obligaciones de las autoridades en la materia, consistentes en crear procedimientos para atender las solicitudes de la población para el acceso y corrección de datos, y que su tratamiento fuera adecuado, pertinente y no excesivo en relación con los fines fijados e informar a los individuos sobre los propósitos de ello; procurar que los datos personales sean exactos y actualizados, caso contrario sustituirlos, rectificarlos o completarlos de oficio, y adoptar las medidas necesarias encaminadas a garantizar su seguridad para evitar su alteración, pérdida, transmisión y acceso no autorizado. Asimismo, otorgó al órgano garante, en ese entonces denominado Instituto Federal de Acceso a la Información (IFAI), la atribución de emitir los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, en posesión de la Administración Pública Federal (APF).

Las anteriores disposiciones fueron complementadas en el **Reglamento** de la Ley, en donde se detallaron las obligaciones de las dependencias y entidades federales en la materia. Asimismo, se estableció el deber de hacer público en el sitio de internet de las instituciones los sistemas de datos personales con los que cuenten, e indicar su objeto, el tipo de información contenida y uso, así como la unidad administrativa y el nombre del responsable de su administración. Cabe advertir que esta normativa especificó el procedimiento de acceso y corrección de datos personales, además señaló que las resoluciones de las dependencias podían ser impugnables a través del recurso de revisión interpuesto ante el IFAI.

Ante la ausencia de una ley específica en materia de protección de datos, en aras de cubrir los vacíos normativos y procedimentales, el entonces IFAI emitió en 2005 los ***Lineamientos de Protección de Datos Personales***[8], bajo el supuesto de que el derecho a la información consagrado en la Carta Magna comprendía la prerrogativa del individuo a tener acceso a la información sobre sí mismo que obra en bancos de datos y a que los mismos no fueran manejados de manera indebida. Esta normativa detalló las políticas generales y procedimientos con el objetivo de asegurar a la población la posibilidad de decidir en relación al uso y destino de su información personal, el adecuado tratamiento de los mismos e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado. Asimismo, delinearon las condiciones y requisitos mínimos a observar en el manejo y custodia de los sistemas de datos en posesión de la APF, para la cual resultaban prescripciones de carácter obligatorio.

Otro aspecto aportado por esta regulación es la enumeración de las características que debían darse en el tratamiento de los datos personales, es decir, que éste sea exacto, adecuado, pertinente y no excesivo; al igual que la incorporación de los principios a observarse en la misma materia: licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión. También reguló el proceso de transmisión de la información y el funcionamiento de los Sistemas de Datos Personales, así como las medidas de seguridad a adoptar. Estos lineamientos, además de establecer las obligaciones de los sujetos obligados, normaron las atribuciones del IFAI en la aplicación y verificación del cumplimiento de los mismos.

La relevancia de esta regulación radicó en que sus disposiciones permitieron efectuar el ejercicio del acceso y corrección de datos personales de los últimos once años, al hacer efectivas las prescripciones previstas en la ley de transparencia y su reglamento. Además, su aplicación hizo que el tema permeara en el sector público, pues la experiencia generada ha sido capitalizada en el impulso y orientación de la configuración de otras normas

7 *El 30 de noviembre del 2001, el gobierno federal presentó ante la Cámara de Diputados, la Iniciativa de Ley Federal de Transparencia y Acceso a la Información. Esta propuesta fue promovida por un colectivo plural de la sociedad civil denominado "Grupo Oaxaca", cuyos integrantes provenían de diversos medios de comunicación de carácter nacional y local, asociaciones civiles e instituciones académicas, emitieron una declaración en la que proponen la creación de una Ley de Acceso a la Información Pública, en la que se reconozca el derecho "a acceder a datos, archivos, registros y todo tipo de dato informativo en manos de los órganos del Estado y empresas privadas que reciben recursos públicos, conforme a los estándares democráticos internacionales en la materia".*

8 *Los lineamientos están conformados por 44 artículos, organizados en los siguientes siete capítulos: I. Disposición general; II. Principios rectores de la protección de los datos personales, III. Del tratamiento, IV. De la transmisión; V. De la Seguridad de los Sistemas de Datos Personales; VI. Del Sistema Persona; VII. Del Instituto.*

de diverso calado, como las reformas constitucionales y la creación de leyes específicas en la materia tanto a nivel federal como local. Toda esta regulación perdió su vigencia a finales de enero de 2017, a partir de la publicación de la ***Ley General de Protección de Datos en Posesión de Sujetos Obligados***.

COMPORTAMIENTO DEL EJERCICIO Y GARANTÍA DE LA PROTECCIÓN DE DATOS (2013-2017)

En México la población ha mostrado un significativo interés sobre la protección de sus datos personales en posesión de instituciones públicas, lo cual se puede constatar a través de las 311,524 solicitudes que han sido presentadas ante los sujetos obligados del ámbito federal en los últimos catorce años; es decir, desde que esta esfera de la vida privada comenzó a ser protegida por la primera Ley Federal del Transparencia. Las cifras registradas en ese amplio periodo tiempo también dan cuenta de que el tema ha permeado en los distintos grupos de la sociedad, aunque el ejercicio de la prerrogativa se ha concentrado más en algunas instituciones y sectores gubernamentales, y entidades de la República mexicana.

Solicitudes para el ejercicio de los derechos ARCO

En principio, es de destacar el sostenido crecimiento que se ha verificado en el número de peticiones de derechos ARCO, las cuales en promedio son presentadas 22 mil al año. Si bien en 2014 y 2015 la cantidad fue inferior a la reportada en 2012 y 2013, cabe advertir que la misma es superior a las registradas en años anteriores. Además, en la mayoría de los casos las personas han considerado satisfactorio la atención de sus requerimientos, pues sólo en el 3.5 de los casos, han tenido que recurrir ante el INAI al considerar no cumplidos sus puntos petitorios.

Número de solicitudes para el ejercicio de los derechos ARCO presentadas a los sujetos obligados del orden federal 2003-2017*

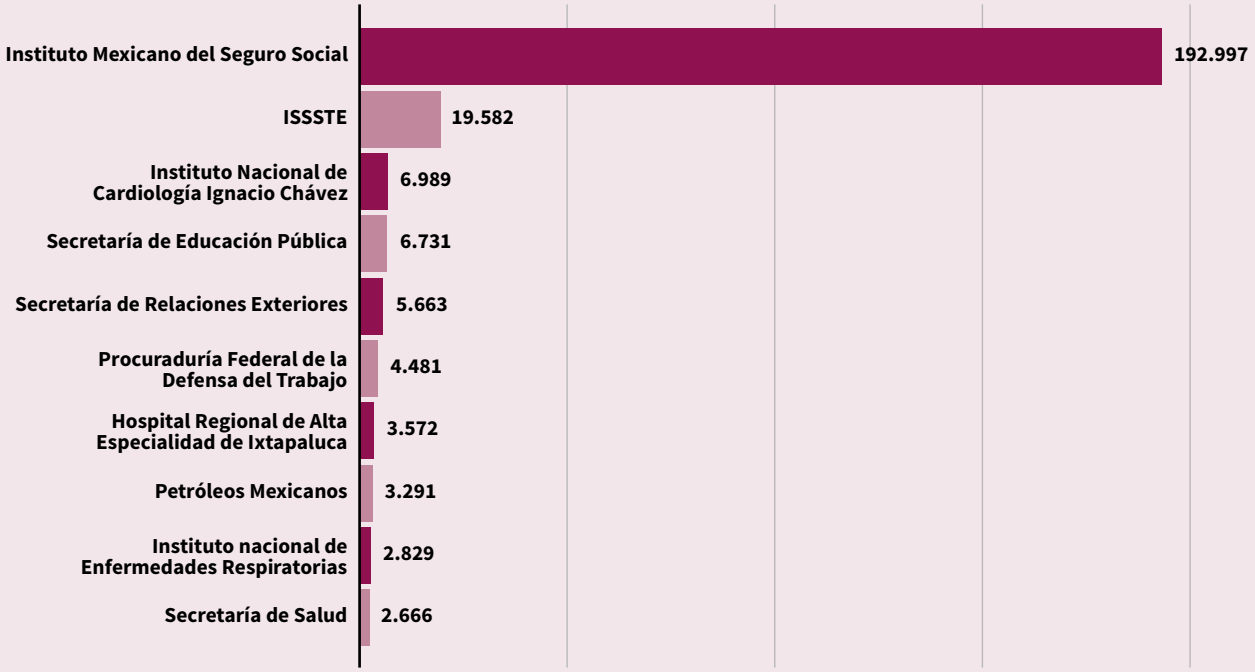
**Información del 12 de junio de 2003 al 30 de abril de 2017. Elaboración propia, con datos proporcionados por las diversas áreas del INAI.*

Es altamente probable que siga incrementándose la formulación de este tipo de requerimientos, ello conforme vayan entrado en vigencia las disposiciones, procedimientos e instrumentos de política pública previstos en la nueva Ley General en la materia, para lo cual se tiene como plazo junio del 2018. También es posible que la población tenga mayor interés en dirigirse a los diversos sujetos obligados (entre los que se encuentran los de reciente incorporación, es decir, los partidos políticos, fideicomisos y fondos públicos), dada la disponibilidad de distintas modalidades para ejercer sus derechos ARCO, como lo son la vía telefónica, Plataforma Nacional de Transparencia y la presencial. Adicionalmente, las instituciones tienen la obligación de proveer medios y procedimientos de fácil acceso, con la mayor cobertura posible, en los que se considere el perfil de los titulares; al igual que la de promover una cultura de la protección de datos personales, los que incluye el ejercicio de los derechos atinentes a la misma.

Principales sectores y requerimientos hechos a través de los derechos ARCO

Una de las características del ejercicio de los derechos ARCO en México, es que la mayor parte de las solicitudes son presentadas ante dependencias de los sectores de la seguridad social y la salud, seguidas por las de la educación, el trabajo y las relaciones exteriores.

Los 10 sujetos obligados del orden federal con mayor número de solicitudes de derechos ARCO 2003-2017*



**Información del 12 de junio de 2003 al 30 de abril de 2017. Elaboración propia, con datos proporcionados por las diversas áreas del INAI.*

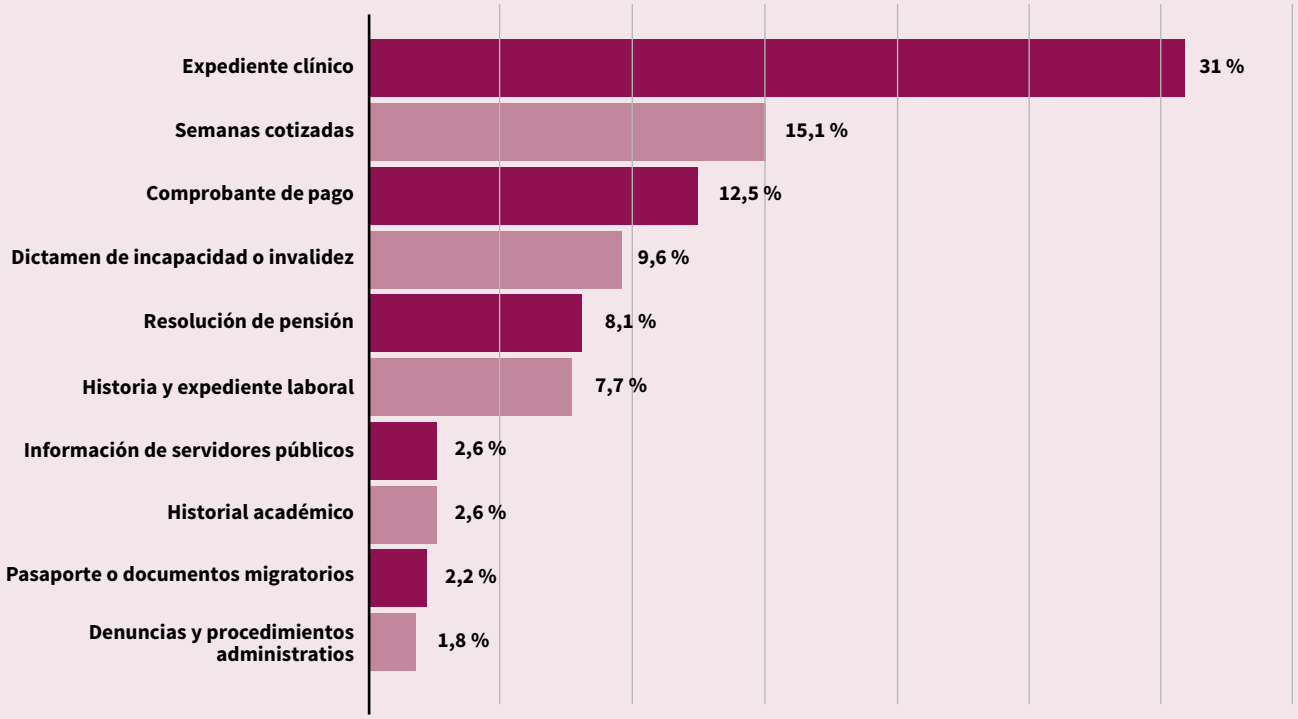
De las más de 311 mil solicitudes generadas en materia de derechos ARCO en todo el ámbito federal en los últimos 14 años, diez sujetos obligados concentran el 83%, aunque es de destacar que tan sólo una de ellas, el Instituto Mexicano del Seguro Social, reúne el 62%. Además, si se agrupan a las instituciones por sector, se tiene que la seguridad social y la salud en conjunto concentran el 77.6% del total del universo de peticiones[9], mientras la Secretaría de Educación Pública, la Secretaría de Relaciones Exteriores y Procuraduría Federal de la Defensa del Trabajo, registraron porcentajes muy

9 *El Instituto Mexicano del Seguro Social (IMSS) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), y Petróleos Mexicanos, prestan servicios de seguridad social y salud; mientras que las instituciones de salubridad son: la Secretaría de Salud, el Hospital Regional, y los institutos nacionales de Enfermedades Respiratorias y el de Cardiología.*

por debajo de los anteriores sectores, con el 2.1%, el 1.8% y el 1.4%, respectivamente.

Como consecuencia de lo anterior, se tiene que las documentos o materias registrales de mayor interés de la población son: el expediente clínico, la cotización en la seguridad social y comprobantes de pago, los cuales en conjunto representaron casi 60% de las solicitudes para el ejercicio de los derechos ARCO.

10 principales temas de las solicitudes de derechos ARCO, presentadas ante los sujetos obligados del orden federal 2003-2017*



**Información del 12 de junio de 2003 al 30 de abril de 2017. Elaboración propia, con datos proporcionados por las diversas áreas del INAI. Porcentajes calculados a partir de una muestra estadísticamente representativa con un nivel de confianza del 90% y un margen de error del 5%.*

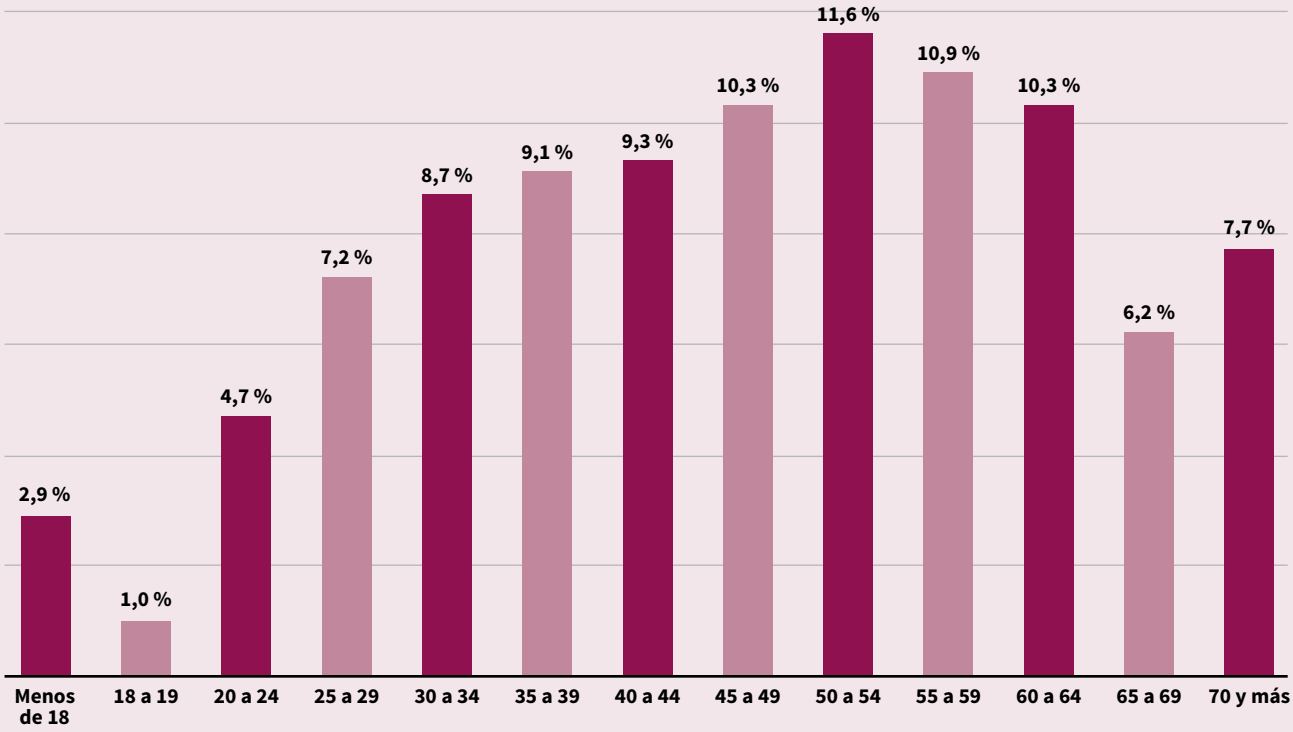
Del listado de la tabla, se puede advertir documentos vinculados con el ejercicio de diversos derechos, o a la prestación de un bien o servicio. La falta de ellos, o la presencia de errores en los mismos, puede derivar en la negativa de atención por parte de las autoridades o la de un particular, así como la presencia de otro tipo de afectaciones en la vida de las personas.

Perfil de los peticionarios del acceso a los derechos ARCO

El ejercicio de la protección de datos registrado en los últimos 14 años, da cuenta también de la forma en que esta prerrogativa ha permeado a la población mexicana, como se observa al analizar las características de los usuarios que han manifestado el rango de edad en que se ubican, su sexo, ocupación y lugar de residencia.

Al respecto, es de destacar que el 60% de los peticionarios son adultos (30 a 19 años), seguido de adultos mayores (60 años y más) y jóvenes, con el 24% y el 13%, respectivamente. Como se puede advertir, el grueso de los usuarios se ubica en un rango de edad en el que la población es económicamente activa, aunque dentro de este grupo los porcentajes más altos se registran en las personas de entre 50 y 59 años de edad. También es significativo que cerca del 3% sean personas menores de 18 años, es decir, niñas, niños y adolescentes; dado que están bajo la tutela de sus padres u otros familiares.

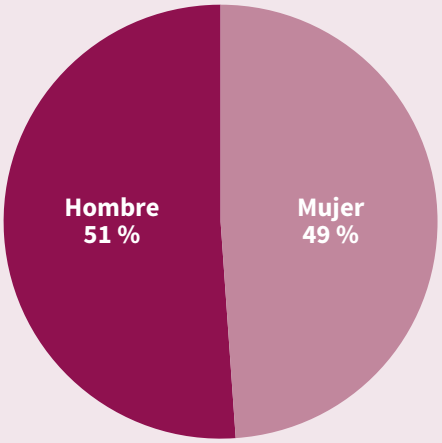
Peticionarios de derechos ARCO de los sujetos obligados del orden federal 2003-2017, por rangos de edad*



**Del total de peticiones, en un 81% de los casos, las personas se ubicaron en un rango de edad. Elaboración propia, con datos proporcionados por las diversas áreas del INAI. Información del 12 de junio de 2003 al 30 de abril de 2017.*

Otro aspecto relevante, es que el ejercicio de los derechos ARCO se da casi en la misma proporción entre hombres y mujeres[10], aunque es mayor el número de usuarias. Este comportamiento es indicativo de la transversalidad del tema, al no presentarse disparidades significativas entre los dos géneros, como todavía se observa en otros derechos, como el laboral.

Peticionarios de derechos ARCO de los sujetos obligados del orden federal 2003-2017, por sexo*

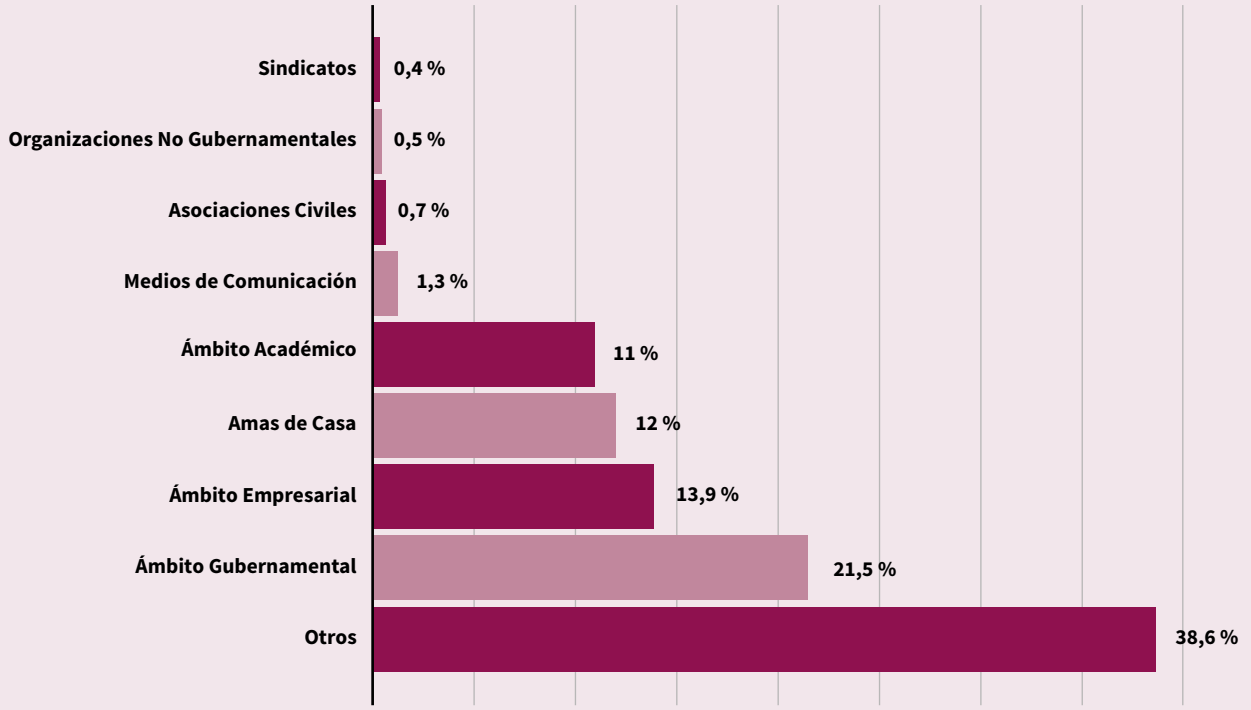


Del total de peticiones, en el 73% de los casos las personas precisaron su sexo. Elaboración propia, con datos proporcionados por las diversas áreas del INAI. Información del 12 de junio de 2003 al 30 de abril de 2017.

10 *De los 311, 524 peticiones de protección de datos ingresadas a sujetos obligados del sector público federal, sólo el 73% precisó su sexo.*

Por lo que refiere a la ocupación o el ámbito en donde se desempeñan las personas que ejercieron los derechos ARCO, se observa una evidente pluralidad, ya que ninguno representa ni una cuarta parte del total de los peticionarios. Si bien el 21.5% dijo ser del sector gubernamental, este porcentaje no se encuentra muy alejado al registrado por quienes señalaron pertenecer a los ámbitos académico, del hogar y el empresarial, los cuales cada uno representan poco más del 10%.

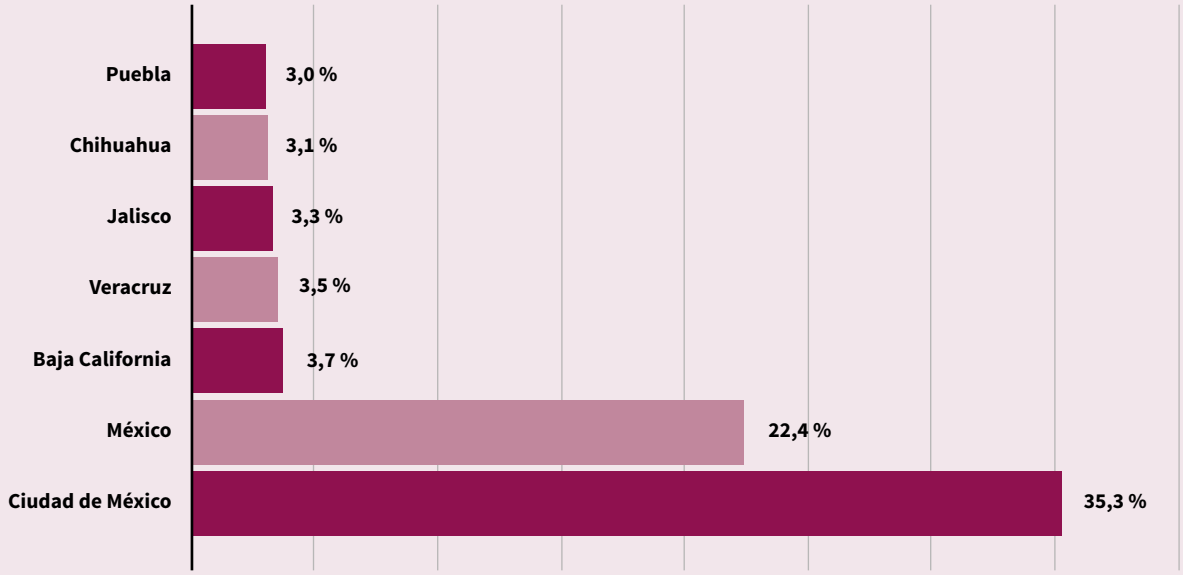
Peticionarios de derechos ARCO de los sujetos obligados del orden federal 2003-2017, por ocupación*



**Del total de peticiones, en el 69% de los casos las personas precisaron su ocupación o ámbito en el que se desempeña. Elaboración propia, con datos proporcionados por las diversas áreas del INAI. Información del 12 de junio de 2003 al 30 de abril de 2017.*

En cuanto al lugar de residencia de quienes han ejercido los derechos ARCO, más de la mitad manifestó habitar en una de las dos entidades de la República más pobladas: la Ciudad de México y el Estado de México. (INEGI, 2015).

Lugares de residencia con mayor porcentaje de peticionarios de derechos ARCO de los sujetos obligados del orden federal 2003-2017*



**Del total de peticiones, en el 99.5% de los casos las personas precisaron su lugar de residencia. Elaboración propia, con datos proporcionados por las diversas áreas del INAI. Información del 12 de junio de 2003 al 30 de abril de 2017.*

EL NUEVO MARCO DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR PÚBLICO

La reciente Ley General de Protección de Datos Personales en Posesión de Sujeto Obligados representa un paso significativo, pues, como se refirió en apartados anteriores, la única regulación aplicable a las instituciones públicas había sido la Ley Federal de Transparencia de 2002, su reglamento y los lineamientos emitidos por la autoridad en la materia. Además, su configuración tuvo varios factores a su favor. Especialmente porque capitaliza la experiencia acumulada en los últimos tres lustros tanto a nivel nacional como internacional, generada a partir del diseño de normas, procedimientos e instrumentos específicos para la protección de datos, y la aplicación de los mismos. De igual forma, incorpora diversos elementos que fueron propuestos durante el proceso legislativo, tanto por el INAI, en su calidad de órgano garante nacional en la materia, como por organizaciones de la sociedad civil y miembros de la academia.

La nueva Ley General contiene diversos aspectos relevantes y novedosos generados en la materia:

1. **Principios:** son los ejes rectores de cualquier legislación; resultan proposiciones abstractas y universales que dan razón, sustentan o fundamentan al sistema jurídico, de tal forma que ayudan a interpretar de mejor manera a la norma. En términos generales, son los que, en última instancia, se toman en cuenta para resolver todas las cuestiones en las cuales el texto de la ley es oscuro, contradictorio e insuficiente.
2. **Procedimientos:** Son los elementos que habrán de garantizar el derecho de toda persona a la protección de sus datos personales, en posesión de sujetos obligados de una manera homogénea, lo que evitará asimetrías en la forma como se da garantía a un derecho fundamental, sin importar de la entidad federativa o nivel de gobierno.
3. **Medios de impugnación:** La norma, además del recurso de revisión, incorpora un nue-

vo mecanismo de defensa llamado recurso de inconformidad cuyo objetivo es que los particulares puedan requerir la revisión de un caso local por parte del Órgano Garante nacional, esto como una alternativa administrativa que resulta más sencilla que optar como alternativa a la vía judicial, ruta que queda, por supuesto, salvaguardada a la libre elección del requirente. En conjunto, ambos recursos permiten garantizar que la actuación de las entidades públicas, se apeguen a la legalidad, a través de las resoluciones del órgano garante.

4. **Medidas de apremio y sanción:** Son elementos importantes pues aseguran el cumplimiento de las decisiones de los órganos garantes, las cuales, según el Poder Reformado, son un factor indispensable a fin de generar en los sujetos obligados la convicción de cumplir con sus obligaciones conforme a las disposiciones normativas, en los plazos y formas que son permitidas por la ley.
5. **Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT):** creado en la Ley General de Transparencia, y complementado en atribuciones por la respectiva de Datos, es la instancia que articulará los esfuerzos de los organismos garantes en la materia de todo el país, y orientará el diseño e implementación de políticas públicas, a la difusión de una cultura del derecho a la protección de los datos y al ejercicio pleno de la prerrogativa.
6. **Programa Nacional de Protección de Datos Personales (Pronadatos):** es el documento donde se determinarán los objetivos, metas y líneas de acción generales en la materia que deberán seguir los integrantes del SNT. Resulta positivo la previsión de realizar la evaluación y actualización anual de este instrumento de política pública, a fin de que sus contenidos sean realizados al año siguiente. El establecimiento de un instrumento rector en la materia, sin duda favorece la unicidad en su abordaje y en la configuración de acciones para su garantía.
7. **Buenas Prácticas:** Son resultado de la evaluación y detección de una condición con expectativa de mejorar y que se desarrollan a partir de controles de eficacia (capacidad de obtener el resultado buscado) pero con expectativa de eficiencia (lograr lo deseado con a partir de la optimización de recursos). En ese sentido, es destacable que la Ley General de Protección de Datos prevea la posibilidad de que los responsables del tratamiento puedan desarrollar o adoptar, esquemas de mejores prácticas tendientes a elevar el nivel de protección de los datos personales; armonizar el tratamiento a partir de sectores específicos; y facilitar el ejercicio de los derechos ARCO, por mencionar algunas.
8. **Portabilidad:** Esta figura fortalece el reconocimiento del derecho de los titulares a requerir a las instituciones una copia de la información objeto de tratamiento o autorizar que la transfiera a otra, en un formato electrónico estructurado y comúnmente utilizado que permita hacer uso de ella. Esta disposición es acorde a estándares internacionales desarrollados en la materia, como el *Reglamento Europeo de Protección de Datos*, que el año pasado introdujo el derecho a la portabilidad de datos en el ámbito de su competencia.

LOS RETOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La emisión de la nueva Ley General, es una muestra de la orientación progresiva que debe prevalecer en materia de derechos fundamentales. Sin duda viene a robustecer la garantía de autodeterminación informativa de las personas que proporcionan información personal a las diferentes instituciones públicas, a partir de un esquema de homogeneidad necesario para evitar dispersiones y desigualdades en el ejercicio de una libertad fundamental.

Sin embargo, cabe advertir que a partir de su entrada en vigor se configura un conjunto de desafíos para los actores institucionales involucrados con las obligaciones en ella planteadas. El más inmediato será la armonización de las normas locales en un periodo de seis meses, lo que permitirá materializar las directrices para el ejercicio pleno del derecho en todo el país, así como sentar bases claras en la relación entre las instituciones públicas y los particulares, con el objetivo de evitar la arbitrariedad en el tratamiento de su información.

Con la intención de evitar la dispersión normativa, el Constituyente Permanente, en la reforma de 2014, concibió la emisión de la Ley General como punto de partida para homologar tanto el ejercicio de la prerrogativa por parte de cualquier individuo, como los deberes de cualquier instancia de gobierno a fin de cuidar este tipo de información. En las disposiciones transitorias de la Ley se manda el referido al proceso de armonización y se especifican los plazos para ello.

Es deseable que al finalizar ese proceso, se cuente con un aparato legal nacional coherente, estructurado, homogéneo en sus bases y principios, así como en sus procedimientos, todo ello con el propósito de que las personas puedan ejercer con claridad su derecho a la protección de sus datos, a la par que a las instituciones les implica claridad de un marco normativo apegado a la Constitución dentro del cual deberán constreñir su actuación y, de esta manera, garantizar la vigencia de tan importante prerrogativa.

Otro desafío tiene que ver con la generación de condiciones políticas que propicien la incorporación de elementos en favor del ejercicio del derecho; es decir, poner en práctica el principio de progresividad que caracteriza a toda prerrogativa fundamental.

Se está ante la oportunidad de hacer de la futura reglamentación, una que pueda traducirse en parámetro nacional, por ejemplo, al incorporar plazos más cortos que, sin detrimento de la calidad en la atención, garanticen la expeditez, tanto al solicitar el ejercicio de algún derecho ARCO, como para resolver los mecanismos de inconformidad respectivos.

Estamos en una coyuntura particularmente importante para la consolidación de los derechos de las personas. Se han dado significativos avances en la protección de datos personales, creando un entorno legal sólido que en la actualidad abarca tanto el ámbito público como el privado. Esto representa una cobertura de todos los actores directa o indirectamente involucrados con el tratamiento de la información de las personas.

Bajo este contexto, el desarrollo y armonización de la normativa no solamente resulta en la configuración de un marco homogéneo en la interpretación y aplicación de los postulados constitucionales, sino que también abona en favor del desarrollo y fortalecimiento de los órganos garantes, con claridad en mandato y objetivos, facilitando así la salvaguarda de las libertades de las personas.

La amplia agenda de tareas por delante apuntalarán las libertades establecidas en nuestra carta magna. Adecuar a las instituciones garantes de la protección de datos personales, disponer de los cauces procedimentales pertinentes del ejercicio de los derechos de las personas, reforzar la promoción y difusión de los mismos, son algunas de ellas, y el INAI está dispuesto a colaborar en este quehacer, en acompañamiento con nuestros pares de las entidades federativas.

BIBLIOGRAFÍA

Declaración de Oaxaca, emitida el 24 de mayo de 2001, en la ciudad de Oaxaca. Disponible en: http://www.saladeprensa.org/art262.htm

INEGI, *Encuesta Intercensal 2015*. La información y documentos sobre la encuentra están disponibles en: http://www.beta.inegi.org.mx/proyectos/enchogares/especiales/intercensal/

INEGI, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales ENAID 2016*. La información y documentos sobre la encuentra están disponibles en: http://proyectos.inai.org.mx/enaid2016/

Murillo de la Cueva, Pablo Lucas y Piñar Mañas, José Luis, *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

Programa de Inclusión Social PROSPERA, *Familias atendidas por PROSPERA en los esquemas con y sin corresponsabilidad desagregadas por entidad federativa y tipo de localidad,* México, marzo de 2017. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/213086/Familias_atendidas_por_PROSPERA_en_los_esquemas_con_y_sin_corresponsabilidd_desagregadas_por_entidad_federativa_y_tipo_de_localidad.pdf

Reglamento Europeo de Protección de Datos. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Senado de la República, "Versión Estenográfica de las audiencias públicas con motivo de la dictaminación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", 1 de diciembre de 2015. Disponible en: http://comunicacion.senado.gob.mx/index.php/informacion/versiones/25170-2015-12-02-01-45-32.html

Sistema de Administración Tributaria, Padrón, por situación ante el Registro Federal de Causantes (actualizado a marzo de 2017). Disponible en: http://www.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page=PadronPorSitRFC.html

Solange Maqueo María, y Moreno Jimena, *Implicaciones de una ley general en materia de protección de datos personales*, México, CIDE, 2014. Disponible en: http://www.libreriacide.com/librospdf/DTEJ-64.pdf

UNAM, Portal del Estadística Universitaria. Disponible en: http://www.estadistica.unam.mx/numeralia/

Constitución Política de los Estados Unidos Mexicanos, última reforma publicada en el Diario Oficial de la

Federación, el 24 de febrero de 2017. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_240217.pdf

Decreto por el que se adiciona la fracción XXIX al artículo 73 de la Constitución Política de los Estados Unidos Mexicano, publicado en el Diario Oficial de la Federación el 30 de abril de 2009. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 1 de junio de 2009. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf

Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el diario Oficial de la Federación el 7 de febrero de 2014. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

Decreto por el que se adiciona un segundo párrafo con siete fracciones al artículo sexto de la de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 20 de junio de 2007. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_174_20jul07_ima.pdf

Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con Proyecto de Decreto por el que se Expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento6.pdf

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, última reforma publicada en el Diario Oficial de la Federación el 18 de diciembre de 2015 (Abrogada). Disponible en: http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2001 (Abrogada). Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=727870&fecha=11/06/2002

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación, el 5 de julio de 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación, el 9 de mayo de 2016. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación, el 26 de enero de 2017. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Lineamientos de Protección de Datos Personales, aprobados por el Pleno del IFAI el 27 de julio de 2005, y publicados en el Diario Oficial de la Federación, el 30 de septiembre de 2005. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=2093669&fecha=30/09/2005

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicado en el Diario Oficial de la Federación, el 11 de junio de 2003 (Abrogado). Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el Diario Oficial de la Federación, el 21 de diciembre de 2011. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

WE MUST HAVE BOTH PRIVACY AND SECURITY:

Enter Global Privacy and Security, by Design

ANN
CAVOUKIAN

La Dra. Cavoukian es reconocida como una de las expertas líderes en privacidad del mundo. Actualmente es Directora Ejecutiva del Privacy and Big Data Institute de la Ryerson University. Dra. Cavoukian cumplió tres términos como Comisionado de Información y Privacidad de Ontario, Canadá. Allí creó Privacy by Design, un marco que busca integrar proactivamente la privacidad en el diseño, logrando así la mayor protección posible. En 2010, los Reguladores Internacionales de Privacidad aprobaron por unanimidad una Resolución que reconoce Privacidad por Diseño como una norma internacional. Desde entonces, PbD ha sido traducido a 39 idiomas. La Dra. Cavoukian ha recibido numerosos premios reconociendo su liderazgo en privacidad, incluyendo ser nombrada como una de las 25 Mujeres más influyentes en Canadá, nombrada entre las 10 mujeres más importantes en materia de Seguridad de Datos y Privacidad, y más recientemente, ha sido nombrada como una de las 100 Líderes en Identidad (Enero, 2017).

SUMARIO

RESUMEN

La privacidad está actualmente bajo la lupa. Con el crecimiento de la computación ubicua, la conectividad en línea, las redes sociales, los dispositivos inalámbricos y "usables", las personas están siendo dirigidas a creer que no tienen más opción que resignarse a no tener privacidad. Pero esto no es así! Un marco de privacidad denominado "Privacidad desde el diseño" habilitará nuestra privacidad y nuestra libertad, permitiéndonos vivir bien en el futuro. Este artículo descarta la noción de que la privacidad actúa como una barrera a la seguridad pública y a la innovación. Argumenta que el paradigma limitante de "suma cero" -que puede tener o privacidad o innovación pero no ambas- es un modelo de aproximación a la cuestión de la privacidad antiguo, de ganar/perder, en la época de la vigilancia masiva de los ciudadanos. En lugar de eso, una solución de "suma positiva" se necesita cuando los intereses de ambas partes deben encontrarse, en una forma de "ganar-ganar" a través de la privacidad desde el diseño (Privacy by Design (PbD)). PbD se funda en el rechazo a las propuestas de suma cero a través de la identificación proactiva de los riesgos, y considerando embeber las medidas de protección necesarias en el diseño y arquitectura de datos involucrados. La Dra. Cavoukian recientemente congregó un nuevo Consejo Internacional, extendiendo PbD a Privacidad y Seguridad Global desde el Diseño, para responder a las presiones crecientes de los modelos de suma cero que buscan hacer avanzar la seguridad a expensas de la privacidad. Digan NO a estos modelos de ganar/perder. Ella detalla como las organizaciones pueden embeber la privacidad y la seguridad en virtualmente cualquier sistema u operación para alcanzar resultados de suma positiva, ganar/ganar, permitiendo la coexistencia de privacidad y seguridad, ninguno a expensas del otro.

ABSTRACT

Privacy is presently under siege. With the growth of ubiquitous computing, online connectivity, social media, wireless and wearable devices, people are being led to believe they have no choice but to give up on privacy. But this is not the case! A privacy framework called Privacy by Design will enable our privacy and our freedom, to live well into the future. This paper dispels the notion that privacy acts as a barrier to public safety and security and innovation. The paper argues that the limiting paradigm of "zero-sum" – that you can either have privacy or innovation, but not both – is an outdated, win/lose model of approaching the question of privacy in the age of massive surveillance of citizens. Instead a "positive-sum" solution is needed in which the interests of both sides may be met, in a doubly-enabling, "win-win" manner through Privacy by Design (PbD). PbD is predicated on the rejection of zero-sum propositions by proactively identifying the risks and embedding the necessary protective measures into the design and data architecture involved. Dr. Cavoukian recently convened a new International Council, extending PbD to Global Privacy and Security, by Design, to respond to the growing pressures of zero-sum models seeking to advance security at the expense of privacy. Say NO to such win/lose models She outlines how organizations can embed privacy **and** security into virtually any system or operation to achieve positive-sum, win/win outcomes, enabling both privacy **and** security – not one at the expense of the other.

INTRODUCTION

The importance of privacy cannot be overstated. Our essential freedoms and liberty rest upon a foundation of privacy. Indeed, history has demonstrated that privacy is the first thread to unravel as a free and democratic state morphs into a totalitarian state. As long as we value liberty—we must also value privacy. For these reasons, we must take every opportunity to reflect on the advances made around the world[1] and celebrate each successive development to enshrine in the principles of law and generally accepted doctrines, the right to the protection of personal data as inherent to human being. While acknowledging these global trends in privacy law, it is on this particular occasion that we take heed of the work of the Regulatory and Control Unit of Personal Data (RCUPD) in Uruguay during its data protection week and their 9 years of approval of the Law No. 18,331, Personal Data Protection and Habeas data. Moreover, it was in 2010 that this law was provided the decision of adequacy from the Working Party 29, making it one among a minority of jurisdictions to receive such approval.[2]

1 *Greenleaf, Graham, Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. Available at SSRN: https://ssrn.com/abstract=2000034*

2 *European Commission. Article 29 Data Protection Working Party. Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay. October 12, 2010. [accessed April 30, 2017 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf]*

Ever since the tragic events of 11 September 2001 and the terrorist acts that have followed, however, privacy has been increasingly cast as an antagonist of public safety.[3] This zero-sum, win/lose paradigm of privacy versus public safety is not only wrong, it is extremely dangerous and must be brought to an end. It is dangerous because, in the tension between privacy and public safety, privacy will always lose, and this loss will directly endanger not only freedom but the prosperity that we enjoy as a free and open society. The remedy to overcoming this zero-sum paradigm is a positive-sum, win/win model, where relevant systems are designed with both objectives in mind.

PRIVACY BY DESIGN

The emergence of *PbD* as the new generation of privacy protection invites the development of innovative approaches to promoting and enshrining it in instruments of various kinds, including regulatory ones. The time is ripe for this kind of innovation. Over the past several years, momentum behind *Privacy by Design (PbD)* has been steadily growing. It is increasingly becoming a "basic principle" of data protection.[4] Global and local businesses alike are starting to implement the 7 Foundational Principles of *PbD*, with mounting interest among regulators and policy-makers in enshrining these principles in privacy policies and frameworks, around the world.[5]

In November, 2009, a prominent group of privacy professionals, business leaders, information technology specialists, and academics gathered in Madrid to discuss how the next set of threats to privacy could best be addressed. The event, Privacy by Design: The Definitive Workshop, was co-hosted by my office when I served as Commissioner and that of the Israeli Law, Information and Technology Authority. It marked the latest step in a journey that I began in the 1990's, when I first focused on enlisting the support of technologies that could enhance privacy.

The late 1990's was a time when privacy protection relied primarily upon legislation and regulatory frameworks—in an effort to offer remedies for data breaches, after they had occurred. As information technology became increasingly interconnected and the volume of personal information collected began to explode, it became clear that a new way of thinking about privacy was needed. Unlike some critics, who see technology as necessarily eroding privacy, we have long taken the view that technology is inherently neutral. As much as it can be used to chip away at privacy, its support can also be enlisted to protect privacy.[6] In this way one can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive. This approach serves to minimize the unnecessary collection, use and disclosure of personal data, and to promote public confidence and trust in data governance.[7]

Just as regulatory approaches proved to be necessary but not sufficient 20 years ago, we can see now that Privacy-Enhancing Technologies are necessary but not sufficient to protect privacy and provide a foundation of trust well into the future. That is why the concept of Privacy by Design extends to a trilogy of encompassing applications: 1) IT systems, 2) accountable business practices, and 3) physical design and networked infrastructure.

Of course, having the role of a Commissioner tasked with overseeing privacy laws, I did not want to suggest that Privacy by Design should be applied in a vacuum. It is a critical part—but only a part of a suite of privacy protections that brings together regulatory instruments, consumer awareness and education, accountability and transparency, audit and control, and market forces.

Privacy by Design seeks to proactively embed privacy protective measures into the design of information technologies, networked infrastructure, and business practices in an effort to prevent privacy harms and data breaches from arising. Privacy by Design is a model of prevention, before the fact: by identifying potential risks proactively, the necessary measures can be embedded into programs and IT to prevent the harms from arising—bake privacy-protective measures into the code, into the data architecture, resulting in positive-sum, win/win solutions. A key step is strong security, which is featured as an essential component: while privacy subsumes a much broader set of protections than security alone, if you don't lead with strong security, end-to-end, with full lifecycle protection, you will never have good privacy.

Given that privacy revolves around personal control over one's data, we must strive to have

3 *I use the term public safety as an all-encompassing term that includes the necessary security measures to bring it about.*

4 *Peter Hustinx, Privacy by design: delivering the promises. Privacy by Design Issue of Identity in the Information Society*

5 *[insert the FTC, GDPR here – I believe you have the references in your ppt]*

6 *Cavoukian, Ann. Privacy by Design ... Take the Challenge. Office of the Information & Privacy Commissioner of Ontario, 2009.*

7 *Cavoukian, Ann. "Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum. Not Zero-Sum." Office of the Information & Privacy Commissioner of Ontario, 2008.*

both privacy and security in equal measure. We need not give up on privacy, we simply need to embed it in design along with security.

PRIVACY AND SECURITY BY DESIGN

To say that privacy and public safety cannot co-exist is simply incorrect. However, the fear of terrorism, as tangible as it is, is overtaking the dissemination of the message that we can have both privacy *and* public safety, without sacrificing the efficacy of one for the other. Therefore, I believe we must expand our efforts relating to the exposure of the messaging of Privacy by Design. So, I am asking those of you who value freedom, privacy, prosperity, security, and public safety to join me in spreading the word—that you can indeed have privacy *and* functionality.

I ask technologists to join me in thinking outside the box—to develop methods that will deliver both privacy and public safety; privacy and data analytics. Likewise, I ask policy-makers, lawyers, and politicians—anyone interested in preserving our freedoms and prosperity—to join us in this endeavor. The vehicle for this nascent movement is the newly created International Council on Global Privacy and Security, by Design (GPS by Design), which, by necessity, must be international in nature since data no longer resides within one's borders. The Mission of GPS by Design is to dispel the commonly held view—held by governments, businesses, the media, and the public at large—that one must choose between privacy and public safety.

Our goal is threefold. First, to educate politicians, businesses, the media, and the public that we can and must engineer systems to protect both privacy and other interests. We can do this by using, for example, innovative technologies, such as recently developed advances in artificial intelligence, machine learning, blockchain, and homomorphic encryption. We must do this because the loss of privacy to surveillance will not only undercut our freedoms, but the prosperity resulting from a society of innovators. "Civilization is the progress towards a society of privacy," wrote Ayn Rand, in *The Fountainhead*, and the loss of privacy is the regression of a society toward an uncivilized society, lacking in freedom. Our second goal is to foster technology innovation in academic institutions around the world that will allow privacy and public safety, as well as privacy and business interests, such as big data and data analytics, to be achieved without sacrificing either. Third, we wish to develop policy templates that will articulate how privacy is to be applied in the new digital age for different government and business segments and the oversight under which these institutions should fall. These policy templates will be important in the development of new, doubly enabling, positive-sum technologies. This is a call to action.

In this day and age of growing fears over terrorist attacks, we cannot forfeit our privacy and, in turn, our freedom and prosperity, to these escalating fears. Law enforcement's approach to access to personal information can raise significant concerns for the public and regulators, particularly if privacy is not addressed from the outset. It is acknowledged that there are two very important values at play regarding law enforcement access to personal information. Individuals should be free from government tracking unless necessary for public safety, and law enforcement should have sufficient access to personal information when it is necessary to protect public safety. We must demonstrate that we can have both privacy and public safety, otherwise our freedom and prosperity will be forfeited, which is simply too high a price to pay.

A SEISMIC SHIFT

There has been a tremendous shift in the balance of power from the individual to the state. Part of this shift has been the government's ability to access a wide range of information about individuals. In the last 40 years, this access has been greatly assisted by advances in technology. But now, because of new technology, this balance of power has a chance of shifting back toward the individual. As a result, governments are growing increasingly concerned and want to prevent this from happening. Encryption technology has now revamped the playing field, wherein governments can no longer readily access personal information at will, as a result of end-to-end encryption. This, in turn, has led to calls by law enforcement for the creation of "backdoors" into encrypted content, which can lead to far greater surveillance. In addition, the introduction of the Internet of Things will create the opportunity for even more subversive surveillance that will widely blanket society. As a result, we as a society are at a nexus. Governments have been fear-mongering, essentially saying that the "terrorist sky will fall upon us" unless they have complete control and access to more personal information. But the evidence suggests otherwise. The failure to stop terrorist attacks, from 9/11 to the present-day San Bernandino/Brussels attacks, has not been the consequence of too little information; it has been the consequence of not connecting the dots with

the existing information that law enforcement and intelligence agencies had already acquired and was in their possession through legitimate means. The evidence suggests that governments largely possess the means to prevent such attacks using tried and true techniques and, if they focus on using and sharing the information they already possess more effectively, without violating individual privacy or mandating insecure encryption. The latter will only serve to strip law abiding citizens of their privacy and the security of their online communications and transactions. Despite these facts, the commonly held view is that privacy is the polar opposite of public safety or business interests, whose enhancement undercuts the effectiveness of the latter two objectives. This is referred to as a *zero-sum game*, whose either/or, win/lose tension can only be addressed by the victory of one objective, always to the detriment of the other. Unfortunately, this is one of the most damaging paradigms in existence in the present day cyber age. It will directly detract from our prosperity and freedom as a society.

LOOKING BACK

New technology can create unique challenges for individual privacy rights and provide novel complications for regulators looking to preserve both privacy rights and technological innovation. Society has long puzzled over how best to design regulatory frameworks that balance privacy rights and emerging technologies. Indeed, as early as 1890, when newspaper and photograph technologies were beginning to ascend, legal scholars called for added privacy protections, including enshrining those rights in the criminal law. Protecting privacy, a "right most valued by civilized men," while still promoting innovation, has never been more challenging than it is in an increasingly online and technology focused world.

Protecting privacy, a "right most valued by civilized men," while still promoting innovation, has never been more challenging than it is in an increasingly online and technology focused world. Now, more than ever, information can cross many nations' borders in a mere instant, and consumers' movements and activities can be tracked through their computers and mobile phones. At the same time, technological innovations can improve lives, increase public safety, build wealth, and promote efficiencies in how we use scarce resources. Just as there is value in information to researchers, marketers, corporations, and governments, there is an equally important value in privacy to the individual. Consequently, managing privacy and technological innovation is important to the global economy and is best addressed by a comprehensive and flexible approach.

In the last century, we have enjoyed tremendous prosperity arising from massive innovation. It was thought that this prosperity arose as a result of unencumbered freedom and the absence of onerous regulations on innovators. But this prosperity was also a result of privacy and minimal levels of surveillance. Prior to the 1980s, today's technologies of surveillance had largely not been invented. An individual's privacy was, for the most part, secured by default—often through practical obscurity. But since then, the technologies developed have lent themselves to assisting surveillance on a grand scale. The type of surveillance developed targeted not only terrorists and criminals but all individuals, including law abiding citizens. Our argument is that privacy is at the root of both freedom and prosperity. It is the prosperity of a society that allows the products of innovation to be shared by all members, including those in the lower socio-economic strata. Smartphones, for example, enhance the lives of both the rich and the poor, but perhaps even more important, innovations in transportation, health care, the arts, smart appliances, and communications are enjoyed by all, making our quality of life far better than that of our parents and grandparents only a few generations earlier. Innovation is what makes it all happen—but what makes innovation happen? Just look around the world. The most innovative societies also happen to be the most free and privacy protective. Freedom and privacy form the foundation, the very bedrock, of innovation. So what is the connection to privacy?

Innovation requires taking risks and being able to think differently, at times contrary to the existing memes prevalent in a given culture. At times, this may require being on the "edge," or perhaps even going over the edge—thinking far outside the box, so to speak. It requires that an individual's mind shed any barriers to imagination, either self- or externally imposed, because innovations arise from the very crystallization of that imagination. Accordingly, we want to enable wild and sometimes crazy imaginative ideas—ideas that may initially fail, but, with greater effort, become the future products of innovation for both commerce and the arts. If I am constantly being watched—continuously surveilled, and all of my activities are monitored and stored for future data mining and assessment, or perhaps to establish a profile of me, of my life, or my edgy predilections (even though lawful)—then in effect, consciously or subconsciously, I will focus on being watched,

and instinctively, I will modify my behavior. But it goes much further than that. The government, through its warnings to be vigilant about potential terrorist acts, and the media, broadcasting constant reminders that things are getting worse, with "talking heads" arguing that we need to give up "some" of our privacy, instill yet more fear and anxiety in society. This is compounded by the government saying that to prevent us from getting potentially "blown up," they must watch and surveil our activities even more. Under such conditions, our cognitive processing will be limited to, at best, a few contexts associated with anxiety and, most likely, fear. We will be less likely to be able to draw upon contexts that may lead to creative imagination and innovation. The reason for this is largely due to our subconscious, which greatly influences our conscious experience of thoughts and reality—in this case, a reality that relates to the anxiety of knowing that we are constantly being watched while, at the same time, fearful of being in danger of getting blown up. This is one of the unfortunate consequences of the state we are in and the surveillance that it engenders. The tragedy of Stasi Germany was a vast psychological experiment that provided strong evidence of this fact (resulting in present-day Germany becoming the leading privacy and data protection country in the world, saying "never again"). We evolved to be wary of the watchers, and that behavior in humans, in direct response to such surveillance, inhibits the ability to allow our imaginations to soar and enter the vistas of true creativity and innovation. There will be individual differences no doubt, but we believe that the level of innovation as a society will drop considerably over the next generation as a result. Privacy means that I am free to voluntarily expose my thoughts and activities as I so choose in whatever areas I wish. As such, I still retain the open vistas of my mind—there is no fear or anxiety that serves to limit my cognitive bandwidth, leaving me open to imagine ideas that potentially extend well beyond the current reality.

PRIVACY AND PUBLIC SAFETY

But what about security and public safety? Don't we have to give up some privacy to remain safe? No, this is precisely the overbearing paradigm that will ultimately destroy all freedom and prosperity in our society, and the overwhelming tragedy is that it is false. We evolved to be wary of the watchers, and that behavior in humans, in direct response to such surveillance, inhibits the ability to allow our imaginations to soar and enter the vistas of true creativity and innovation. privacy, and freedom without sacrificing or needing to "balance" one of these interests against another. It is ludicrous to think that a society of innovators cannot develop systems that protect both public safety and privacy.[8] This is the type of thinking that arises from a perspective of fear. It results in accepting the status quo of ignorance.

Unfortunately, the reality is that most government agencies, public media, and society have bought into this zero-sum view of thinking. It is the prevailing view held by most governments, politicians, and businesses alike, being treated as a given. That is why we see public polling that favors public safety, always at the expense of privacy. But privacy versus public safety is not a fact of reality; it is a meme that has pervaded our culture because of bad information, ignorance, and, especially, fear. The reality is that this view of privacy versus public safety harms both. For example, law enforcement and intelligence agencies engage in broad fishing expeditions in an attempt to find the needle in the haystack while creating a trove of false positives. This is not effective public safety because law enforcement resources must be used, and, in effect, wasted, to filter through millions of false positives based on the billions of data records collected.

Privacy is clearly harmed since more of an individual's activities may be monitored without the necessary probable cause/warrant rationale. But also, in some cases, public safety is harmed since, in trying to balance against privacy, the necessary steps and precautions to protect society may not be taken, all in the name of privacy, in which case, zero-sum harms both privacy and security. If we are to survive as a free and prosperous society, we must replace the zero-sum meme with positive-sum messaging, which will allow us to be serious about building innovative systems that integrate both privacy and public safety, without either one being compromised, allowing us to achieve doubly enabling solutions. This mind shift in society can only be accomplished through massive education and raising of awareness. It rests in the design of the systems and the technologies that we put into place. The former represents a win/lose, zero-sum paradigm—privacy versus public safety—that, over time, degenerates into a negative sum, lose/lose proposition. The latter represents a win/win, positive-sum framework, wherein the interests of both privacy and public safety may be reflected.

8 *See the paper on Operationalizing Privacy by Design (Cavoukian, 2012).*

THE BIG CHALLENGE

Law enforcement officials have significant public safety-related duties. Privacy is not meant to stand in the way of the proper fulfilment of these responsibilities. At the same time, taking a zero-sum approach, where privacy is sacrificed in the interests of security, should not and cannot be the default option. The zero-sum paradigm is the view that we wish to dispel. In my previous role as Information and Privacy commissioner of Ontario, Canada we demonstrated countless ways in which this could be achieved, leading to positive, win/win outcomes. Here's to the end of zero-sum paradigms and a future filled with privacy, security, freedom, innovation, and prosperity!

INICIATIVAS LEGISLATIVAS SOBRE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

o Projeto de Lei 5.276/2016

DANILO DONEDA

Danilo Doneda es Licenciado en Derecho por la Universidad Federal de Paraná y Doctor en Derecho Civil por la Universidad Estatal de Río de Janeiro. Es profesor universitario en la Universidad Estatal de Río de Janeiro. Es miembro del consejo asesor de privacidad de los Grupos de Privacidad Global de las Naciones Unidas y del consejo consultivo de InternetLab y del Proyecto de Niños y Consumo (Instituto Alana). Fue Coordinador General del Departamento de Protección al Consumidor y Defensa del Ministerio de Justicia así como del Comité Directivo Brasileño de Internet (Brasil). Doneda fue profesor en la Universidad Estatal de Río de Janeiro (UERJ), Pontificia Universidad de Río de Janeiro (PUC-Rio), UniBrasil y Fundación Getulio Vargas (FGV). Fue investigador visitante en la Autoridad Italiana de Protección de Datos (Roma, Italia), Universidad de Camerino (Camerino, Italia) y en el Instituto Max Planck de Derecho Comparado e Internacional Privado (Hamburgo, Alemania). Es autor de libros y artículos sobre derecho civil, derechos digitales, privacidad y protección de datos.

LAURA SCHERTEL MENDES

Laura Schertel Mendes es profesora adjunta de la Universidad de Brasilia (UnB) y del Instituto Brasiliense de Derecho Público (IDP). Es Doctora summa cum laude en derecho privado por la Universidad Humboldt de Berlín, Magister en "Derecho, Estado y Constitución" por la UnB y graduada en derecho por la UnB. Es directora de la Asociación Luso-Alemana de Juristas (DLJV-Berlín) y directora financiera del Instituto Brasileño de Política y Derecho del Consumidor (Brasilcon). Tiene experiencia en las áreas de derecho civil, derecho del consumidor y derecho constitucional, actuando principalmente en los siguientes temas: derechos de la personalidad, protección de datos personales, derecho e internet, interfaz entre derecho constitucional y derecho civil, así como políticas públicas en la Sociedad de la Información. Gestora Gubernamental en ejercicio en el Consejo Administrativo de Defensa Económica - CADE.

SUMARIO

RESUMEN

El artículo analiza los principales aspectos de la Ley 5276 de 2016 – Ley de Protección de Datos-, una cuestión no regulada aún en Brasil por una ley general. Luego de varias consideraciones acerca de sus antecedentes históricos y legislativos, el artículo se enfoca en las caracerísticas generales y únicas de la Ley y, luego, comenta algunas de las cuestiones principales de ésta, tales como la definición de dato personal e identificadores electrónicos, los conceptos de datos anónimos y datos sensibles, la noción de interés legítimo, cuestiones vinculadas a la seguridad de la información y violaciones de datos, flujos transfronterizos de datos y competencias de la autoridad de protección de datos.

RESUMO

O artigo analisa os principais aspectos do Projeto de Lei n° 5276 de 2016, sobre proteção de dados pessoais, tema ainda não tratado pelo ordenamento brasileiro na forma de uma lei geral. Após verificar aspectos dos contextos histórico e jurídico da proteção à privacidade e dados pessoais no Brasil, destaca-se o caráter geral e unitário da lei proposta para, a seguir, traçar o perfil geral de alguns dos temas abordados pelo projeto, como a definição de dado pessoal e os identificadores eletrônicos, os conceitos de dados anônimos e dados sensíveis, a noção de legítimo interesse, os tópicos de segurança da informação e vazamento de dados, a transferência internacional de dados e as competências de uma autoridade de proteção de dados.

ABSTRACT

The article analyses the main aspects of the Bill 5276 of 2016 - the Data Protection Bill - a matter that isn't regulated in Brazil by a general law as of yet. After some considerations about its historical and legal background, the article stresses the general and unified characteristics of the Bill and, afterwards, comments on some of the main issues present on the Bill such as the definition of personal data and electronic identifiers, the concepts of anonymous data and sensitive data, the notion of legitimate interest, issues on information security and data breach, transborder data flows and the competences of a data protection authority.

INTRODUÇÃO E CONTEXTO

No dia 11 de maio, após mais de 5 anos de debates, o Projeto de Lei de Proteção de Dados Pessoais foi encaminhado pelo Poder Executivo para o Congresso Nacional, sendo recebido na Câmara dos Deputados como o PL nº 5.276/2016. Tendo passado por duas consultas públicas (nos anos de 2010 e 2015) que obtiveram mais de 2000 contribuições da academia, sociedade civil, empresas e setor público, trata-se de uma proposta compatível com os padrões atuais da legislação internacional sobre a matéria e em harmonia com a proteção da pessoa no ordenamento jurídico brasileiro e com a consolidação de uma verdadeira agenda digital no país.

O Brasil não conta em seu ordenamento jurídico com uma legislação de caráter geral sobre proteção de dados pessoais. Projetos de lei sobre este tema tramitam nas duas casas legislativas: no Senado Federal, o Projeto de Lei 330, de 2013, e na câmara dos Deputados, além do mencionado PL 5.276/2016, tramita desde 2012 o PL 4060 - sendo que os projetos na Câmara encontram-se no momento (maio de 2016) apensados e sob análise da Comissão Especial de Tratamento e Proteção de Dados Pessoais (CETPDP). Considerando que o PL 5.276/2016 é, dentre os projetos de lei sob análise, o mais detalhado e minucioso, examinaremos seus aspectos principais.

O PL 5.276/2016 visa concretizar o direito fundamental à privacidade e proteção de dados pessoais, indispensável para o exercício da cidadania, da autodeterminação informativa e da proteção da dignidade da pessoa humana na sociedade contemporânea, caracterizada pelo uso cada vez mais intenso de informações por entes públicos e privados. Neste cenário, o cidadão, nos seus mais diversos papéis sociais - como contribuinte, paciente, trabalhador, beneficiário de programas sociais ou como consumidor - tem seus dados processados diuturnamente. Uma combinação de técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos e a construção de verdadeiros perfis virtuais, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais, criando uma demanda por instrumentos capazes de contrabalancear possíveis abusos.

A revolução das tecnologias da informação e comunicação apresenta complexos desafios ao direito contemporâneo. Infraestruturas de comunicação e informação perpassam hoje todos os aspectos da vida, o que levou à criação do conceito da onipresença ou ubiquidade dos meios informáticos *(ubiquitous computing)*. Especialmente a digitalização, os sistemas informáticos e a conectividade em rede são responsáveis por essa ubiquidade: *smartphones*, web semântica, *cloud computing* são algumas expressões que representam esse fenômeno que, com a ligação em rede de um sem-número de objetos e dispositivos preconizada pela

internet das coisas, tende a se tornar uma realidade cada vez mais concreta. Associado à ampliação das formas de comunicação pessoal e pública, de mobilização social, de representação da personalidade e de circulação de conhecimento, ampliam-se as formas de controle social, de exposição indesejada, de discriminação e de restrição à liberdade individual. Para enfrentar esses desafios cumpre estabelecer, por meio da edição de uma lei geral de proteção de dados pessoais, uma arquitetura regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro pólo de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo independente, responsável pela implementação e aplicação da legislação. Sem isso, pode-se comprometer tanto a segurança jurídica das atividades empresariais que envolvam o processamento de dados, como a tutela da personalidade dos indivíduos.

FUNDAMENTOS

Nesse sentido, o PL nº 5.276/2016 é extremamente apropriado para essa finalidade, por estabelecer um marco normativo geral sobre proteção de dados pessoais, cujo âmbito de aplicação abrange os setores privado e público, diante dos quais o cidadão deve possuir a prerrogativa de proteção de seus dados pessoais. Seu ponto de gravitação é a pessoa; os dados pessoais são o eu objeto e a sua finalidade é a proteção da personalidade seja em qual situação seja necessário, ao garantir a privacidade, a liberdade, igualdade e livre desenvolvimento da personalidade em vista do tratamento de dados pessoais em qualquer ocasião que seja necessário. Ao se propor centrada na pessoa, a proposta estabelece regras para o tratamento de dados pessoais independente de qual seja o setor que os trate - seja por ente público ou privado, por empresa de uma área ou de outra, o que lhe assegura a característica de lei geral e unitária. Este é um ponto fundamental da proposta, visto que eventuais variações do nível de proteção a dados pessoais em vista de determinados setores acabam por gerar insegurança ao cidadão, que teria direitos diferenciados em relação a seus dados quando tratados por entes diferentes, além de fulminar a eficácia da lei como um todo, visto que o grande fluxo de dados pessoais a que hoje assistimos faz com que seja comum a transferência destes de um setor a outro, o que torna tanto mais relevante a uniformidade de regras para cada setor como um pressuposto da eficácia dos direitos e garantias presentes na proposta.

Não obstante, o projeto estabelece exceções à aplicação da lei, como para a utilização de dados para fins exclusivamente pessoais ou então para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos. Esta segunda exceção à aplicação da lei, em particular, reconhece a necessidade da manutenção de um espaço livre para a utilização de dados pessoais para fins relacionados a interesses de ordens específicas e de natureza pública e que eventualmente poderiam ser potencialmente prejudicados caso submetidos ao regime padrão da proposta, podendo, eventualmente ser restringida a alçada da liberdade de expressão e o direito à informação. Tais exceções, no entanto, somente se justificam caso o tratamento de dados esteja relacionado exclusivamente com estas finalidades e não permite a utilização das informações pessoais para quaisquer outros fins.

O PL estrutura-se em torno de princípios gerais que orientam toda a sua disciplina, quais sejam: os princípios da finalidade, livre acesso, transparência, necessidade, segurança, qualidade dos dados, prevenção e não-discriminação. De extrema relevância é a previsão do consentimento livre e informado como requisito para o tratamento legítimo de dados pessoais, em consonância com a idéia do livre controle do indivíduo sobre os seus dados pessoais. Há também outros casos específicos para a legitimação do tratamento, como nos casos em que há legítimo interesse do responsável pelo tratamento ou quando os dados pessoais forem necessários para a execução de um contrato. Ainda, o projeto de lei atribui aos cidadãos os direitos de acesso, retificação, oposição, bloqueio, cancelamento e dissociação sobre seus próprios dados; além de prever que a tutela dos direitos e garantias deverá ser realizada com o auxílio de uma autoridade competente.

DEFINIÇÕES. DADOS PESSOAIS.

De acordo com o seu Art. 5º, I, dado pessoal é o *"dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa [...]."* O Inciso III do referido artigo define o que são dados sensíveis: *"dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos".*

O conceito de dados pessoais proposto no PL 5.276/2016 - entendido como aquele que permite identificar a pessoa natural - é adequado e apto para possibilitar que a lei atinja o seu objetivo principal, qual seja, o de proteger a pessoa contra os riscos derivados do processamento de dados

pessoais na sociedade da informação. Além disso, o conceito está em consonância com as legislações internacionais sobre proteção de dados pessoais. Nesse sentido, cabe mencionar a definição presente no Regulamento Geral de Proteção de Dados Europeu, de 27 de abril de 2016, em seu art. 4°, 1, que conceitua dados pessoais como "informação relativa a uma pessoa singular identificada ou identificável". O dispositivo prescreve que é "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

A informação pessoal difere de outras informações por possuir um vínculo objetivo com a pessoa, isto é, por revelar aspectos que lhe dizem respeito. Desse modo, resta claro que tais informações merecem tutela jurídica, uma vez que, por terem como objeto a própria pessoa, constituem um atributo de sua personalidade. Fundamental é perceber que tal tutela visa à proteção da pessoa e de sua personalidade e não dos dados *per se*.

Como se sabe, por meio do processamento eletrônico de dados possibilitado pelas tecnologia da informação contemporânea, dados que se referem a uma pessoa determinada ou determinável podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, os riscos para o cidadão.

Desse modo, percebe-se que a informatização dos meios para o tratamento de dados pessoais afetou o direito à privacidade do indivíduo principalmente por duas razões: i) ao ampliar a possibilidade de armazenamento, tornando-a praticamente ilimitada; ii) ao possibilitar a obtenção de novos elementos informativos por meio da combinação de dados em estado bruto, a princípio, desprovidos de importância, a partir da utilização de novas técnicas, tais como o *"profiling"*, *"data mining"*, *"data warehousing"*, *"scoring-system"*, entre outros.

Conforme afirmou o Tribunal Constitucional alemão no famoso julgamento que consolidou o direito à autodeterminação informativa (1983), a partir das possibilidades de combinação e processamento da tecnologia da informação, "um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados insignificantes no contexto do processamento eletrônico de dados".[1] Isso explica porque o campo de aplicação da lei deve abarcar um conceito amplo e objetivo de dados pessoais, entendido pela possibilidade de vinculação do dado à pessoa, independente dos dados se referirem a aspectos íntimos e privados ou públicos e notórios. Dessa forma, são considerados dados pessoais tanto os dados relativos à comunicação privada, correspondência, endereço e telefone da pessoa, como dados referentes a opiniões políticas, opção religiosa, hábitos, gostos e interesses da pessoa - enfim, qualquer informação que possa ser ligada à pessoa.

Os avanços no processamento automatizado de dados pessoais são, muitas vezes, abordados do ponto de vista quantitativo - isto é, em relação ao grande volume de dados que é passível de tratamento, das inúmeras fontes que passam a ser acessíveis e relacionadas, e assim por diante. O que nem sempre salta aos olhos é o fato de que à esta mudança quantitativa, soma-se uma nova perspectiva qualitativa em relação aos dados pessoais: considerada a ampla possibilidade de que cada fração de informação sobre uma pessoa possa ser cruzada, relacionada ou agregada com outras informações, passa a fazer menos sentido um modelo que mensure o grau de risco potencial para a pessoa em relação ao tratamento de sua informação a partir somente ou predominantemente da natureza da informação pessoal tratada. E é justamente neste sentido que, a partir da noção que já estava presente no julgamento do Tribunal Constitucional alemão de 1983, é cada vez mais claro que fragmentos aparentemente inócuos de informação pessoal não possam ser desconsiderados ou relativizados em uma regulação de proteção de dados, dado que contextualmente possam ter importância impossível de ser antecipada em uma mera avaliação de sua natureza, pois os efeitos de seu tratamento somente serão produzidos quando consideradas as demais informações disponíveis sobre uma pessoa.[2] Assim, não assiste razão à desconsideração de determinadas categorias de dados

1 *BVerfGE 65, 1, "Recenseamento" (Volkszählung). MARTINS, Leonardo. (org.) Cinqüenta anos de Jurisprudência do Tribunal Constitucional federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245.*

2 *WEINGARTEN, Elizabeth. "There's No Such Thing as Innocuous Personal Data", in Slate, 8 de agosto de 2016, disponível em <http://www.slate.com/articles/technology/future_tense/2016/08/there_s_no_such_thing_as_innocuous_personal_data.html>*

da abrangência da definição de dados pessoais (como eventualmente se pretende com a categoria de "dados cadastrais"), tanto pela necessidade de manter a coerência com a definição básica de dados pessoais (os dados que se referem a pessoa identificada ou identificável, disposição presente no ordenamento brasileiro no artigo 4º, IV da Lei 12.527 de 2011, Lei de Acesso à Informação), como pela impossibilidade de, *a priori*, avaliar os efeitos para a pessoa decorrentes do processamento de uma determinada informação.

Discussão interessante dá-se igualmente em torno do endereço de IP. Ele seria um dado pessoal ou não? Nesse contexto, importa mencionar a doutrina alemã, que destaca ser o dado pessoal um conceito relativo: nas situações em que for possível vincular um dado a uma pessoa determinada ou determinável, como é o caso em que o endereço de IP acaba por proporcionar o acesso a inúmeras outras informações pessoais, o IP pode ser considerado dado pessoal. Isso acontece, por exemplo, sob a perspectiva do provedor de acesso, que possui outras informações contratuais, que permitem a vinculação do endereço de IP ao usuário da máquina que se conectou à internet. Em diversas outras situações, o endereço do IP não levará à identificação do usuário da máquina, não podendo, portanto, ser considerado dado pessoal. Tal interpretação está em consonância com a parte final do art. 5º, I, do PL 5.276, que considera dado pessoal "inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa"

DADOS SENSÍVEIS

Questão importante diz respeito ao conceito de dados sensíveis, presente em diversas legislações de proteção de dados pessoais. O debate acerca dos dados sensíveis acompanha a história da proteção de dados e esteve presente desde o início das discussões acadêmicas e iniciativas legislativas sobre o tema[3]. Já em 1973 a lei nacional de dados pessoais da Suécia abordou a questão dos dados sensíveis, sendo seguida por França (1978), Dinamarca (1978), Noruega (1978) e Luxemburgo (1979).[4]

A diferenciação da categoria dos dados sensíveis foi consagrada pelo Convênio 108, editado pelo Conselho da Europa, em 1981, em seu art. 6°.[5] O Convênio previu, em seu dispositivo voltado às "categorias especiais de dados", que os dados pessoais relativos à origem racial, saúde, vida sexual e condenações penais somente poderiam ser objeto de tratamento, caso o direito interno previsse as garantias adequadas para o seu processamento.[6]

O estabelecimento de um regime especial para os dados sensíveis está presente na legislação da maioria dos países europeus e na Diretiva Européia 95/46/CE e continuou a ser regulado por meio do Regulamento Geral de Proteção de Dados Europeu (art. 9º).

Quanto ao conceito de dados sensíveis previsto no PL 5.276, esses devem ser entendidos como "os dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos".

Como se percebe, parece haver um consenso de que o tratamento de dados sensíveis acarreta riscos e, portanto, merece uma atenção especial do legislador. Mas quais são, de fato, os dados sensíveis e por que eles precisam de uma maior proteção?

Uma análise das normas internacionais mencionadas e da redação do dispositivo proposta pelo PL 5.276, é possível inferir que os países estabeleceram nas suas legislações uma lista exemplificativa de dados de caráter especial ou sensível, com o objetivo de lhes garantir uma proteção mais adequada. Embora as listas variem de país para país, há várias categorias que se repetem, como os dados relativos à origem racial, vida sexual e convicções religiosas e políticas. Desse modo, para os fins de sistematização dogmática, pode-se afirmar que a categoria dos dados sensíveis está relacionada à percepção de que o armazenamento, processamento e circulação de alguns tipos de dados podem se constituir em um risco maior à personalidade individual, especialmente, se utilizados com intuito discriminatório. Os dados referentes à raça, opção sexual, saúde e religião, são exemplos desse tipo.

Tal perspectiva permite realçar as discussões acerca da violação da igualdade material em um contexto em que a privacidade somente era vista sob a ótica da autonomia e da liberdade. Desse modo, passa-se a considerar também os abusos decor-

3 *SIMITIS, Spiros. „Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion. In: BREM (Hrsg.), Festschrift zum 65. Geburtstag von Mario M. Pedrazzini, 1990, p. 469.*

4 *Idem, Ibidem.*

5 *HIGUERAS, Manuel Heredero. La Directiva Comunitaria de Protección de los datos de carater personal. Aranzadi Editorial, 1997, p. 116 e 117.*

6 *Art. 6°, Convenção 108 do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. O texto pode ser acessado em: http://www.cnpd.pt/bin/legis/internacional/Convenca0108.htm (acesso em 29.02.2012)*

rentes do tratamento dos dados pessoais como um problema de igualdade, sempre que sua inadequada utilização acarretar ações potencialmente discriminatórias. Exemplo disso é a discriminação racial realizada com base em dados pessoais, também denominada de *racial profiling*, em que bancos de dados com perfis étnicos ou raciais são utilizados para fundamentar determinadas decisões.

Uma análise acurada do PL 5276 permite identificar quais as consequências para um tratamento de dados pessoais, quando os dados são considerados sensíveis:

1. ampliação das exigências para a validade do consentimento do indivíduo sobre a disposição de seus dados pessoais: o PL passa a exigir o consentimento expresso, livre e informado, mediante manifestação própria e distinta da manifestação de consentimento relativo ao tratamento de outros dados pessoais;
2. ampliação das exigências legais para o tratamento desses dados pelo responsável: os interesses legítimos do responsável (art. 7º, IX) e a execução de um contrato (art. 7º, V) não legitimam o tratamento de dados sensíveis, embora sejam hipóteses válidas para o tratamento de dados pessoais em geral.
3. aumento do controle pela autoridade administrativa para a autorização de armazenamento, processamento e circulação dos dados sensíveis (vide art. 12 do PL).

Deve-se destacar que, além da proteção especial reservada aos dados definidos expressamente no PL 5276 como sensíveis, é fundamental proteger também outros dados que, embora aparentemente insignificantes, podem vir a se tornar sensíveis, a depender do tipo de tratamento a que são submetidos. Trata-se na realidade, de um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias. Exemplo desse fato são as listas negras, que constituem registros criados pelos empregadores para agregar o nome dos trabalhadores que acionaram a Justiça do Trabalho, serviram como testemunhas ou que por qualquer outro motivo não sejam bem vistos por algumas empresas. Tais listas são utilizadas com a finalidade de dificultar o acesso ao mercado de trabalho das pessoas cujo nome estava registrado. O Tribunal Superior do Trabalho (TST) tem reconhecido reiteradamente o direito à indenização por dano moral em razão de inserção do nome do trabalhador nessas listas.

Dessa forma, destaca-se que o conceito de dados sensíveis, nos moldes previstos no PL ora analisado, é de suma relevância para a proteção da pessoa contra os riscos de discriminação decorrentes do processamento de dados na sociedade da informação. No entanto, esse rol não é exaustivo, podendo abarcar outros dados que venha apresentar potencial discriminatório, a depender do contexto em que a informação pessoal for utilizada. Neste sentido, o PL reconhece claramente a possibilidade de que o tratamento de dados que, embora em si não se caracterizem como sensíveis, possa proporcionar discriminação ao seu titular por meio do chamado tratamento sensível, especificamente no § 1º do art. 11. Este dispositivo funcionaliza o princípio da não-discriminação, mencionado no art. 6º, IX, ao especificar situação na qual um regime específico é dispensado ao tratamento sensível de dados por conta do seu potencial discriminatório.

O INTERESSE LEGÍTIMO

Dentre as hipóteses que autorizam o tratamento de dados pessoais, o PL 5.276/2016 inclui os interesses legítimos do responsável ou de terceiro (art. 7°, IX). A hipótese de tratamento de dados pessoais baseada nos interesses legítimos do responsável ou de terceiro é relevante, ao reconhecer que outras partes – além do próprio titular - podem ter interesses protegidos juridicamente no processamento, uso ou circulação de determinadas informações, como é o caso, por exemplo, do tratamento de dados pessoais realizado pelo empregador para o controle dos seus empregados.

Ocorre que tal cláusula não deve ser lida como uma válvula de escape geral, a partir da qual qualquer tratamento de dados pessoais passa a ser autorizada. Para que não se incorra nesse erro, dois aspectos devem ser considerados. Em primeiro lugar, o art. 7º, IX, impõe a realização pelo responsável – ou da autoridade competente, se for o caso - de uma ponderação de interesses e de direitos, a partir da qual se decidirá se há ou não interesse legítimo do responsável. Vejamos a redação da parte final dispositivo: "quando necessário para atender aos interesses legítimos do responsável ou de terceiro, **exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais"** (grifo nosso). Fica claro, portanto, a necessidade de um balanceamento de interesses; na hipótese de prevalecerem os direitos do titular, o tratamento de dados baseado nesse dispositivo não está autorizado. O segundo aspecto consiste na norma prevista no art. 10 do PL, que prevê inúmeros requisitos para o tratamento baseado nos interesses legítimos: i) a adoção de medidas para garantir a

transparência do tratamento baseado nessa hipótese e a possibilidade de o titular manifestar oposição ao tratamento; ii) a estrita necessidade como critério de legitimidade do tratamento de dados baseado nesse requisito e a necessidade de anonimização quando possível; iii) possibilidade da autoridade requisitar impacto de privacidade. Esse dispositivo é fundamental para a adequada aplicação da cláusula do legítimo interesse. Uma eventual interpretação por demais ampla da cláusula do legítimo interesse acabaria por descreditar a própria regra, além de pôr em xeque a sua constitucionalidade, por violação ao direito fundamental à intimidade e vida privada.

DECISÕES AUTOMATIZADAS

O PL 5.276 garante uma série de direitos ao titular dos dados pessoais, como portabilidade e eliminação, a qualquer momento, dos dados pessoais coletados. Além disso, a lei confere ao titular a possibilidade de solicitar revisão de decisões tomadas com base no tratamento automatizado de seus dados pessoais.

O direito de não se ficar sujeito a uma decisão individual automatizada consiste no direito do cidadão de não ficar submetido a decisões que influenciem significativamente a sua posição jurídica, tomadas exclusivamente com base no tratamento automatizado de dados.

Norma semelhante pode ser encontrada da Diretiva Europeia 95/46/CE de proteção de dados, em seu art. 15, 1: "Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento". Tal regra constitui uma proibição geral referente a decisões automatizadas, podendo ocorrer apenas em duas hipóteses, conforme a Diretiva: desde que existam medidas adequadas que garantam a representação e expressão do titular dos dados para a sua defesa ou que ocorra no âmbito da celebração ou execução de contratos.

O art. 13º, no. 1, da Lei de Protecção de Dados de Portugal estabelece também norma nesse mesmo sentido: admite-se que os dados armazenados de forma automatizada possam ser utilizados para ajudar uma tomada de decisão, v.g. fornecendo mais informação, ou seguindo a atuação apropriada, mas os computadores e os dados que armazenam não devem ser utilizados como único meio para fundamentar determinada decisão.

O art. 20 do PL 5276 é de extrema importância, pois garante uma regra de justiça, que visa assegurar a possibilidade de defesa do titular e a mínima participação do titular em um processo de decisão tomado com base em seus dados e que afetará de forma significativa as suas oportunidades de vida.

Deve-se ressaltar que igual norma já existe em relação ao cadastro positivo, pois a Lei 12.414/2011 prevê em seu art. 5º, VI, o direito do titular de "solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados". Essa norma reveste-se de importância central quando aplicada ao sistema de avaliação de risco (credit scoring), pois possibilita ao consumidor a revisão de uma "nota" ou "valor" inadequado, que lhe foi atribuído com base em dados equivocados, desatualizados ou que não poderiam ter sido armazenados.

SEGURANÇA E VAZAMENTO DE DADOS

A utilização massiva de dados pessoais acarreta aumento em riscos relacionados à segurança destes dados, riscos estes de danos que podem se fazer sentir seja pelos titulares dos dados pessoais, seja pelos responsáveis pelo tratamento. Assim, a segurança da informação é outro ponto abordado pelo Projeto de Lei ora em análise. Por segurança da informação, entenda-se que o projeto procura fomentar práticas que tornem tão difícil quanto possível o acesso não-autorizado a informações pessoais constantes em sistemas informatizados, seja por meio de intrusões perpetradas por meio informatizado, seja pela ação maliciosa de pessoas que utilizem indevidamente seus privilégios de acesso a sistemas informatizados. E, ainda, procura-se estabelecer parâmetros para minorar eventuais danos sofridos em incidentes de segurança que resultem na divulgação ou na disponibilização de informações pessoais para além dos seus destinatários.

Em relação às obrigações dos agentes do tratamento de dados de segurança, o Projeto não as determina de forma literal ou taxativa, preferindo identificá-las a partir do seu resultado esperado, isto é, que sejam aptas para evitar incidentes de segurança e o acesso não autorizado. Isto pela dificuldade e mesmo pelo não cabimento de abordar diretamente em um documento normativo práticas de segurança que, para que sejam realmente atuais e eficazes, são fluidas e costumam mudar e se atualizar constantemente. De toda forma, caso seja necessária uma composição entre esta fluidez e um patamar mínimo de práticas consideradas

como necessárias, existe a possibilidade, reconhecida no art. 45, § 1º, de que órgão competente estabeleça os padrões técnicos e organizacionais mínimos de segurança.

Em seus artigos 47 e 48, o Projeto estrutura uma sistemática para o tratamento dos chamados incidentes de segurança, considerados estes como aqueles capazes de causar dano ou risco relevante aos titulares de dados. Estas ocorrências, que muitas vezes são referidas como "vazamento de dados", costumam representar um risco a uma coletividade de titulares de dados e o tratamento dispensado pelo Projeto é no sentido de, além de incentivar boas práticas em segurança da informação para minorar a ocorrência destes incidentes, estabelecer procedimentos para aliviar os riscos e danos a titulares de dados uma vez que o vazamento tenha acontecido.

Neste sentido, é estabelecida a necessidade de o responsável comunicar ao órgão competente a ocorrência de um incidente de segurança, a fim de que a gravidade deste seja avaliada para que sejam tomadas medidas consideradas necessárias para a gestão do incidente e contenção do risco, seja através da comunicação do incidente aos titulares, da sua divulgação pública ou da tomada de outras medidas consideradas necessárias.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Um derradeiro ponto a ser destacado é a sistemática adotada pelo Projeto acerca da transferência internacional de dados, prevista em seu Capítulo V. O envio de dados pessoais para outros países é um ponto tradicionalmente abordado em legislações do gênero, visto o risco de perda de controle do cidadão sobre seus próprios dados caso estes sejam transferidos a um país no qual não existam garantias análogas em relação aos seus dados. Ao mesmo tempo, há hoje um trânsito extremamente volumoso de informações pessoais que são cotidianamente transferidas entre diversos países, muitas vezes no âmbito da operação habitual de diversos produtos e serviços da Sociedade da Informação. Assim, torna-se necessário coadunar um sistema que, ao mesmo tempo e na máxima medida, proporcione à pessoa transparência e controle sobre os seus dados que são transferidos a outros países sem, no entanto, inviabilizar a operação de serviços que realizem legitimamente estas operações e que sejam benéficos ao cidadão.

Neste ponto, a proposta do Projeto inspira-se em padrões presentes na legislação da União Europeia sobre a disciplina, ao estabelecer condições para legitimar a transferência internacional de dados pessoais, inclusive recepcionando o instituto da adequação, pelo qual o Estado estrangeiro cujo marco regulatório em tema de proteção de dados seja considerado compatível com os direitos e garantias a este respeito presentes no ordenamento brasileiro é considerado, para fins da transferência de dados, como apto a receber a transferência sem que quaisquer outros requisitos sejam cumpridos (art. 33, I).

Este mecanismo de transferência facilita sobremaneira a transferência para países com patamares adequados de proteção de dados, procurando manter intactos os direitos e garantias dos titulares, sendo que o reconhecimento de tal adequação deve ser realizado por órgão competente. O projeto também estabelece diversas modalidades de legitimação para a transferência de dados para países que não tenham recebido esta mencionada adequação, como, por exemplo, mediante a autorização dada por órgão competente para uma transferência, no caso de consentimento específico do titular, no âmbito de cooperação internacional, em alguns casos de cooperação internacional, para a execução de políticas públicas, no caso do reconhecimento de cláusulas corporativas globais em uma corporação, entre outras. Especialmente a possibilidade de transferência de dados pessoais com base em cláusulas contratuais padrão (art. 34, §1°) e em normas corporativas globais (art. 34, §2°) dão a necessária flexibilidade ao sistema de transferência internacional de dados pessoais, preservando ao mesmo tempo, a proteção à personalidade e à privacidade do indivíduo.

O PL 5.276/2016 E OUTRAS INICIATIVAS LEGISLATIVAS CONGÊNERES

Deve-se ressaltar, no entanto, que o Projeto de Lei n° 5.276 de 2016 não é a única proposta atualmente sendo considerada no processo parlamentar brasileiro para a regulamentação da proteção de dados. Ao seu lado se encontra o Projeto de Lei do Senado 330, de 2013 (PLS 330/2013), que também se identifica como uma proposta de lei geral sobre proteção de dados.

Ambos os projetos possuem uma identidade comum e, pode-se afirmar, coincidem em seus objetivos, propósitos e estrutura fundamentais. Como contrastes mais acentuados entre ambos, podemos mencionar, em primeiro lugar, o fato do PLS 330/2013 não apontar para uma autoridade de proteção de dados para o encaminhamento de diversas questões, como o faz o PL 5276/2016. Este fato se deve a uma questão formal: sendo projeto de lei de origem no Poder Legislativo, não poderia este projeto criar ou alterar estruturas da administra-

ção pública concernentes ao Poder Executivo, motivo pelo qual a técnica legislativa utilizada não contemplou tal tipo de estrutura (relate-se porém que, neste ponto, o relatório do Senador Aloysio Nunes, relator do referido projeto na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, externa sua opinião pela pertinência da criação de referida autoridade, conclamando o Poder Executivo a tomar iniciativa neste sentido[7]). Em relação a outros pontos, há diferenças de detalhamento e modulação em diversos pontos do projeto, sem que haja propriamente qualquer conflito ou incompatibilidade de monta.[8]

CONCLUSÃO

A demanda do cidadão por direitos e garantias sobre os próprios dados, que o projeto de lei procura estruturar de forma sistemática, vem sendo sentida de forma cada vez mais intensa. Similarmente, os setores privado e público também necessitam de regras e limites claros para a utilização de dados pessoais, de forma a obter segurança jurídica em diversos processos que hoje utilizam dados pessoais ou que teriam muito a ganhar se os utilizassem. Com uma legislação geral como a proposta pelo PL nº 5.276/2016, ambas as demandas podem ser atendidas: por um lado, com a atualização da proteção da privacidade de forma que o brasileiro possa gozar efetivamente de uma cidadania digital, e, por outro, por meio da criação de um espaço favorável para a inovação e utilização de dados pessoais dentro de um ambiente de legitimidade e de respeito às escolhas fundamentais do cidadão. Nesse ponto, vale mencionar importante reflexão do mestre italiano Stefano Rodotà, que relaciona a proteção de dados pessoais diretamente com o grau de democracia de um país: *"a proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isto a cada momento não é verbosidade, pois toda a mudança que afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar."*

7 *http://www.senado.leg.br/atividade/rotinas/materia/getTexto.asp?t=171779&c=PDF&tp=1*

8 *Para mencionar um exemplo, o tema da segurança da informação é explicitado de forma mais detalhada no PL 5.276/2016, em grande parte, provavelmente, pelo fato do referido projeto ter passado por um período de redação mais longo que compreendeu, inclusive, a realização de dois debates públicos pela internet.*

NAVIGATING THE PRIVACY LANDSCAPE

Reflections from the Privacy Commissioner

JOHN
EDWARDS

El Dr. Edwards fue asignado como Comisionado de Privacidad en febrero de 2014 por un término de cinco años. Desarrolla comentarios independientes sobre políticas públicas y asuntos relevantes vinculados con información personal. Antes de su nombramiento, el Dr. Edwards ejerció el Derecho en Wellington por más de 20 años, especializándose en derecho de la información, mientras que representaba a una amplia gama de clientes del sector público y privado. Ha desempeñado funciones legales para el Ministerio de Salud, la Comisión de Servicios del Estado, el Departamento de Primer Ministro y Gabinete así como el Departamento de Inland Revenue. Durante 15 años, se desempeñó como inspector de distrito para la salud mental y también ha sido inspector de distrito para servicios de discapacidad intelectual.

SUMARIO

RESUMEN

El autor en su calidad de Comisionado de la Privacidad de Nueva Zelanda plantea su perspectiva respecto a la forma de encarar los nuevos retos a la privacidad derivados de la transformación digital que actualmente impacta en la vida de las personas.

Realiza una detallada cronología asociada a la definición de la privacidad, a su rol respecto a otros derechos, y a su inclusión en distintos instrumentos internacionales a través del tiempo.

Asimismo, realiza consideraciones respecto del verdadero valor público de la privacidad, y a la forma en la que esta se encuentra regulada en Nueva Zelanda, destacando -luego de una pormenorizada relación de las circunstancias legales asociadas a su reconocimiento-, que actualmente la privacidad es un verdadero derecho humano.

El autor examina distintas sentencias judiciales asociadas al tema, así como las principales cuestiones reguladas en la Ley de Privacidad neozelandesa.

Finalmente, presenta una serie de reflexiones sobre la privacidad proponiendo un análisis contextual del derecho a la privacidad, asociado a sus limitaciones derivados de la existencia de otros derechos -como la libertad de expresión y la justicia-, sin olvidar que nos encontramos, en definitiva, ante un derecho fundamental.

INTRODUCTION

My comments in this paper are made from the perspective of my statutory privacy jurisdiction. As the Privacy Commissioner, I am constantly making line calls on privacy – on privacy complaints, data breaches, or consultations about privacy interests with other organisations and in response to media stories.

In dealing with the full array of human circumstances, the courts may encounter privacy issues in one form or another. Occasionally privacy might feature as the main event - the occasional privacy tort perhaps, or a challenge to a search under section 21 of the NZ Bill of Rights Act. In other cases, privacy, like other human rights, will be a relevant dimension or raise specific issues in a case you are hearing.

My prediction is that the privacy dimension to the work of the courts is likely become more significant. The basis for that is the ocean of personal information now captured and collected through digital technologies. Privacy is now everywhere you look – it's hard to find a sphere of human activity that does not involve personal information in some way.

The ongoing digital transformation of people's lives, business, government and the economy is producing vast swathes of personal data and information. Individuals are embracing the device driven world and actively create and capture large amounts of data about their lives.

Think for a moment about all the information that is increasingly being collected about us:

- Smartphones that know our every move and the most intimate and personal aspects of our lives
- Intelligent cars that know where we go and how we drive
- The internet of things where the objects we own collect information about us
- Wearable tech that collects information about our fitness and our health
- Big data that functions by saving as much information as possible
- Artificial intelligence and learning tools that can turn data in to useful information and make inferences based on seemingly unconnected information

We are at a turning point where the collection and generation of personal information is no longer consciously controlled by the choice of the individual. Valuable personal information is now also generated passively (and largely unconsciously) through the new online services and devices and these are highly connected, providing insights and richer information about our daily lives.

It is becoming increasingly harder to understand when our information remains on our device, when it goes somewhere else, how long it stays there, who has access to it, when it is encrypted, and who has access to the encryption keys.

Taking a helicopter view, what are the implications of the digital age on the right to privacy? Decisions about what is done with personal information, how it is shared, for what purpose, and how it is protected, can be significant. While the positive uses of data are clearly beneficial to business and society, the risks to privacy cannot be overlooked. New devices create new methods of surveillance and intrusion. What was formerly private or obscured can now be readily revealed, often covertly. There are risks to personal control over personal information, risks of injustice such

as discrimination from the misuse of personal information, and risks to personal dignity from the release of personal information.

While warnings about the risks to privacy from technological developments need to be carefully addressed have been made and repeated by Privacy Commissioners since the 1990s, it remains just as relevant and takes on a heightened significance as each new phase of the data society is rolled out.

People care about their privacy, especially over information held about them by government agencies, by businesses and by online providers. This is evident from the results of my Office's public opinion surveys, from public reaction to privacy issues in the media, particularly high profile data breaches, and from the nature of individual complaints that are brought to my Office for investigation.

OVERVIEW

How does the legal landscape respond to current privacy challenges? Privacy in the law is a unique patchwork with a history of incremental development. There is no one definitive expression of privacy in the law – it has all manner of guises (and disguises), depending on the context. But the sum of these different legal expressions all point to the multi-faceted expression of the right to privacy under New Zealand law.

One of the challenges is ensuring that New Zealand's privacy law continues to develop in a logical way. This is no easy task. Because of the variety of forms that privacy can take, the variety of different circumstances in which privacy rights arise and the variety of ways that privacy in reflected in the law, there is no one unified legal approach. This means that privacy decision-makers need to understand the broader context, and be on the look-out for the different interplay of rights and interests in any given circumstance.

In this paper, I intend to cover privacy and its different expressions in the legal landscape, beginning with an outline of some of the international origins and influences.

I intend to note the various forms that the right to privacy takes in the New Zealand legal landscape, and some of the different conceptual approaches that are used.

I would like to also discuss the statutory design of New Zealand's Privacy Act and its key elements and features, and the particular role of the Act and the Privacy Commissioner's jurisdiction in the privacy landscape.

THE CHALLENGE OF DEFINING PRIVACY

Privacy has proved notoriously difficult to define. Scholars have laboured long and hard to try to come up with a unified theory of privacy. The Law Commission carried out a fulsome review of different theories in their efforts to come up with a workable privacy taxonomy on which to underpin its review of New Zealand privacy law five years ago.

It is the interplay of privacy-related rights and interests has proved difficult to capture in definitional form. Attempts to try to define privacy demonstrate its multifaceted nature - privacy is really an umbrella term for a number of related interests or values namely access, control, and is strongly based on individual dignity.

Often, definitions of privacy revolve around the control of personal information but miss those forms of privacy invasions that consist of invading private spaces or paying unwanted attention.

Various ideas for defining privacy include:

- the individual's "right to be left alone", a concept developed by Warren and Brandeis (1890) who argued that privacy was the most cherished of freedoms in a democracy.[1]
- the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others - Alan Westin, author of "Privacy and Freedom" (1967)
- privacy as an interest of the human personality - protecting the inviolate personality, the individual's independence, dignity and integrity - Edward Bloustein, author of "Individual and Group Privacy" (date)[2]
- the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information - the Calcutt Committee's first report on privacy (United Kingdom, 1990)
- According to scholar Ruth Gavison, there are three elements in privacy: secrecy,

1 *See Hosking v Runting Tipping J at [238].*

2 *According to Bloustein "Privacy as an aspect of Human Dignity: An Answer to Dean Prosser" (1964): "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality ....Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones."*

anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person.

- Victoria University academic Dr Nicole Moreham has developed a useful approach where she regards privacy as a state of desired inaccess or freedom from unwanted access i.e. being seen, touched or heard, obtaining physical proximity, or obtaining information about a person.[3]
- A fundamental component I would add is the right to access one's own personal information, and to request any necessary correction. (This dimension of privacy overlaps with freedom of information.)

Although these definitions have substantial commonality and overlapping concepts, the elemental messiness is something that can't be avoided. That's not to say there isn't a conceptual framework for privacy that works pretty well on the whole. A working definition can be readily be brought forward that can be employed in a particular sphere or context.

My approach is to think in terms of the three main strands of privacy:[4] namely **bodily privacy** – that is the integrity of the body should not be violated without legal justification; **physical privacy** – certain places such as person's home carry a high privacy value requiring adequate legal justification for any intrusion; and **informational privacy** – information about an individual gives rise to a privacy interest that varies in strength depending on factors such as level of sensitivity, and the purpose for which it is collected, used or disclosed.

Each of these three dimensions can have varying privacy impacts ranging from the negligible or minor, through to the highly significant and harmful. But importantly, just because there may be no privacy intrusion in one sphere, does not automatically mean there is not a breach in another sphere. Each sphere has to be assessed in turn.

This approach probably makes me a privacy pragmatist, in the company of Daniel Solove (A Taxonomy of Privacy, 2006). Professor Solove has said:

> Privacy is a set of protections against a related set of problems. These problems are not all related in the same way but they resemble each other. There is a social value in protecting against each problem, and that value differs depending on the nature of each problem.

Because the landscape of privacy is constantly changing with society and technology, Professor Solove notes there is a risk of trying to fit new problems into old conceptions. For Solove, privacy must be context-specific and it depends on examining privacy intrusions as disruptions such as interference with peace of mind, intrusion on solitude, or loss of control over one's information.

While the three dimensions of privacy (bodily, physical and informational privacy) offers a practical and generally reliable starting point, one cannot be too rigid about categorisation in today's dynamic environment, given emerging overlaps between them, for example:

- The body itself is now the source of sensitive identifying personal information through the increasing use of biometric technologies and wearables
- the sanctity of the cell-phone is now rivalling the sanctity of the home as a repository of significant personal information and intimate details about a person's life and connections.

PRIVACY HAS COME TO MEAN MANY THINGS - ORIGINS AND INFLUENCES ON THE RIGHT TO PRIVACY

A rapid look back through legal history illustrates the variety of ways in which the law has responded to protect things that are significant to the private life of the individual. Both English law and US law have had influential impacts, as well as European human rights law.

Diverse developments touching on the rights of the individual can be linked by applying a privacy lens. For example:

- As far back as 1361, the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers.
- the English common law of trespass that protected an Englishman's home as his castle
- the principle of legality established by *Entick v Carrington* as the classic early search warrant case

3 *NA Moreham "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" from Law, Liberty, Legislation Jeremy Finn and Stephen Todd (eds) (2008).*

4 *Sometimes communications privacy is considered as a fourth strand to privacy.*

- the incidental protection of privacy by the common law, equity and the criminal law via causes of action ranging from assault, battery and negligence to breach of confidence, copyright, defamation, malicious falsehood and the tort of passing off.
- The right to be let alone seeded in US law by Warren and Brandeis and extending as far as finding protection against State intrusion into private matters in cases such as *Roe v Wade* (reproductive rights) and *Griswold v Connecticut* (contraceptive rights)
- The rights of celebrities to be left alone via the English breach of confidence, overlaid by the application of privacy rights under article 8 of the European Convention on Human Rights – Michael Douglas and Catherine Zeta Jones, Naomi Campbell, JK Rowling, and Max Mosley,
- the emergence in Europe (in Germany) of the world's first data protection laws, responding to 20th century advances in information processing, and influenced by the lingering memories of the uses that census and other official records had been put to during the time of National Socialism, and the surveillance period of East German communism.

United Kingdom – the common law

From Lord Coke's seminal laws of England (1628) the English dictum that a man's home is his refuge firmly entered the common law. Or as rather more colourfully expressed by Sir William Pitt the elder (British PM, 1763):

> "The poorest man may in his cottage bid defiance to all the forces of the crown. It may be frail - its roof may shake - the wind may blow through it - the storm may enter - the rain may enter - but the King of England cannot enter."

A high point of this period is *Entick v Carrington* (1765), well known to every law student but worth including as a direct influence on privacy law, with echoes to our s 21 BORA cases such as the Supreme Court's decision in *Hamed* (2011) and receiving a specific mention by Whata J in *C v Holland* establishing the tort of intrusion upon seclusion.

The government of the day suspected Entick of anonymously writing "scandalous reflections and invectives upon His Majesty's Government, and upon both Houses of Parliament". The Earl of Halifax, "acting as Secretary of State" issued a warrant to search Entick's home. Carrington and three others broke into his premises "with force and arms [...] without his consent and against his will" in pursuance of this warrant. They spent a total of four hours looking for evidence to confirm the government's suspicions, prying into Entick's personal papers and removing a number of documents and personal items.

While *Entick v Carrington* is a seminal case in English constitutional law, and reinforced the principle of legality, it is also credited as a principal influence behind the US Fourth Amendment (unreasonable search and seizure). Articles 6 and 8 of the European Convention on Human Rights, guaranteeing a fair trial as prescribed by law and right to private life respectively, can also be said to trace their DNA back to this case.

Other aspects of the common law and equity have protected privacy indirectly through the guise of other established causes of action. While the common law did not previously recognise the right to privacy per se, reliance could be placed on some other tort or right of action that might incidentally provide a remedy. For example violations of the integrity of the body have long been protected by specific criminal offences or civil actions such as assault, battery and negligence.

In relation to the disclosure of personal information, relevant causes of action employed over the years have included breach of confidence, negligence, copyright, defamation, malicious falsehood and the tort of passing off.

United States

From the United States, the 1890 article "the Right to Privacy" by Samuel Warren and Louis Brandeis has been highly influential in articulating recognition of the right to privacy as necessary to protect the person and secure the right to be let alone. Warren & Brandeis based the right to privacy on the concept of "inviolate personality" – the right to privacy being part of the more general right to the immunity of a person – the right to one's personality (as per the German legal and philosophical tradition)

Privacy as the right to be let alone influenced William Prosser's Restatement of the Law of Torts (1960) that articulated four types of invasion of privacy, tied together, according to Prosser, by the fact that each represents an interference with the right to be let alone.

The other influential strand of US privacy law is the right to privacy that is found in the US Constitution, as protecting the citizen against

intrusions of the State. Justice Brandeis in his famous *Olmstead* dissenting judgment described the Constitution as conferring as against the Government, the right to be let alone – to protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. This view was later adopted by the Supreme Court in 1967 in *Katz v United States*.

Privacy has also been extended beyond Fourth Amendment search and seizure cases to matters such as rights to contraception (*Griswold v Connecticut* (1965)) and abortion (*Roe v Wade* (1973)), the common theme being a recognition of privacy as protection against State intrusion into private spaces or private matters, also known as "decisional interference".

Europe – Twin human rights – origins in dignity and autonomy

Europe's influence on privacy development has been considerable. This is due to the development of distinct but related rights privacy and data protection rights. Europe has also provided a human rights framework for these rights, namely:

- the right to *respect* for private life and the need to prevent undue *interference* in private matters - Article 8 of the European Convention on Human Rights (ECHR)[5]
- the right to the *protection* of one's personal data and the need to ensure adequate *control* for individuals over matters that may affect them – (Data Protection Convention 1981, the European Directive (1995) - recently updated by a new General Regulation that will come into force in 2018).

These are related as both are expressions of the universal idea of the dignity, autonomy and unique value of every human being and the associated right of the individual to develop their own personality and to have a fair say on matters that may have a direct impact on them.

To develop one's personality, in the European context, a person needs to be able to participate in society by disclosing only such information as they wish and to whom they wish. Without this right of informational self-determination, the individual gives up some of their right to freely develop their personality, as they are uncertain what processing is being done on their personal information. If a person does not know what information about them is being recorded, or otherwise processed, to keep control of their information they may withdraw from the public actions and debates necessary for a democratic society.

Data protection has been regarded from the outset in Europe as a matter of great structural importance for a modern society. In the Population Census case (1980) for example, the German constitutional court determined that in the age of data processing, the right to informational self-determination, requires protection against the unlimited collection, storage, use and disclosure of personal information.

The decision of the court created a series of procedural safeguards. The requirements for legal purpose-specific collection were enunciated, as well as accuracy of information, the ability to access and revise it, timeliness, limits on retention of personal data, collecting the minimal amount of data required and the independence of data protection officers. The court also noted the unconstitutionality of one level of government passing the data to another dictated a requirement for organizational and procedural safeguards. These initial principles are still central to data protection laws today including our down Privacy Act.

The European context is instructive in how these two strands of privacy protection inter-relate. On the one hand, 'data protection' is broader than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data that may be private in some contexts while mundane in others. At the same time 'data protection' is a more limited concept because it exclusively concerns the handling of personal information, and not other aspects of privacy protection, such as physical or bodily privacy.

This "broader but narrower" dichotomy demonstrates some of the logical steps involved in privacy analysis. A privacy decision-maker needs to be mindful of the context in which an issue arises and whether it is one of data protection, or triggers a more intensive right of privacy. This may largely be determined by the forum in which an issue is raised. But to what extent can the protection of privacy in one context influence the other? This is an issue I intend to explore later in this paper.

5 *European Convention on Human Rights 1950. Article 8. Under Article 8 everyone has the right to respect for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in accordance with the law and where necessary in a democratic society for certain important and legitimate interests.*

PRIVACY AS A CONDITION PRECEDENT TO OTHER HUMAN RIGHTS

As noted by Thomas J in *Brooker v Police*, privacy is an aspect of "human autonomy and dignity".[6]

> Probably [no human right] is more basic to human dignity than privacy. It is within a person's sphere of privacy that the person nurtures his or her autonomy and shapes his or her individual identity. The nexus between human dignity and privacy is particularly close.

Dignity has been described as central to all human rights and having a uniting role on human rights. Privacy is valuable in its own right, but also plays a pivotal role in supporting other significant human rights such as freedom of expression, thought, conscience and religion.

The connection between privacy and autonomy and the protection of human dignity, means that privacy serves as the foundation upon which many other human rights are built. Adverse privacy intrusions (such as surveillance) can have a significant impact on the dignity of the individual including related human rights including freedom from discrimination, freedoms of expression, thought, peaceful assembly, movement and association.

Privacy provides an important space for a person to be themselves, to think freely, to nurture intimacy, relationships and social interaction, and thereby flourish. In this sense, privacy contributes to the development of personality and citizenship.

Privacy also enables a person to exercise a degree of autonomy and control against arbitrary and unjustified use of power, whether by the State or by private enterprise.

INTERNATIONAL INSTRUMENTS

Rights of privacy in international instruments

Privacy is internationally recognised as a human right, International instruments such as the Universal Declaration of Human Rights 1948[7] and the International Covenant on Civil and Political Rights[8] have framed these rights and freedoms in modern times and have helped shape New Zealand's laws including the Bill of Rights Act 1990, the Human Rights Act 1993 and the Privacy Act 1993. The right to privacy does not exist in isolation but in the context of these international human rights instruments.

Data Protection Frameworks

Data protection rights have been supported by the development of regional data protection instruments that have influenced the uptake of privacy laws in numerous jurisdictions including New Zealand. As well as the European Convention (1981), other important frameworks for New Zealand include the OECD Guidelines (1980) on which our own Privacy Act is based, and the APEC Privacy Framework (2004).

OECD Guidelines 1980.

The OECD data protection principles were developed to encourage economies to provide basic privacy protection so that people can trust that their information is treated appropriately wherever it ends up in the world. That trust leads to people being willing to engage in the economy and creates business opportunities. The OECD's standards for handling personal information have contributed to the growth of e-commerce and personal communication technologies. The principles are now enshrined all over the world and have been very influential as a benchmark for data protection laws in economies outside Europe.

The Guidelines apply to personal data whether in the public or private sectors that pose a danger or risk to privacy and individual liberties, because of the manner in which personal data is processed, or because of its nature or the context in which it is used.

The preface to the OECD Guidelines discussed the potential of developing technologies around data storage and transfer:

> The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced

6 *Brooker v Police [2007] 3 NZLR 91, [182].*

7 *Universal Declaration of Human Rights 1948. Article 12. "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."*

8 *International Covenant on Civil and Political Rights 1966. Article 17. 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, not to unlawful attacks on honour and reputation. 2. Everyone has the right to the protection of the law against such attacks.*

> shortly, ... to prevent what are considered to be violations of fundamental human rights, such as the storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

APEC Privacy Framework 2004

Data protection principles have also been developed in the APEC region as a means of reducing barriers to trade by removing obstacles to information flows, to encourage economic growth.

UN Special Rapporteur for Privacy 2015

Another more recent international development has been the appointment of a dedicated Special Rapporteur for privacy issues. This role has been taken up by Professor Joseph Cannataci who has recently provided his second report to the United Nations Human Rights Council focussing on governmental surveillance.[9]

PUBLIC VALUE OF PRIVACY

Having surveyed some of the influences in the development of the right to privacy, I would like to note the broader role that the right to privacy fulfils, beyond protecting the dignity of the individual.

The right to privacy plays an important role in supporting other fundamental rights. Adverse privacy intrusions such as surveillance can affect people's freedom of movement, freedom of expression, freedom of information, freedom of religion, and freedom from discrimination. The effect can be a direct on the target of the intrusion, or can have an indirect chilling effect on others.

As well as the impacts on the individual, there are wider ramifications for related human rights and for preserving the necessary space for individuals to participate in a functioning and healthy democracy. Privacy protects aspects of freedom of speech and association that are essential to the functioning of a democratic society and creates the necessary conditions for a healthy public sphere.

There's also a strong case that the right to privacy not only protects individuals, but also has beneficial effects for the public and private agencies who serve them. One of the public interests I am keenly aware of in my role as Privacy Commissioner is the need to maintain trust and confidence in public institutions. This is a strong argument in favour of promoting compliance with privacy rights and standards. Public agencies will undermine their mission to effectively provide public services and perform their public duties if they do not maintain the trust of the individuals who use their services.

WHAT FORMS DOES THE RIGHT TO PRIVACY TAKE IN NEW ZEALAND?

For a long time privacy's role was confined to the shadows of the law. While not explicitly recognised or named in its own right, its shady existence was nevertheless influential in certain cases, in particular, rights of privacy in private property.

We've reached the point now where we can confidently declare that privacy is a full-blown human right. The significant developments in the law of privacy in New Zealand, such as the privacy torts by the Court of Appeal in *Hosking v Runting* (2004) and the High Court in *C v Holland* (2012), and section 21 cases from *R v Jefferies* (date) onwards that have broadened the focus in protecting the right to be free from unreasonable search and seizure beyond property rights to a focus on the protection of privacy rights of individuals, illustrate and confirm the existence of the right to privacy in our law.

Privacy also has a clear presence in the statute book.

A survey of the statutes

The idea of a Privacy Commissioner was mooted in the **Preservation of Privacy Bill 1972**, responding to a report on the storage of information in computers. The job of the Commissioner would have been to register all computer installations in New Zealand, including the nature of data stored in each installation and the purpose for which it was stored. It was also proposed that everyone about whom information was stored would receive a print-out of all information stored about them. 45 years later this seems quite outlandish, but interestingly the concept that people should be able to obtain a download of the information that is held about them is now being discussed as the right to data portability, a new data protection right that is set to become part of the European Data Protection framework from next year.

The role of Privacy Commissioner was subsequently created under the **Wanganui Computer Centre Act 1976**, being tasked with overseeing the operation of the system.

The **Human Rights Commission Act 1977** signalled a more general concern about privacy. The Human Rights Commission was given a general watchdog

9 A/HRC/34/60

role in relation to privacy, with the power to inquire into matters that may unduly infringe the privacy of the individual, to make reports to the Prime Minister on matters relating to privacy, and to receive and invite submissions from the public on privacy issues. These are functions that I have inherited under the Privacy Act.

In 1979, crimes against personal privacy relating to the interception of communications were added to **the Crimes Act**.

The **Official Information Act 1982** was a milestone in freedom of information in New Zealand. It is noteworthy though that the long title records that the Act is to make official information more freely available, to provide proper access by each person to official information that relates to them and to protect official information not only in the public interest but also to the extent necessary to preserve personal privacy.

The Act provided a judicially enforceable right of access to an individual's own personal information, a right that has been described by the Court of Appeal as "constitutional" in 1988.[10] This right was extended to personal information held by local government agencies, educational institutions and health boards in 1987. The right of access to information was eventually transferred across to the Privacy Act when it was enacted in 1993.

There is also an express reason in the Act to recognise privacy as a ground to withhold official information from being released (even if the person is deceased), subject to the public interest.

In 1988, the Information Authority established under the OIA produced a report recommending an amendment to the Act to include a set of rules to govern the collection and use by government agencies of personal information. An alternative home for these rules, but modified into principles, was found in the Privacy Act in 1993.

There are important privacy aspects present in the **New Zealand Bill of Rights Act 1990**, including section 14 (the freedom to seek information) and section 21 (protection from unreasonable search and seizure). Section 28 also confirms that existing rights or freedoms are not to be abrogated or restricted only because they have not been included or only partially included, leaving room for the right to privacy.

Section 21 of the Bill of Rights Act is significant in protecting an individual from unreasonable search and seizure, based on the touchstone concept of a reasonable expectation of privacy. [The Chief Justice in *Hamed* described s 21 as a constraint on State activity. The right protects privacy, but, also, and more fundamentally, holds a constitutional balance between the State and citizen by preserving space for individual freedom and protection against unlawful and arbitrary intrusion, requiring the authority of law for State intrusion upon personal freedom.]

However, there is no general guarantee of privacy rights in the Bill of Rights Act, as noted in the 1985 White Paper:

> There is not in New Zealand any general right to privacy although specific rules of law and legislation protect some aspects of privacy. It would be inappropriate therefore to attempt to entrench a right that is not by any means fully recognised now, which is the course of development, and whose boundaries would be uncertain and contentious.

The Right Honourable Sir Geoffrey Palmer and Dr Andrew Butler in their current joint project, *A Constitution for Aotearoa New Zealand*, note that right to privacy was deliberately left out of the Bill of Rights Act – although this was a protected right under some overseas Bill of Rights, there was real uncertainty about how it might be applied by the courts as it was too vague and uncertain.

Sir Geoffrey and Dr Butler now consider that as a substantial body of case law has developed overseas this concept (as well as the right to security of the person) have become much more concrete and less frightening:

> the last 30 years have only served to emphasize how important a right such as the right to privacy is in preserving human dignity and freedom. Indeed, we believe there is little exaggeration in saying that one of the biggest threats to human freedom and dignity lies in the digital transformation of society and the consequent ease with which information can be acquired, retained, and analysed in respect of individuals. A bill of rights that does not protect these rights from unjustifiable encroachment would be seriously deficient.

The draft proposed Constitution would include the ICCPR article 17 right not to be subject to arbitrary or unlawful interference with that person's privacy, family, home or correspondence.

Back from the future of our Constitution to the 1990s, where the **Privacy Commissioner Act 1991** introduced a data matching oversight role for the Privacy Commissioner in relation to

10 *Commissioner of Police v Ombudsman.*

government data matching between some of the larger departments. But the privacy principles didn't arrive until 1993 with the introduction of a introduced a comprehensive data protection framework into New Zealand law with the enactment of the **Privacy Act 1993**. The preamble records that the Act is to promote and protect individual privacy in general accordance with the OECD data protection principles and guidelines. The Act protects personal information in both the public and private sectors.

Despite its name, the Act is largely concerned with a person's interest in information privacy. The Act was originally introduced as the **Privacy of Information Bill**, the Explanatory Note confirming that the legislation did not purport to be a comprehensive privacy law. Despite the last minute name change, information privacy is still the core scope.

However the general privacy watchdog role (lifted from the Human Rights Act) is not confined to information privacy but allows me to inquire into any matter of privacy, and to make suggestions, recommendations and comments about privacy issues.

In 1997, **the Harassment Act** introduced both civil and criminal penalties for various types of harassment and in 2006, a further offence against personal privacy was added to the **Crimes Act** for covertly making an intimate visual recording.

The **Harmful Digital Communications Act 2013** has now enacted a set of communication principles, and a process for bringing complaints about serious breaches to the District Court, if not first resolved by Netsafe, the agency appointed by Government to first handle HDCA complaints. Principle 1 is directly privacy related - a digital communication should not disclose sensitive personal facts about an individual.

Privacy also finds expression in other non-statutory instruments such as the Code of Health and Disability Consumers Rights, and the media standards maintained by oversight bodies (Press Council, BSA and OMSA) include explicit privacy standards against unreasonable intrusion.

Privacy in the courts – the torts

The law of privacy has also undergone significant development in our tort law. As you will be well aware, the tort protecting informational privacy in *Hosking v Runting*[11] – the tort of public disclosure of private facts[12] - is now accompanied by a tort of intrusion into solitude identified by Whata J in *C v Holland*.[13]

Public disclosure of private facts

The first privacy tort of publication of private facts requires:

- the existence of facts in respect of which there is a reasonable expectation of privacy; and
- publicity given to those facts that would be considered highly offensive to an ordinary reasonable person i.e. publicity that is determined objectively to be offensive by causing real hurt or harm.

The defence of legitimate public concern in matters such as public health, the economy, safety, the detection of crime, and the protection of national security, allows a balancing exercise to ensure that there is no unjustifiable limitation on freedom of expression.

This tort is based on the core idea that certain facts are inherently private, such as personal and sexual relationships, financial matters and medical conditions. This question of whether facts are sufficiently private to give rise to a reasonable expectation of privacy can be complex where a mix of public and private elements may be present in a factual matrix, or where any publicity given to certain facts has waned over time. Professor Cheer has endorsed a contextual approach to determine this issue including the element of intrusiveness and the nature of the publication.[14]

The role and need for the threshold requiring that the publication must be highly offensive has been critiqued by Dr Nicole Moreham, suggesting that the reasonable expectation of privacy requirement, that depends on a wide range of contextual factors, places a sufficient control on the breadth of the tort, along with the public concern defence.

Interestingly, as an example of cross fertilisation between different privacy contexts, the highly offensive threshold has now been put to use in the Privacy Act. Section 56 of the Act that limits the application of the privacy principles in a personal, family or household context, is now subject to a floor based on an objective highly offensive test.

---

11 *Hosking v Runting [2005] 1 NZLR 1 (CA). See also Brown v Attorney-General [2006] DCR 630; Andrews v Television New Zealand [2009] 1 NZLR 220 (HC)); Rogers v Television New Zealand [2007] NZSC 91.*

12 *[other cases]*

13 *C v Holland [2012] NZHC 2155.*

14 *Ursula Cheer "The Tort of Privacy – recent legal development in New Zealand".*

The exemption in subsection (1) ceases to apply once the personal information concerned is collected, disclosed, or used, if that collection, disclosure, or use would be highly offensive to an ordinary reasonable person.

The highly offensive threshold also features in the second tort – intrusion upon seclusion or solitude.[15]

Intrusion into solitude

The *Holland* decision introduced a new category of privacy tort in New Zealand. Whata J described the elements of the tort as:

- an intentional and unauthorised intrusion;
- into seclusion (intimate activity, space or affairs);
- involving infringement of a reasonable expectation or privacy;
- that is highly offensive to a reasonable person.

Like the publication tort, the infringing activity must directly impinge on human autonomy and must cause real hurt or harm, objectively determined.

His honour engaged in a survey of privacy and intrusion in New Zealand, including the Broadcasting Standards Authority privacy principles, the Privacy Act's privacy principle 4, section 21 of the New Zealand Bill of Rights Act, Supreme Court decisions *R v Williams* (2007), *Brooker v Police* (2007) and *Hamed v R* (2011) and statutory provisions in the Crimes Act 1961, the Search and Surveillance Act 2012, and the Residential Tenancies Act. On this basis he concluded:[16]

> New Zealand's legal framework has embraced freedom from unauthorised and unreasonable physical intrusion or prying into private spaces or personal spaces such as the home, and freedom from unauthorised recordings of personal, particularly intimate affairs, whether published or not. But it has to be said that the extent to which privacy values are vindicated still depends on the legislative framework within which the impact on those values is being assessed. Legislation affording protection of privacy is invariably moderated by public interest considerations.

As one commentator notes, much of the interest in the decision has been centred on the implications of the tort development for journalism. But perhaps more intriguing is the future possibility of the intrusion tort on seclusion in the digital realm such as email, social media or banking.

For example the Ontario Court of Appeal recognised a cause of action for invasion of privacy in an employee browsing case.[17] Ms T used her workplace computer to access personal information of a co-worker, Ms J over a period of 4 year while Ms T was in a relationship with Ms J's former husband. The court found that Ms T committed a tort of intrusion upon seclusion when she repeatedly examined Ms J's private bank records. The intrusion was intentional, it amounted to an unlawful invasion of Ms J's private affairs, it would be viewed as highly offensive to the reasonable person and it caused distress, humiliation or anguish, and Ms J was awarded $10,000 damages. One of the court's stated reasons was that technological change has motivated greater legal protection of personal privacy and poses a novel threat to privacy interests.

THE PRIVACY COMPLAINTS JURISDICTION – THE PRIVACY ACT AND ITS KEY DESIGN ELEMENTS

I would like to highlight some of the key features of the Privacy Act that are important in understanding the overall statutory scheme. There is increasing reference being made to the privacy principles in cases being argued before the courts.

While the Act can offer some guidance to the particular issue in a proceeding, such as in the employment context where a departure from the privacy principles may be indicative of in deciding whether there has been a breach of good faith, it is important to think of the Act as an integrated scheme and the role of a particular provision must be understood within that scheme.

I have some concerns about the trend of citing the Act in legal argument, as I see risks in cherry picking individual provisions to bolster a counsel's submissions, for example that an action is unfair or unlawful, or conversely that an action is categorically asserted to be permitted, due to the existence of a provision in the Privacy Act.

There is a risk that legal counsel will apply a very specific lens to a provision or principle in

15 *C v Holland at [97], Whata J noting that a reasonable expectation of privacy test on its own is not sufficiently prescriptive to limit conflict with other rights.*

16 *[32].*

17 *Jones v Tsige (2012) ONCA 32.*

the Privacy Act, without providing the court with the full context of the statutory scheme in which that provision sits. The court may not have the benefit of full argument about the appropriate role of that provision and whether other aspects of the statutory scheme may be relevant to the interpretation being argued.

My concerns in this area led me to intervene in an evidential challenge in the Supreme Court last year. (That proceeding has been decided, but the court has not yet released the reasons for the decision.) I felt it important and I hope the court found some value in hearing impartial and objective submissions about the influence, scope and limits of the Privacy Act when considering the statutory intersection of the privacy principles with other contexts such as the Evidence Act, the Search and Surveillance Act and the New Zealand Bill of Rights Act.

It is necessary in my view for decision-makers to deliberately centre themselves in the privacy landscape – an approach demonstrated in decisions such as *Brooker v Police* (NZSC 2007); *Hosking v Runting* (NZCA, 2004) and *C v Holland* (NZHC 2012, Whata J). By this I mean taking stock of relevant aspects of the privacy landscape and assessing their influence based on a contextual analysis of the circumstances. This approach allows for considered coherent development of the law and reduces the risk of conceptual confusion.

It ensures due consideration of the wider privacy eco-system and the potential for a decision (or dicta!) to have broader unintended implications on our "right to privacy", by casting a shadow on the fundamental right to privacy, or discrediting the nature of the Privacy Act.

Privacy law is highly contextual. While this is also true of other areas of the law, the basic privacy law mantra is "it all depends on the circumstances" is fundamental. This includes, not only the particular factual situation (which is critical), but also the nature of the privacy interest arising from those facts (what type of privacy interest arises?), and the areas of law engaged and the statutory interface (what part of the privacy landscape is applicable?).

Each aspect of the contextual matrix can influence the decision-making process and the outcome. While it is clearly helpful or even necessary to look to related contexts or decisions for guidance, this needs to be done with eyes wide open to the broader implications.

Scope of the Privacy Act – informational privacy

The statutory scheme of the Act is to provide a code for resolving certain types of privacy disputes, as a necessary precondition to bringing proceedings.

Although broadly named, the Act is primarily New Zealand's data protection statute and specifically regulates informational privacy, rather than the entire privacy field. While I have powers to inquire into broader privacy issues, my complaints jurisdiction is limited to investigating alleged breaches of the information privacy principles and the extent to which there is a resulting identifiable privacy "harm".

Interference with privacy

An important element of the statutory scheme is the pivotal concept of an "interference with privacy" in section 66. Generally, as well as a breach of a principle, the breach must have resulted in actual or potential loss or adverse effects or significant humiliation, significant loss of dignity or significant injury to the feelings on the individual.

However breaches of process under privacy principle 6 (access to one's own personal information) or principle 7 (correction of one's own information) automatically create an interference with privacy, regardless of whether the breach caused any specific form of "harm".

Principle 6, in particular, is accorded special significance in the statutory scheme. It has been described as a fundamental right of constitutional significance and is the only principle directly enforceable in the courts (against public sector agencies). This expressly preserves the legal rights formerly housed in the Official Information Act 1982.

Not enforceable in the courts (with one exception)

The generally expressed information privacy principles and the highly contextual nature of their application mean that the principles are not amenable to direct enforcement in the courts.

Except for principle 6 in relation to public sector agencies, the privacy principles are not enforceable in a court of law (s 11), but the Courts have been prepared to take notice of them in assessing the actions of parties to disputes, for example in the employment context or in discovery, as well as aspects of tort law and human rights cases.

However the other principles are expressly stated not to confer any legal right that is enforceable

in a court of law (s11(2)). At the time the Privacy Act was introduced as a Bill, it was considered more appropriate for the principles generally to be enforced "through conciliation by a public official who specialises in information privacy. Accordingly, the Act provides an exclusive mechanism for the enforcement of the principles for breaches that meet the threshold of an "interference with privacy" in terms of s 66, as determined by the Commissioner or in Human Rights Review Tribunal proceedings.

The Act is rather a compromise or hybrid as it provides both a low level dispute resolution scheme while at the same time recognising the importance of informational privacy and providing a gateway for aggrieved individuals to bring proceedings via the Human Rights Review Tribunal.

Breadth and flexibility

The Privacy Act is a set of principles that are sufficiently flexible to provide a framework for agencies for the vast majority of scenarios involving personal information. Its information privacy principles are technology neutral, and provide exceptions to accommodate an agency's legitimate business needs.

The Privacy Act regulates the handling of personal information. The Act adopts a principles-base approach, rather setting strict rules. The 12 privacy principles provide a roadmap to the way personal information can be collected, stored, used, and disclosed. They also entitle an individual to request access to their own personal information (IPP 6) and to request the correction of their personal information (IPP 7). The advantage of the principles-based approach is that it allows the Act to remain relevant as technology changes.

The Privacy Act regulates the collection and disclosure of personal information about individuals. It covers both the public and private sectors. Apart from some specific exceptions (including the news media and the courts) it has blanket coverage across a variety of civil, regulatory and criminal law contexts.

However, section 7 of the Privacy Act makes certain principles (access and disclosure) subject to any particular other enactment. This means that those privacy principles need to be construed in light of any other relevant legislation that is either more restrictive about how information is to be treated, or more permissive, or otherwise regulates the manner in which personal information may be obtained or made available. One example is s 15 of the Children, Young Persons and their Families Act 1989, disclosures of personal information are permitted in circumstances where there is a risk of harm to a child or young person.[18]

"Personal information" is "information about an identifiable individual." The Act does not define "information" and the ordinary meaning of the word "that which informs, instructs, tells or makes aware" applies. The Human Rights Review Tribunal has taken a wide and purpose approach to the definition. It is not necessary that the individual is identifiable from the information alone. It can apply also apply where an individual could reasonably be expected to be identifiable from readily available sources.

The Privacy Act therefore applies to all types of personal information, from the routine or trivial to the highly sensitive. This is regardless of how the information is generated or recorded, noting that information can even be held in someone's memory. The Act applies broadly, by virtue of this definition, because of the myriad of circumstances that can impact on information privacy. A piece of information can be mundane in one context, but the level of sensitivity can be significantly increased when it is combined with or linked to other information.

Focus on dispute resolution

There is a clear public policy benefit in disposing of privacy complaints efficiently and effectively so that only a limited and manageable number of cases proceed to the Human Rights Review Tribunal. Accordingly, the Act reflects a clear emphasis on dispute resolution.

As well as an investigation function, I have an express conciliation function (s 69(1)(b)). I am to use my best endeavours to secure a settlement and assurance if it appears that such outcomes may be possible and appropriate (s 74) and once I have investigated a complaint that has substance (s 77). I can call the parties to a compulsory conference to try to obtain an agreement on resolution (s 76(2)(b)).

This feature of the Act means that a reasonable proportion of complaints will track down the path of alternative dispute resolution and do not require a formal finding or a certificate of investigation.

18 *Section 15, CYF Act: Reporting of ill-treatment or neglect of child or young person: Any person who believes that any child or young person has been, or is likely to be, harmed (whether physically, emotionally, or sexually), ill-treated, abused, neglected, or deprived may report the matter to a social worker or a constable.*

Wider influence

While the Act can be seen as a private law scheme to provide civil remedies and dispute resolution, nevertheless its provenance defines individual rights against the State.

There are statutory sign-posts to the Privacy Act that reflect its importance. For example, some statutes require a consultation process with the Privacy Commissioner or apply the Act's complaints process by cross reference. Other provisions contain broader indications of the Act's importance e.g. section 5 of the Search and Surveillance Act.[19]

The information privacy principles create a public expectation as to the good stewardship of personal information and provide a set of standards against which policy and legislative proposals are measured and amended.

The influence of the Act on policy development can also be noted for example by its inclusion in the principles of legislative design, and in the Cabinet Manual requirement that departments consult the Privacy Commissioner on proposals that impact on personal privacy.

Conclusion

The Privacy Act sets out a roadmap that is designed for the Act's particular statutory scheme. Concepts in the Privacy Act may inform other areas of the law but may not translate directly and there are limits on "enforcing" the principles. I caution against relying unduly on stand-alone provisions from the Act, without taking full note of their place in the statutory scheme, both within the Act and in light of any other statutory considerations.

REFLECTIONS ON THE PRIVACY LANDSCAPE - NO ONE SIZE FITS ALL

Privacy has a chameleon quality and takes a variety of forms in the law. It is apparent that, just as there is no one single unified theory or definition of privacy, neither is there a single privacy right of general application. Aspects of the right to privacy are dispersed throughout our law, and takes on a variety of guises. The building blocks of privacy law are diverse, but related, so as to embed privacy rights or values in a contextually appropriate way.

While it may appear that this is an ad hoc patchwork, I suggest that this is actually a practical and flexible approach and is one of the reasons that privacy rights operate effectively in our legal system. It reflects that no one legal incarnation of privacy can serve all purposes. The context is everything.

Clearly this is because of the need to ensure that due protection of privacy does not overreach into other fundamental rights such as freedom of expression, and rights to justice, unless the privacy intrusion is significant enough that the privacy interest ought to prevail. There are also other societal interests to protect such as the need for security and for law enforcement to effectively investigate and prosecute criminal offending. This is where concepts of necessity, legality, proportionality and reasonableness are of vital importance.

It's a matter of boundary setting in different areas of the law, to keep fundamental rights, societal interests and government actions in balance, and to guard against perverse outcomes. This is done in a variety of ways, whether by broadening or narrowing the scope of the privacy interest, by raising or lowering thresholds, or by including exceptions and defences.

Care needs to be taken in cross-applying concepts from one area of the law to another, with a disciplined approach to borrowing from different areas of the law. While there is a degree of productive cross- fertilisation, I am concerned that legal mechanisms or concepts deployed in one context may/can produce a strange result or raise uncertainty if translated to a different context without careful assessment.

Privacy rights and interests must be assessed in a deliberative, contextually specific way, as to both the factual and legal contexts. This approach, of course, applies to other areas of the law, but I suggest that it is an approach which must be applied with rigour in the privacy context . Otherwise, there is risk that overlaps between different areas of privacy law will become blurred, difficult to reconcile and to subsequently apply.

Where a privacy issue in the legal landscape arises may fundamentally influence how it is considered and disposed of. It may also make precedents either more or less relevant depending on the extent of contextual similarity. Privacy is a fundamental human right, therefore care must also been taken not to inadvertently limit that right.

19 *The purpose of this Act is to facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values by – (b) providing rules that recognise the importance of the rights and entitlements affirmed in other enactments, including the New Zealand Bill of Rights Act 1990, the Privacy Act 1993, and the Evidence Act 2006.*

THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA:

a unique tool to protect our freedoms and fundamental rights[1]

SOPHIE
KWASNY

Sophie Kwasny es Jefe de la Unidad de Protección de Datos del Consejo de Europa y es responsable de la elaboración de estándares (en particular, el actual ejercicio de modernización del Convenio 108) y políticas de protección de datos y privacidad, incluidas las nuevas tecnologías e Internet. Es graduada de la Universidad de Derecho de Estrasburgo y trabaja para el Consejo de Europa desde hace más de 15 años en una variedad de temas que abarcan desde la reforma penitenciaria, la independencia del Poder Judicial o la normatividad sobre nacionalidad.

SUMARIO

1 *The views expressed are those of the author.*

RESUMEN

En su artículo la autora procede a una revisión de la situación actual de la Convención Nº 108 del Consejo de Europa para la protección de los individuos en relación al tratamiento automatizado de datos personales. Se destaca la inclusión de países no europeos al ámbito de la Convención, como partes, entre los que se encuentra Uruguay.

En relación a la Convención actual y a su protocolo adicional la autora menciona la existencia de principios vinculados al tratamiento, a la calidad de los datos, a los derechos de los titulares -especialmente los de información, acceso y rectificación-, al tratamiento de datos sensibles -que requiere necesariamente de salvaguardas adecuadas- y a la regulación de los flujos transfronterizos de datos y la asistencia mutua entre estados partes.

La Convención se encuentra actualmente en un proceso de modernización con los objetivos de mantener su naturaleza neutral desde lo general y lo tecnológico, preservar su coherencia y compatibilidad con otros marcos legales internacionales y reafirmar su potencial como estándar universal. En ese sentido, se desarrollan por la autora modificaciones importantes en una serie de ítems, a lo largo del artículo.

INTRODUCTION

The Convention for the protection of individuals with regard to automatic processing of personal data[2] (hereafter referred to as 'Convention 108') was adopted by the Council of Europe and opened for signature in Strasbourg on 28 January 1981.

It was at that time, and still is, the only legally binding international instrument in the field of data protection. Convention 108 is open for accession by any country in the world as over 35 years ago, its drafters already envisioned the global nature of data flows and acknowledged the need to spread a common understanding of the protection of personal data.

The Convention currently gathers a total of 50 countries that are legally bound by it.

47 of them are the member States of the Council of Europe and 3 are from other regions of the world, like Uruguay.

Uruguay was the first country from another region than Europe to accede to the Convention, in 2013. It has since been joined by Mauritius and Senegal, and more are to come as the Kingdom of Morocco, Tunisia, Cap Verde and Burkina Faso have been invited to accede to the Convention. More will follow hopefully, as should be the case for Argentina which just requested to be invited to accede.

Under Convention 108, the Parties are required to take the necessary steps in their domestic legislation to apply the data protection principles it lays down in order to ensure respect for the fundamental human rights of individuals with regard to the processing of personal data. The objective is simple: allowing as many countries as possible from all regions of the world, to adopt legislation based on common principles, bring them closer to exchange and cooperate, and facilitate information flows.

Protecting the individuals with the regard to the processing of their personal data is the pre-condition to the functioning of democratic societies and this is the backbone of the action of the Council of Europe in the field

THE CONVENTION TODAY

Convention 108 protects the individuals in the context of the processing of personal data. It has been complemented in 2001 by an additional protocol[3] dealing more specifically with the supervisory authorities (also called 'data protection authorities') and transborder data flows to non-Parties to the Convention.

Its scope of application is fully horizontal: it applies in an indistinct manner to the public or the private sector, this is one the strengths of the Convention.

The principles laid down in the Convention concern in particular the fair and lawful processing of data, for specified legitimate purposes and for no longer than is necessary.

They concern also the quality of the data, in particular that data must be accurate, adequate, relevant and not excessive (proportionality principle).

Furthermore the Convention establishes a right of information of the data subject, a right of access and rectification, as well as the right to have a remedy.

In addition to providing guarantees in relation to the processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal

2 *CETS 108: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm*

3 *CETS 181 : http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm*

record, etc., in the absence of proper legal safeguards.

The Convention also provides for specific security measures that need to accompany the data processing.

Restriction on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

While the Convention provides for free flow of personal data between Parties to the Convention, it also imposes some restrictions on transborder flows of personal data to States which do not provide equivalent protection.

Finally, the Convention calls upon the Parties to render each other mutual assistance and provides a framework for the cooperation of the designated authorities.

Another important achievement of the normative data protection work of the Council of Europe is the flexible manner in which the basic and general principles established by Convention 108 have been unfolded to various specific sectors such as law enforcement, employment, statistics, etc[4].

Over 35 years of existence and in light of the increasing collection and use of personal data in the new digital environment, it has been decided to review the provisions of the Convention in order to better adapt it to emerging challenges and strengthen the protection of individuals.

... AND THE CONVENTION TOMORROW...

The process to modernise Convention 108 started formally on the occasion of the 30th anniversary of Convention 108 (i.e. 28 January 2011, a date celebrated globally as data protection day) and we have now reached, after six years of negotiations, the final stage of this crucial work.

The modernisation of Convention 108 pursues two main objectives: to deal with challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation.

While the core principles contained in Convention 108 have stood the test of time and its technologically-neutral, principle-based approach constitutes an undeniable strength, its original principles have to be applied to the new realities of the on-line world while new practices have also led to the recognition of new principles in the field. The principles of accountability, data minimisation, privacy by design, etc. are now acknowledged as key elements of the protection mechanism and have to be integrated in our modern instrument.

The objectives pursued with the modernisation exercise are the following:

- maintain the general and technologically neutral nature of the Convention with more detailed sectoral texts by way of soft-law instruments (opinions and recommendations);
- preserve the coherence and compatibility with other relevant international legal frameworks;
- reaffirm the Convention's potential as a universal standard.

The main novelties brought by the modernisation of the Convention can be summarised as follows:

Object and purpose of the Convention (Article 1)

Under article 1, it is proposed to underline to a greater extent the objective of the Convention, namely to guarantee to every individuals within the jurisdiction of one of the Parties, regardless of their nationality or place of residence, the protection of their personal data when undergoing processing, thus contributing to respect for their rights and fundamental freedoms, and in particular their right to privacy.

Using this wording, the Convention does not create a hierarchy of rights but highlights the fact that the processing of personal data may positively enable the exercise of other fundamental rights and freedoms, which can thus be facilitated by guaranteeing the right to data protection.

Definitions and scope of application (Articles 2 and 3)

While essential notions such as the definition of personal data and the one of data subjects will not be modified, other changes are proposed in the definitions: the concept of 'file' is proposed to be abandoned. 'Controller of a data file' will be replaced by 'data controller', in addition to which the terms 'processor' and 'recipient' will be used.

It is furthermore proposed to extend the scope of application to include both automated and non-automated processing of personal data (manual processing where the data form part of a structure which makes it possible to search for data by data subject according to pre-determined criteria) which falls under the jurisdiction of a party to the

4 *The list of sectorial Recommendations is accessible at: http://www.coe.int/en/web/data-protection/legal-instruments*

Convention. The scope of application will naturally continue to cover the processing in the private and public sector indistinctly, as this is one of the great strengths of the Convention.

On the other hand, the Convention will no longer apply to data processing carried out by a natural person for the exercise of purely personal our household activities.

Duties of the parties (Article 4)

Each Party has to adopt in its own domestic laws the measures necessary to give effect to the provisions of the Convention. Furthermore, each Party should demonstrate that such measures have actually been taken and are effective and accept that the Convention Committee may check that these requirements have been complied with. The Parties must also contribute actively to this evaluation process.

Legitimacy of data processing and quality of data (Article 5)

It is proposed to clarify the application of the principle of proportionality (which deals essentially with data which should be adequate, relevant and not excessive in relation to the purposes for which they are stored) to underline that it should apply throughout the entire processing, and in particular in respect of the means and methods used in the processing. This principle is also complemented by the principle of data minimisation, according to which the collection and processing of data should be limited to an absolute minimum.

Currently, the Convention does not provide a list of grounds under which data processing is permitted. It sets out in simple and general terms that personal data may only be processed lawfully. It is proposed to introduce a new provision under which data processing may only be carried out on the basis of the consent (which to be valid has to satisfy several criteria) of the data subject or of some other legitimate basis laid down by law.

Sensitive data (Article 6)

In the case of sensitive data, it is proposed to review the catalogue of sensitive data, to which will be added genetic and biometric data, as well as data processed for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life (personal data relating to offences, criminal proceedings and convictions will continue to require complementary protection).

Data security (Article 7)

In terms of data security, the requirement to notify, without delay, any security breaches is being introduced. However, this requirement is limited to cases which may seriously interfere with the rights and fundamental freedoms of data subjects. These should be notified, at least, to the supervisory authorities.

Transparency of processing (Article 7bis)

Controllers will have the obligation to guarantee transparency of the data processing and will to that end have to provide a minimum of information, in particular relating to their identity and usual place of residence or establishment, on the purposes of the processing, the data recipients, how long the data will be stored and how the data subjects will exercise their rights. If required, they should provide additional information if this is necessary to ensure that data is fairly processed.

Rights of data subjects (article 8)

It is proposed that data subjects be given greater rights so that they have greater control over their data.

The modernised Convention will extend the catalogue of information to be transmitted to data subjects when they exercise their right of access. Furthermore, data subjects will be entitled to obtain knowledge of the reasoning underlying the data processing, the results of which are applied to him/her. This new right is particularly important in terms of profiling of individuals[5]. It is associated with another new right, namely the right not to be subjected to a decision which affects the data subject to a significant degree or which has legal effect with respect to them when this decision is taken solely on the basis of automatic data processing, without the data subject having their views taken into consideration. Data subjects will have a right to object at any time to their personal data being processed, unless the controller demonstrates compelling legitimate grounds for the processing which override their interests or rights and fundamental freedoms.

Additional obligations (Article 8bis)

The modernisation of the Convention should also increase the responsibilities of those who process

5 *On this subject see Recommendation (2010) 13 on the Protection of Individuals with regard to Automatic Processing of Personal Data in the context of profiling and its Explanatory memorandum.*

data or have data processed. The project establishes the principle that the controller is responsible for respecting data subjects' right to data protection at all stages of data processing and should take all appropriate measures – including when the processing is outsourced – to ensure that data protection provisions are respected. They will have to be able to demonstrate compliance, integrate privacy by design, and examine the likely impact of the intended data processing on the rights and fundamental freedoms of data subjects.

Exceptions and Restrictions (Article 9)

This provision is one of the most debated, and upon which discussions are still underway. The main idea is that the rights laid down by the Convention are not absolute and may be limited when this is foreseen by the law and constitutes a necessary measure in a democratic society on the basis of specified and limited grounds (such as national security). It is important to note that contrary to the existing provisions of Convention 108, Parties to the Convention will no longer be able to exclude from the scope of application of the Convention certain types of processing, as is currently the case through the possibility under Article 3 to make declarations.

Transborder data flows (Article 12)

The aim of this provision is to facilitate, where applicable, the free flow of information regardless of frontiers, while ensuring an appropriate protection of individuals with regard to the processing of personal data.

The purpose of the transborder flow regime is to ensure that information originally processed within the jurisdiction of a Party, when the processing is subsequently submitted to the jurisdiction of a State which is not Party to the Convention, continues to be processed in line with data protection principles that are appropriate with regard to the Convention. What is important is that data subjects originally concerned by the data processed within the jurisdiction of a Party to the Convention always remain protected by appropriate data protection principles no matter the particular law applicable to the processing at stake.

Data flows between Parties cannot be prohibited or subject to special authorisation as all of them, having subscribed to the common core of data protection provisions set out in the Convention, offer a level of protection considered appropriate. In the absence of additional regional binding harmonised rules governing data flows, data flows between Parties should thus operate freely.

Regarding transborder flows of data to a recipient that is not subject to the jurisdiction of a Party, an appropriate level of protection in the recipient State or organisation is to be guaranteed. As this cannot be presumed since the recipient is not a Party, the Convention establishes two main means to ensure that the level of data protection is indeed appropriate; either by law, or by ad hoc or approved standardised safeguards that are legally binding and enforceable, as well as duly implemented.

Supervisory authorities (Article 12bis)

The modernisation also addresses the issue of supervisory authorities. Building on Article 1 of the additional protocol, the draft complements the catalogue of the authorities' powers with a provision that, in addition to their powers to intervene, investigate, engage in legal proceedings or bring to the attention of the judicial authorities violations of data protection provisions, the authorities also have a duty to raise awareness, provide information and educate all players involved (data subjects, controllers, processors etc.). It also allows the authorities to take decisions and impose sanctions. Furthermore, the draft specifies that the supervisory authorities should be independent in exercising these tasks and powers. The draft also emphasises the importance of cooperation between supervisory authorities, which should work together to a sufficient degree in order to accomplish their tasks, in particular by exchanging information on data transfers or on their laws and administrative practices in the field of data protection. They should also work together to coordinate their investigations or interventions, and to conduct joint activities.

Convention Committee (Articles 18, 19 and 20)

This committee plays a fundamental role in interpreting the Convention, encouraging the exchange of information between the Parties and developing data protection standards. The role and powers of this committee should be strengthened with the Modernised Convention. It will no longer play a purely consultative role but will also have assessment and monitoring powers. It is proposed that it should in the future be able to provide an opinion on the level of data protection provided by a state or international organisation before accession to the Convention. It will also be able to assess the compliance of the domestic law of the Party concerned and determine the effectiveness of the measures taken (existence of

a supervisory authority, responsibilities, existence of effective legal remedies). It will also be able to assess whether the legal norms governing the data transfers provide sufficient guarantee of an appropriate level of data protection.

THE IMPORTANCE OF CONVENTION 108 IN A NUTSHELL

The importance and relevance of the current modernisation of Convention 108 is to be underlined, at a time where countries from different regions of the world are calling for a global instrument safeguarding the right to privacy. Indeed, with increasing flows of ubiquitous data, processed by the private sector and public sector alike (even more so in a mass surveillance context) and the related legal uncertainty comes the necessity to ensure that common core principles are in place in as many countries as possible around the globe to guarantee an appropriate level of protection of individuals with regard to the processing of personal data.

The fact that Mexico, Indonesia, Japan, the Philippines and Korea has in the past year decided to join the work of the Committee of the Convention, in Strasbourg, in France is a clear indication of the global interest for the Convention, something that Uruguay seized already 4 years ago.

NUEVO MARCO EUROPEO DE PROTECCIÓN DE LOS DATOS PNR*

ÁLVARO
SÁNCHEZ BRAVO

Doctor en Derecho. Profesor de la Facultad de Derecho de la Universidad de Sevilla. Presidente de la Asociación Andaluza de Derecho, Medio Ambiente y Desarrollo Sostenible. Expert European Research Council Executive Agency. European Comission. Académico Correspondiente Academia Sul RioGrandense de Direito do Trabalho. Coeditor Revista Internacional de Direito Ambiental (RIDA).

SUMARIO

* *Texto del trabajo presentado como conclusión de los Estudios de PosDoctorado en el Programa de Pós-Graduação em Direito – Mestrado e Doutorado. Universidade Regional Integrada do Alto Uruguai e das Missões. URI-San, bajo la supervisión del Prof. Dr. Joao Martin Bertaso.*

RESUMEN

El autor reseña claramente la problemática existente con respecto al tratamiento de los datos vinculados a los nombres de pasajeros de aerolíneas (o PNR -por sus siglas en inglés passenger name records-). Tratamiento fuertemente influido por los contralores asociados al combate contra el terrorismo.

En particular, el autor hace referencia al proceso llevado adelante por la Unión Europea, considerando especialmente la directiva (UE) 2016/681, respecto de la cuál efectúa un pormenorizado análisis.

Hace referencia también a la postura de los Estados Unidos y a los matices y diferencias con la postura reflejada en el documento antedicho.

Finalmente, el autor concluye poniendo énfasis en la necesidad de conservar el principio de inocencia al amparo de las nuevas realidades, no cediendo ante el nuevo paradigma de "seguridad a toda costa" y proponiendo continuar la lucha contra la violencia y el terrorismo con respeto a los derechos y libertades de los individuos.

INTRODUCCIÓN

La protección de las personas físicas en lo tocante al tratamiento de datos personales constituye un derecho fundamental, recogido en la Carta de los Derechos Fundamentales de la Unión Europea (art. 8.1)[1] y en el Tratado de Funcionamiento de la Unión Europea (art. 16.)[2], estableciéndose que toda persona tiene derecho a la protección de los datos personales que le conciernen.

La sociedad globalizada[3] exige, cada vez más, un acopio, utilización y transmisión de datos personales que abarca las actividades más cotidianas, y las decisiones globales más relevantes. En el ámbito de la Unión europea, las normas y principios relativos a la protección de datos personales deben, independientemente de la nacionalidad o residencia de sus titulares, respetar sus libertades y derechos fundamentales; contribuyendo igualmente a la consecución de un espacio europeo de libertad, seguridad y justicia[4].

Ahora bien, esa globalización también a ha llegado a las actividades delictivas, al terrorismo y a otras formas de barbarie que intentan destruir o menoscabar la pacífica convivencia, como cimiento de sociedades democráticas y libres.

El terror "viaja" o al menos lo intenta, por todo el planeta, por lo que se hizo necesario el establecimiento de unos mecanismos de control y vigilancia y de intercambio de información que permitan detectar, prevenir y contrarrestar los efectos delos atentados criminales. Ahora bien, esto no puede hacerse de cualquier forma, a cualquier preciso, pues con el pretexto de defender la democracia, podemos convertirla en un estado totalitario, sometiendo a los ciudadanos a un control sistemático de sus datos personales y actividades vinculadas.

Los desgraciados acontecimientos del 11 de septiembre de 2001, en New York, llevaron a Estados Unidos a adoptar una serie de medidas legislativas y policiales tendentes a blindar su territorio frente a eventuales nuevos ataques terroristas. La promulgación de la PatriotAct y la creación de la Oficina Nacional de Seguridad son solo algunos ejemplos relevantes de estas iniciativas.

Paralelamente, en aplicación de la Ley de Seguridad en los Transportes la Administración estadounidense obligó unilateralmente, bajo la amenaza de fuertes sanciones e incluso la pérdida de los derechos de aterrizaje, a las compañías aéreas que operan vuelos con destino a su territorio a transferirle los datos personales sobre pasajeros

1 *ARTÍCULO 8.- Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.*

2 *Artículo 16 (antiguo artículo 286 TCE) 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.*

3 *SANCHEZ BRAVO, A., Internet y la sociedad europea de la información: implicaciones para los ciudadanos, Publicaciones de la Universidad de Sevilla, 2001.*

4 *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DO L 119.04.05.2016. Considerando (2).*

y los miembros de las tripulaciones de los vuelos con destino procedentes de este país. En concreto las compañías aéreas debían suministrar al Servicio de Aduanas y Protección de Fronteras (abreviatura en inglés, CBP) un acceso electrónico a los datos de los pasajeros que figuran en el *registro de los nombres de los pasajeros* (abreviatura en inglés, ***PNR***) para los vuelos que tienen destino, origen o que hacen escala en Estados Unidos[5].

Esta imposición suponía en el ámbito comunitario europeo la necesidad de considerar si el cumplimiento de las exigencias estadounidenses por parte de las compañías aéreas supone una subversión de las exigencias y garantías que para la protección de datos establece la Directiva 95/46/CE[6]. En concreto su artículo 25, establece que para la transferencia a terceros países, éstos deberán garantizar un "nivel de protección adecuado". Y es precisamente la determinación de ese nivel el que desató la polémica entre las instituciones comunitarias y la zozobra en los ciudadanos.

No obstante, la problemática terrorista soportada por Estados Unidos, se ha expandido en los últimos años al territorio europeo, que ha soportado, y soporta execrables atentados que desde diversas ideologías radicales, fundamentalmente de base islamista, intentan colocar en jaque nuestra modelo civilizatorio, nuestra democracia, y en definitiva, nuestros derechos humanos.

Ello, como veremos ha llevado con extraordinaria celeridad, a la adopción de la normativa necesaria para un correcto uso de los datos PNR, que sea coherente con la normativa europea de protección de datos, recientemente modificada.

Es por ello que resulta interesante mostrar cual fue el *iter* legislativo, y, sobre todo, constatar como cuando los hechos nos son más próximos se aceleran las soluciones, aún a riesgo de conculcar los derechos de los ciudadanos.

ACUERDO DE LA COMISIÓN EUROPEA DE 2004

Tras las medidas aprobadas por el Gobierno USA de acceso a las listas de los pasajeros, las compañías aéreas europeas, con el respaldo de la Comisión, plantearon serias objeciones a su aplicación en cuanto podía vulnera la normativa comunitaria de protección de datos. No obstante, pese a unos iniciales aplazamientos, las autoridades estadounidenses, y concretamente el CBP, comunicó que a partir del día 5 de marzo de 2003 comenzaría a imponer sanciones.

Ante tal situación, la Comisión inició una serie de negociaciones con el Departamento estadounidense de Seguridad Interior (DHS) en un intento de garantizar que los datos del PNR gocen de una protección adecuada, en línea con la normativa europea de protección de datos.

En diciembre de 2003, la Comisión declaró haber llegado a un acuerdo con Estados Unidos, y manifestó su disposición para elaborar una Decisión que estableciese que el Servicio de Aduanas y protección de Fronteras de Estados Unidos (abreviatura en inglés, CBP) garantizaba un nivel de protección adecuado.

Dicha Decisión fue adoptada por la Comisión el 14 de mayo de 2004[7], incorporando como anexo los Compromisos del CBP.

La Decisión establece dos consideraciones respecto a su ámbito material de aplicación;

El CBP ofrece, conforme al apartado 2 del art. 25 de la Directiva 95/46[8], un nivel de protección adecuado de los datos de PNR que se transfieren desde la Comunidad relativos a vuelos con destino u origen en Estados Unidos.

Los compromisos de la Decisión no empecen el cumplimiento de otras condiciones o restricciones que puedan imponerse en aplicación de la Directiva 95/46.

Pero quizás lo más relevante sea considerar el contenido de los Compromisos del CBP. Dichos compromisos suponían, a juicio de la Comisión,

5 *Grupo del artículo 29 sobre protección de datos. Dictamen 4/2003 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de los pasajeros, 13 de junio de 2003, 11070/03/ES WP 78.*

6 *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. Sobre su contenido, vid., SANCHEZ BRAVO, A., La protección del derecho a la libertad informática en la Unión Europea, Publicaciones de la Universidad de Sevilla, 1998; e Internet y la sociedad europea de la información: implicaciones para los ciudadanos, Publicaciones de la Universidad de Sevilla, 2001.*

7 *3C(2004) 1914. 2004/535/CE. DOUE L 235/11. 06.07.2004.*

8 *Art. 25.2 Directiva 95/46: " El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad vigentes en dichos países".*

una importante mejora de la situación, que se concreta en:

Las autoridades estadounidenses recogerían y conservarían menos datos. Se acordó una lista de 34 categorías de datos (los PNR de algunas compañías aéreas contienen más de 60 campos) y en la mayoría de los registros individuales sólo se cumplimentará un número limitado de estos campos.

Los datos sensibles, como las preferencias alimentarias o las necesidades especiales de los pasajeros, que pueden revelar su raza, religión o estado de salud, no se transferirían o, si se transfirieran, serían filtrados y eliminados por el CBP.

Los datos del PNR se utilizarían exclusivamente para prevenir y combatir el terrorismo y los delitos conexos, y otros delitos graves, incluida la delincuencia organizada, que tengan carácter transnacional, lo que supone una mayor precisión de las finalidades anteriormente previstas por Estados Unidos.

Los datos del PNR no se compartirían «en masa»; se intentaba responder así a las preocupaciones relativas a la utilización de estos datos en planes de vigilancia generalizada que se están preparando en Estados Unidos. El CBP compartiría los datos del PNR de forma limitada, caso por caso, y únicamente para las finalidades acordadas; cuando los datos procedentes de la UE se transfieran conforme a estas condiciones estrictas a las autoridades policiales de países distintos de Estados Unidos, se comunicará este hecho sistemáticamente a una autoridad de la UE designada al efecto.

La mayoría de los datos PNR se suprimirían al cabo de tres años y medio (frente a los cincuenta años que proponía en un principio Estados Unidos). Los ficheros a los que se haya accedido se conservarán en un fichero de datos suprimidos durante ocho años suplementarios con fines de auditoría (frente al plazo indefinido que se pretendía en un principio).

Las autoridades de protección de datos de la UE tendrían la posibilidad de examinar con el Director responsable de la protección de la intimidad (Chief Privacy Officer) del DHS los casos de los pasajeros cuyas denuncias, por ejemplo, por presuntos abusos en la utilización de los datos que les conciernen o por no rectificación de datos imprecisos no haya resuelto de forma satisfactoria el DHS[9].

El Acuerdo elaborado por la Comisión fue aprobado por el Consejo de la Unión en su Decisión de 17 de mayo de 2004[10], facultando al Presidente del Consejo para que designe la/s persona/s que firmarán el Acuerdo en nombre de la Comunidad Europea.

LAS OBJECIONES DEL GRUPO DEL ART. 29 SOBRE PROTECCIÓN DE DATOS.

El Grupo del art. 29[11], emitió un primer Dictamen sobre estas cuestiones en octubre de 2002[12], y un segundo dictamen en junio de 2003[13], donde ponía de manifiesto serias objeciones a los Acuerdos que entonces se negociaban y que ponían en cuestión el régimen protector que respecto a los datos personales se había conseguido en la Unión. En concreto, se cuestionaba la finalidad de las transferencias, la adecuación al principio de proporcionalidad de los datos a transferir, el tratamiento de los datos sensibles, el momento de las transferencias y el período de conservación de los datos, la opción por un sistema de transferencia "push"[14] el control estricto de la posterior cesión de datos a terceros, las garantías y los derechos de los interesados, el mecanismo de aplicación y de resolución de los litigios, y el nivel de los compromisos.

Posteriormente en su Dictamen de enero de 2004[15], tras haber recibido de la Comisión la versión actualizada de los Acuerdos con Estados Unidos, y constatar la mejora en los Acuerdos, concluye de manera contundente que no puede estimarse que se haya alcanzado un nivel adecuado de protección de los datos. A mayor abundamiento, indica que cualquier decisión al respecto debe cumplirse como exigencias indispensables:

- Calidad de los datos:

la finalidad de la transferencia de datos debe ser únicamente la lucha contra los actos de terrorismo y determinados delitos conexos que habrá que definir; la lista de los datos que deben transferirse debe ser proporcionada y no excesiva; el cotejo de

9 *IP/04/650.*

10 *DO L 183/83, 20.05.2004.*

11 *Grupo creado en virtud del art. 29 de la Directiva 95/46/CE. Se trata de un organismo de la Unión, de naturaleza consultiva e independiente, para la protección de datos y el derecho a la intimidad. Según el art. 30 tendrá, de entre sus cometidos: "b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros."*

12 *Dictamen 6/2002, de 24 de octubre, WP 66. http://europa.eu.int/comm/internal_market/privacy/workingroup_fr.htm*

13 *Dictamen 4/2003, de 13 de junio, WP 78.*

14 *Según el propio Grupo del art. 29, "el único mecanismo de transferencia de datos cuya aplicación no suscita problemas importantes es el sistema push, según el cual las compañías aéreas seleccionan y transfieren los datos a las autoridades estadounidenses, en oposición al sistema pull, en el que las autoridades estadounidenses disponen de acceso directo en línea a las bases de datos de las compañías aéreas y de los sistemas de reserva." Dictamen 4/2003, cit., p. 6.*

15 *Dictamen 2/2004, de 29 de enero de 2004, WP 87.*

datos con los de personas sospechosas debe atenerse a normas de elevada calidad que garanticen la certeza de los resultados; los períodos de conservación de los datos deben ser cortos y proporcionados;los datos de los pasajeros no deben utilizarse para implantar y/o probar el sistema CAPPS II[16], o sistemas similares.

- Los datos sensibles no deben transmitirse.
- Derechos de los interesados:

deben facilitarse a los pasajeros información clara, actual y comprensible; debe garantizarse sin discriminación un derecho de acceso y rectificación; deben preverse disposiciones suficientes que garanticen a los pasajeros el acceso a un mecanismo de recurso verdaderamente independiente.

- Nivel de compromiso de las autoridades estadounidenses:
- los compromisos asumidos por las autoridades estadounidenses deben ser plenamente vinculantes para Estados Unidos; procede clarificar el ámbito de aplicación, la base jurídica y el valor de un posible «acuerdo internacional ligero».
- Las transferencias posteriores de datos del PNR a otras administraciones o autoridades extranjeras deben limitarse estrictamente.
- Método de transferencia: conviene establecer un método de transferencia «push», es decir, que los datos sean seleccionados y transferidos por las compañías aéreas a las autoridades estadounidenses.

Tras la aprobación del Acuerdo por la Comisión y el Consejo, el Grupo volvió a posicionarse, en su Dictamen de junio de 2004[17], claramente en contra del contenido del Acuerdo, señalando que la "Comisión no ha tenido en cuenta, más que parcialmente las exigencias mínimas formuladas por el Grupo", y exhortando a que, como mal menor, se adopten una serie de medidas urgentes para "evitar al máximo los ataques a los derechos de los pasajeros"[18].

Posteriormente, en su Dictamen de septiembre de 2004[19], ha elaborado una serie de orientaciones acerca de las informaciones que deben suministrarse a los pasajeros, donde de manera simple y didáctica se pasa revista a todas las cuestiones que pueden surgir respecto a la recepción por el CBP de los datos PNR de los pasajeros de vuelos entre la Unión Europea y Estados Unidos.

LA FIRME POSICIÓN DEL PARLAMENTO EUROPEO

El Parlamento Europeo, una vez tuvo conocimiento de las negociaciones de la Comisión, y a la vista de la propuesta de Decisión, se posicionó abiertamente en contra del mismo, tanto por cuestiones de forma, como en lo atinente al fondo de los acuerdos que en ese momento se pretendían adoptar. Tal es así que en su Resolución de marzo de 2004[20], señala: *"6. Pide a la Comisión que bloquee: a) el sistema "pull" a partir del 1 de julio de 2004, y que desde esa fecha aplique el sistema "push" con los 19 puntos propuestos el 13 de junio de 2003 por el Grupo a que se refiere el artículo 29 de la Directiva 95/46/CE; b) las iniciativas para crear una gestión europea centralizada de los datos de PNR, tal como contempla la Comunicación COM (03) 826 y ha confirmado recientemente el comisario competente a la comisión parlamentaria, en la medida en que, en las actuales circunstancias, esas iniciativas violan los principios de proporcionalidad y subsidiariedad;*

7. Entretanto, se reserva el derecho a recurrir al Tribunal de Justicia en el caso de que la Comisión Europea adoptara el proyecto de Decisión; asimismo, recuerda a la Comisión el principio de cooperación leal entre las

16 *El sistema CAPPS II ha sido desarrollado por la Oficina de Seguridad Nacional de los Estados Unidos; organismo creado por la Administración Bush tras los atentados del 11-S. El CAPPS I (ComputerAssistedPassenger Pre-Screening. Preinspección de Pasajeros asistida por Ordenador) se basaba exclusivamente en el registro de direcciones de los pasajeros, historial de viajes, antecedentes criminales y otras informaciones no determinadas. El CAPPs II introduce un mayor número de variables, además de un acceso a bases de datos comerciales relativos a datos financieros, historiales médicos, seguros y datos de empadronamiento , entre otros. A cada pasajero se le asigna un código de seguridad durante su registro en una compañía aérea: verde, para los que supongan un riesgo mínimo, amarillo para los de un riesgo mayor (situación de alerta) y rojo para los considerados como altamente peligrosos. En función de cada calificación el pasajero es objeto o no de ulteriores revisiones "en profundidad". Cfr. http://www.cem.itesm.mx/dacs/publicaciones/logos/anteriores/n37/fgutierr.html*

17 *Dictamen 6/2004, de 22 de junio, WP 95.*

18 *Estas medidas urgentes se concretarían en: 1) las compañías aéreas deberán modificar tan rápido como sea posible el sistema de transferencia de datos y pasar del sistema "global" al sistema "concreto"; 2) los pasajeros deben ser correctamente informados de la transferencia de los datos; 3) el acuerdo no obliga ni autoriza a las compañías aéreas a recoger otros datos que los registrados y conservados con fines comerciales; 4) deben ponerse en marcha las reuniones periódicas de control del cumplimiento de los Acuerdos, establecidas para verificar el correcto cumplimiento de la protección de datos; y 5) convocatoria de una reunión con las compañías aéreas.*

19 *Dictamen 8/2004, de 30 de septiembre, WP 97.*

20 *P5_TA-PROV (2004)0245. Protección de datos personales de los pasajeros aéreos. Resolución del Parlamento Europeo sobre el proyecto de Decisión de la Comisión por la que se determina el nivel de protección adecuado de los datos personales incluidos en los registros de nombres de pasajeros aéreos (PNR) transferidos a la Oficina de Aduanas y Protección de Fronteras de los Estados Unidos (2004/2011(INI))*

Instituciones, en aplicación del artículo 10 del Tratado, al tiempo que la insta a no adoptar durante el período de elecciones una decisión cuyo contenido corresponda al de la propuesta examinada en la presente Resolución;

8. Se reserva el derecho de recurrir al Tribunal de Justicia para verificar la legalidad del acuerdo internacional previsto y, en particular, su compatibilidad con la protección de un derecho fundamental;

9. Considera de vital importancia que los resultados de las negociaciones no sirvan de modelo para la actividad posterior de la Unión Europa con miras al desarrollo de sus propios medios de lucha contra la delincuencia, así como en materia de almacenamiento de datos y protección de la confidencialidad de los mismos;

10. Insta a la Comisión a que retire el proyecto de Decisión".

El desarrollo de los acontecimientos evidenció como la Comisión y el Consejo hicieron caso omiso a las prevenciones apuntadas por el Parlamento Europeo.

En mayo, el propio Parlamento declaró la no pertinencia de la tramitación por vía de urgencia del Acuerdo sobre transferencia de datos, tal y como había solicitado el Consejo. Además el Parlamento acordó solicitar un dictamen al Tribunal de Justicia sobre la viabilidad de la propuesta, optando por posponer el voto final y reenviando el informe a la Comisión parlamentaria a la espera del dictamen del Alto tribunal comunitario sobre si el acuerdo es compatible o no con la normativa comunitaria[21].

No obstante esta solicitud de dictamen judicial, la Comisión y el Consejo aprobaron, como ya hemos referido, sendas Decisiones dando validez al Acuerdo.

Ante esta actitud la Comisión de Asuntos jurídicos de la Eurocamara pidió, en su reunión del 16 de junio, al Presidente del Parlamento que denunciase la Decisión de la Comisión y el Consejo. El entonces presidente, Pat Cox, tras unos iniciales "titubeos" planteó ante el Tribunal de Justicia de la Unión Europea un recurso de anulacanulación. Su conveniencia la expresa de manera muy elocuente: "Esta decisión ha sido tomada tras una larga consulta y refleja la preocupación de una inmensa mayoría del Parlamento Europeo, en cuanto a la necesidad de defender los derechos y libertades fundamentales de los ciudadanos europeos".

21 *Cfr. http://www.noticias.info/Archivo/2004/200405/20040505/20040505_23258.shtm*

SENTENCIA DEL TJCE DE 30 DE MAYO DE 2006

La sentencia del Tribunal de Justicia Europeo de 30 de mayo de 2006[22] anuló la Decisión de la Comisión sobre el carácter adecuado de la protección y la Decisión del Consejo por la que se concluye un acuerdo en materia de registros de los nombres de los pasajeros (PNR) La sentencia obligaba a las instituciones de la Comunidad a denunciar el Acuerdo con los Estados Unidos en materia de transferencia de datos de pasajeros el 30 de septiembre de 2006, a más tardar. Por esta razón, toda transferencia de datos de pasajeros a las autoridades de los Estados Unidos no tendría fundamente jurídico en el Derecho europeo tras la denuncia de dicho Acuerdo. Como señalo el Grupo de Trabajo del art. 29[23], era posible que fuera necesario introducir medidas a nivel de la legislación nacional, como, por ejemplo, la total suspensión de las transferencias de datos a las autoridades de los Estados Unidos.

Los argumentos son contundentes:

"Sobre la Decisión sobre el carácter adecuado de la protección

En primer lugar, el Tribunal de Justicia examina si la Comisión podía válidamente adoptar la Decisión sobre el carácter adecuado de la protección sobre la base de la Directiva 95/46/CE. A este respecto, recuerda que el artículo 3, apartado 2, de la Directiva excluye de su ámbito de aplicación el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario y, en cualquier caso, el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguri-

22 *SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)de 30 de mayo de 2006. «Protección de las personas físicas en lo que respecta al tratamiento de datospersonales – Transporte aéreo – Decisión 2004/496/CE – Acuerdo entre laComunidad Europea y los Estados Unidos de América – Registros de nombres delos pasajeros que se transfieren al Servicio de aduanas y protección de fronteras delos Estados Unidos de América – Directiva 95/46/CE – Artículo 25 – Estadosterceros – Decisión 2004/535/CE – Nivel de protección adecuado»En los asuntos acumulados C-317/04 y C-318/04. https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/28._Sentencia_de_30_de_mayo_de_2006._Asuntos_C-317-04_y_C-318-04_Parlamento_Europeo_v_Consejo_de_la_Uni-oo-n_Europea.pdf*

23 *DICTAMEN 5/2006 DEL GRUPO DE TRABAJO EN RELACIÓN CON LA PROTECCIÓN DE LAS PERSONAS POR LO QUE SE REFIERE AL TRATAMIENTO DE DATOS PERSONALES sobre la sentencia del Tribunal de Justicia Europeo de 30 de mayo de 2006 en los asuntos acumulados C-317/04 y C-318/04 sobre la transmisión de los registros de nombres de pasajeros a los Estados Unidos. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp122_es.pdf*

dad del Estado y las actividades del Estado en materia penal.

Se desprende de la Decisión sobre el carácter adecuado de la protección que la exigencia de que se transfieran los datos se basa en la normativa estadounidense relativa a la intensificación de la seguridad, que la Comunidad apoya plenamente a Estados Unidos en su lucha contra el terrorismo y que los datos de los PNR deben utilizarse únicamente para los fines de prevención y lucha contra el terrorismo y delitos conexos y otros delitos graves, incluida la delincuencia organizada. En consecuencia, la transferencia de los datos de los PNR al CBP constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal.

Si bien es correcto considerar que los datos de los PNR son inicialmente recogidos por las compañías aéreas en el marco de una actividad comprendida en el ámbito de aplicación del Derecho comunitario, a saber, la venta de un billete de avión que da derecho a una prestación de servicios, sin embargo, el tratamiento de datos contemplado en la Decisión sobre el carácter adecuado de la protección tiene una naturaleza bien distinta. En efecto, el tratamiento de datos a que se refiere esta Decisión no es necesario para la realización de una prestación de servicios, sino que se considera necesario para salvaguardar la seguridad pública y para fines represivos.

El hecho de que los datos de los PNR sean recogidos por operadores privados con fines mercantiles y de que sean éstos quienes organizan su transferencia a un Estado tercero no se opone a que dicha transferencia se considere un tratamiento de datos excluido del ámbito de aplicación de la Directiva. En efecto, esta transferencia se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública.

El Tribunal de Justicia concluye que la Decisión sobre el carácter adecuado de la protección no está comprendida en el ámbito de aplicación de la Directiva dado que se refiere a un tratamiento de datos personales que está excluido de ésta. Por consiguiente, anula dicha Decisión. No es necesario examinar los demás motivos invocados por el Parlamento.

Sobre la Decisión del Consejo

El Tribunal de Justicia señala que el artículo 95 CE en relación con el artículo 25 de la Directiva no puede constituir la base de la competencia de la Comunidad para celebrar el Acuerdo controvertido con Estados Unidos. En efecto, este Acuerdo se refiere a la misma transferencia de datos que la Decisión sobre el carácter adecuado de la protección y, por tanto, a tratamientos de datos que están excluidos del ámbito de aplicación de la Directiva. Por consiguiente, el Tribunal anula la Decisión del Consejo por la que se aprueba la celebración del Acuerdo y no considera necesario examinar los demás motivos invocados por el Parlamento"[24]

Los efectos de la Sentencia no se hicieron esperar, y la presión del gobierno norteamericano tampoco, que continuó en la idea de exigir los datos PNR, si bien intentando adaptarlo a las nuevas exigencias jurisprudenciales de la Unión Europea.

El 27 de junio de 2006, el Consejo decidió autorizar a la Presidencia, asistida por la Comisión, a entablar negociaciones para un Acuerdo con los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional (Department of HomelandSecurity) de los Estados Unidos[25].

El 11 de octubre de 2006, el Departamento de Seguridad del Territorio Nacional de los Estados Unidos envió una nota dirigida a la Presidencia del Consejo y a la Comisión relativa a la interpretación de determinadas disposiciones de los Compromisos publicados el 11 de mayo de 2004 por el DHS en relación con la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas[26].

La respuesta por parte de las instituciones comunitarias, fue la siguiente: "A la vez que tomamos conocimiento del contenido de su nota, deseamos reiterar la importancia que la Unión Europea y los Estados miembros conceden al respeto de los derechos fundamentales, en especial a la protección de los datos personales.

El hecho de que el DHS se comprometa a seguir aplicando los Compromisos permite a la Unión Europea considerar que, a efectos de la aplicación del Acuerdo, el DHS garantiza un nivel adecuado de la protección de datos".

Con base en dichas negociaciones, el 16 de octubre en Luxemburgo y el 19 de octubre, ambos de 2006,

---

24 *Prensa e Información. COMUNICADO DE PRENSA N° 46/06. 30 de mayo de 2006. Sentencia del Tribunal de Justicia en los asuntos acumulados C-317/04 y C-318/04. CJE/06/46.*

25 *DECISIÓN 2006/729/PESC/JAI DEL CONSEJO de 16 de octubre de 2006 relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DOUE C 298/27, 27.10.2006.*

26 *Nota del Departamento de Seguridad del Territorio Nacional (DHS) de los Estados Unidos de América a la Presidencia del Consejo y a la Comisión relativa a la interpretación de determinadas disposiciones de los compromisos publicados el 11 de mayo de 2004 por el DHS en relación con la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas (2006/C259/01), DOUE C 259/1, 21.10.2006.*

se firma el Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

Hasta la fecha la Unión europea sólo ha celebrado acuerdos similares a los descritos anteriormente, también con Canadá y Australia, y limitados al transporte aéreo. En junio de 2015 el Consejo adoptó una Decisión por la que se autoriza la apertura de negociaciones con vistas a un acuerdo con México.

De esta manera, las únicas disposiciones vigentes en materia de transferencia de datos por las compañías aéreas a las autoridades de la UE, eran las contenidas en la Directiva 2004/82/CE del Consejo[27], según la cual las compañías aéreas tienen la obligación de comunicar a las autoridades competentes de los Estados miembros los datos de información anticipada sobre pasajeros (AdvancePassengerInformation, (API).

Los datos API, son datos esencialmente biográficos, que incluyen el número y tipo de documento de viaje utilizado, la nacionalidad, el nombre y apellidos completos, la fecha de nacimiento, el puesto fronterizo de entrada, el código de transporte, los horarios de salida y llegada del transporte, el número total de pasajeros transportados y el lugar de embarque inicial.

No obstante, la transferencia y tratamiento de los datos PNR se considera una aplicación mucho más eficaz en la lucha contra el terrorismo internacional, ya que contienen más elementos y se dispone de ellos antes que de los datos API, lo que permitirá una mayor anticipación[28].

MARCO JURÍDICO DATOS PNR EN LA UNIÓN EUROPEA: DIRECTIVA (UE) 2016/681.

No obstante el acuerdo con Estados Unidos, la Comisión Europea continuó trabajando en el marco regulatorio de los datos PNR, y, en concreto, en lo relativo a la utilización de esta categoría de datos con fines policiales[29], que no llegó a aprobarse debido a la entrada en vigor del Tratado de Lisboa[30] en 2009, dado que no se ajustaba a los nuevos requisitos exigidos en los Tratados.

Dentro de lo que se dio en llamar el "nuevo" marco europeo de protección de datos, se ha aprobado recientemente, junto al Reglamentoo general de protección de datos[31], y la Directiva de protección de datos en asuntos criminales[32], la *Directiva relativa a la utilización de los datos PNR*[33].

Sus objetivos, como indica, su Considerando (5), son garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes.

Como señaló el propio Consejo europeo, la necesidad del uso de los datos PNR deriva de que *"las actividades terroristas y de delincuencia organizada a menudo conllevan desplazamientos internacionales. En respuesta a la supresión de los controles en las fronteras interiores en virtud del Convenio de Schengen, la UE prevé el intercambio de datos personales entre autoridades policiales. El sistema PNR va encaminado a complementar los instrumentos que ya existen*

27 *Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas, DO L 261. 06.08.2004.*

28 *https://es.wikipedia.org/wiki/Sistema_PNR_europeo*

29 *Propuesta de Decisión marco 2007/0237 (CNS) del Consejo, de 6 de noviembre de 2007, sobre la utilización de datos del registro de nombres de los pasajeros (PassengerName Record-PNR) con fines represivos.*

30 *TRATADO DE LISBOA POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA Y EL TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA (2007/C 306/01). DOUE C 306. 17.12.2007.*

31 *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DO L 119.04.05.2016.*

32 *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DO L 119.04.05.2016.*

33 *Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. DO L 119.04.05.2016.*

para hacer frente a la delincuencia transfronteriza. El tratamiento de datos PNR permitiría a las autoridades policiales descubrir a las personas no sospechosas de realizar actividades delictivas o terroristas antes de que un análisis específico de los datos mostrara que podrían serlo.

Además, la mayoría de los Estados miembros ya utilizan los datos PNR a disposición de la policía u otras autoridades en virtud de la legislación nacional. Un sistema de PNR de la UE permitiría también armonizar las disposiciones legales de los Estados miembros, evitando así la inseguridad jurídica y las deficiencias de seguridad, salvaguardando al mismo tiempo la protección de datos".[34]

La finalidad de la recogida y uso de los datos PNR, viene determinada por la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo[35] y delitos graves (entendiéndose por tales, conforme al apartado 9) del art. 3 de la Directiva, *"los delitos incluidos en el anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al derecho nacional de un Estado miembro")*[36]. El tratamiento de datos personales debe ser proporcional a los objetivos específicos de seguridad que se pretenden alcanzar con la Directiva (Considerando (11).

Pero ¿que son los PNR, y cual su extensión? De nuevo, la Directiva en su art. 3, apartado5) establece que por «*registro de nombres de los pasajeros*» o «*PNR*»: *una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades".*

La lista de los datos PNR, conforme al Considerando 15) debe elaborarse teniendo en cuenta las necesidades de información de las autoridades públicas para el cumplimiento de los fines determinados anteriormente, debiendo contener la información detallada sobre las reservas e itinerarios de viajes que permita a las autoridades competentes identi-

34 *http://www.consilium.europa.eu/es/policies/fight-against-terrorism/passenger-name-record/*

35 *DECISIÓN MARCO DEL CONSEJO, de 13 de junio de 2002, sobre la lucha contra el terrorismo. (2002/475/JAI). DOCE L 164. 22.06.2002. Conforme a su art. 1, deben considerare "delitos de terrorismo los actos intencionados a que se refieren las letras a) a i) tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o su contexto, puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de:*
— intimidar gravemente a una población,
— obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo,
— o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional;
a) atentados contra la vida de una persona que puedan tener resultado de muerte;
b) atentados graves contra la integridad física de una persona;
c) secuestro o toma de rehenes;
d) destrucciones masivas en instalaciones gubernamentales o públicas, sistemas de transporte, infraestructuras, incluidos los sistemas informáticos, plataformas fijas emplazadas en la plataforma continental, lugares públicos o propiedades privadas, que puedan poner en peligro vidas humanas o producir un gran perjuicio económico;
e) apoderamiento ilícito de aeronaves y de buques o de otros medios de transporte colectivo o de mercancías;
f) fabricación, tenencia, adquisición, transporte, suministro o utilización de armas de fuego, explosivos, armas nucleares, biológicas y químicas e investigación y desarrollo de armas biológicas y químicas;
g) liberación de sustancias peligrosas, o provocación de incendios, inundaciones o explosiones cuyo efecto sea poner en peligro vidas humanas;
h) perturbación o interrupción del suministro de agua, electricidad u otro recurso natural fundamental cuyo efecto sea poner en peligro vidas humanas;
i) amenaza de ejercer cualesquiera de las conductas enumeradas en las letras a) a h)".

36 *ANEXO II*
Lista de los delitos a que se refiere el artículo 3, punto 9
1. pertenencia a una organización delictiva
2. trata de seres humanos
3. explotación sexual de niños y pornografía infantil
4. tráfico ilícito de estupefacientes y sustancias psicotrópicas
5. tráfico ilícito de armas, municiones y explosivos
6. corrupción
7. fraude, incluido el que afecte a los intereses financieros de la Unión
8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro
9. delitos informáticos/ciberdelincuencia
10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas
11. ayuda a la entrada y residencia ilegales
12. homicidio voluntario, agresión con lesiones graves
13. tráfico ilícito de órganos y tejidos humanos
14. secuestro, detención ilegal y toma de rehenes
15. robo organizado y a mano armada
16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte
17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías
18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos
19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento
20. tráfico ilícito de materiales radiactivos o sustancias nucleares
21. violación
22. delitos incluidos en la jurisdicción de la Corte Penal Internacional
23. secuestro de aeronaves y buques
24. sabotaje
25. tráfico de vehículos robados
26. espionaje industrial.

ficar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior. El Anexo I, bajo la denominación de *"Datos del registro de nombres de los pasajeros recopilados por las compañías aéreas"* establece como categorías de datos: 1. Localizador de registro PNR 2. Fecha de reserva/emisión del billete 3. Fecha(s) fechas de viaje prevista(s) 4. Nombre(s) y apellido(s) 5. Dirección y datos de contacto (número de teléfono, dirección de correo electrónico) 6. Todos los datos de pago, incluida la dirección de facturación 7. Itinerario completo del viaje para el PNR específico 8. Información sobre viajeros asiduos 9. Agencia de viajes/operador de viajes 10. Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva 11. Información PNR escindida/dividida 12. Observaciones generales (incluida toda la información disponible sobre menores de 18 años no acompañados, como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada) 13. Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos *(Automatic Ticket FareQuote)* 14. Datos del asiento, incluido el número 15. Información sobre códigos compartidos 16. Toda la información relativa al equipaje 17. Número de viajeros y otros nombres de viajeros que figuran en el PNR 18. Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API) (incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada) 19. Todo el historial de cambios de los datos PNR indicados en los números 1 a 18.

Como se observa, un detallado y problemático elenco de datos que podrán ser objeto de tratamiento, estableciendo la obligación de la transferencia de datos PNR de las compañías aéreas a las autoridades nacionales (art. 8), así como el tratamiento que estas efectúen de esos datos. Con arreglo a la nueva Directiva, las compañías aéreas tendrán que facilitar los datos PNR de los vuelos que entren en la UE o salgan de esta. También permitirá, aunque no será obligatorio, que los Estados miembros recopilen los datos PNR correspondientes a determinados vuelos interiores de la UE.

Ahora bien, dichas listas no podrán basarse (Considerando (15), ni consecuentemente tratarse datos, estando expresamente prohibido (art.13. 4), cuando revelen el origen racial o étnico, las opinionespolíticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona.

Cada Estado miembro deberá crear la denominada «Unidad Información sobre los Pasajeros» (UIP), que recibirá los datos PNR de las compañías aéreas, tal y como establece el art. 4. Sus funciones se desglosan en dos: a) recoger los datos PNR, almacenar, procesar y transferir los datos o el resultado de su tratamiento a las autoridades competentes (conforme al art. 7, cada Estado elaborará la lista de autoridades competentes, que lo serán siempre en función de su capacidad para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo); b) intercambiar los datos y/o los resultados de tratamiento con las UIP de otros Estados (art. 9) y con Europol (art. 10). Igualmente, conforme al art. 11, se autoriza la transferencia de datos a terceros países, que solo podrá producirse en circunstancias muy particulares y deberá estudiarse caso por caso.

Importante en esta materia es la obligación, establecida en el art. 5, de que de todas las UIP tendrán que designar un responsable de la protección de datos personales que, junto a la labor de control del tratamiento de datos y efectivación de garantías, constituirá también el punto único de contacto en el que los interesados podrán ejercer sus derechos en todo lo relativo al tratamiento de sus datos PNR.

En el marco de estas actividades, conforme al art. 6, los datos PNR pueden utilizarse de distintos modos:

- para la evaluación previa a la llegada o a la salida de los pasajeros en comparación con criterios de riesgo predeterminados o para identificar a determinadas personas;
- como contribución a la definición de estos criterios de riesgo;
- con vistas a investigaciones o enjuiciamientos determinados.

En lo tocante a la conservación y despersonalización de los datos (art. 12), éstos se conservarán inicialmente durante seis meses, después de lo cual se enmascararán y conservarán durante otros cuatro años y medio, con un estricto procedimiento de acceso a la totalidad de los datos.

El art. 13 contiene las previsiones relativas a la protección de los datos de carácter personal, que pueden agruparse:

- prohíbe la recogida y el uso de datos sensibles
- los Estados miembros deberán asegurarse de que los pasajeros reciban una información precisa, de fácil acceso, y comprensión sobre la recogida de datos PNR y sus derechos.
- el tratamiento automatizado de los datos PNR no podrá ser la única base para tomar decisiones que tengan consecuencias jurídicas adversas o que afecten gravemente a una persona.
- Cuando existan indicios de una posible violación de los datos personales que suponga un elevado riesgo para la protección de estos o afecten negativamente a la intimidad del interesado, se debe comunicar, sin demora injustificada, al interesado y a la autoridad supervisora nacional.

La Directiva establece, igualmente, la obligación de desarrollar protocolos técnicos comunes, que hagan interoperables las transferencias de datos por medios electrónicos, y que ofrezcan, conforme al art. 16, garantías suficientes en relación con las medidas de seguridad técnicas y las medidas organizativas que rigen el tratamiento de datos a llevar a cabo. No obstante, pude producirse algún fallo técnico. En este supuesto, se autoriza la transmisión de datos por otro procedimiento adecuado, siempre que se conserve el mismo nivel de seguridad y se cumpla estrictamente lo relativo a la protección de datos personales.

La Directiva opta por el sistema de transmisión de datos, frente al de extracción, y así las compañías aéreas "transmitirán" los datos PNR a la autoridad solicitante, manteniendo aquellas el control de los datos suministrados, lo que proporciona un mayor nivel de protección de datos. Este sistema será obligatorio para todas las compañías aéreas (Considerando (16).

REFLEXIONES FINALES

El resurgimiento de los nacionalismos exacerbados y violentos, de las teologías de la guerra y la aniquilación, de las tribus y grupos de la caverna ha colocado al planeta al borde de una hecatombe, donde los sufridos ciudadanos, como casi siempre, seremos los primeros en pagar.

Pero la constatación de esta realidad no nos debe llevar, como se está comprobando en la realidad, a un control planetario de nuestras actividades, de nuestra vida. No podemos caer en la inversión del sagrado principio de la presunción de inocencia, por el peligroso y antidemocrático de la "presunción de culpabilidad", donde se nos exige, en el mejor de los casos, que entreguemos nuestra intimidad, para que no se sabe muy bien quien, sin control, decida si somos o no ciudadanos honorables; o tan simplemente, ciudadanos.

Estamos asistiendo a la consolidación de un nuevo paradigma harto peligroso para los derechos de los ciudadanos y las libertades públicas. Este no es otro que el de la "seguridad a toda costa". Frente a los esfuerzos por mantener y agrandar el ámbito de las libertades en las sociedades democráticas, la seguridad es el valor-guía que lo modula y delimita todo.

No es asumible, en estas coordenadas, que el Estado pretenda, amparado en lo indeterminado de la seguridad, protegerse de sus propios ciudadanos, pues, desposeído de la base social y legitimadora que lo sustenta, sus acciones carecen de sentido, deviniendo pura arbitrariedad. La seguridad es fácilmente obtenible en Estados totalitarios que ven a sus ciudadanos como potenciales delincuentes frente a los cuales todo, o casi todo, vale, pues lo relevante y prioritario es mantener la estructura de poder al precio que sea menester.

Hay que luchar contra la violencia y el terrorismo, pero de manera ejemplificante. Con determinación, pero sin intrusiones innecesarias; con normas contundentes, pero que respeten las libertades y derechos de los ciudadanos.

DIC
TÁ
ME
NES

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
2/2016	2015-2-10-0000425

Montevideo, 24 de febrero de 2016

VISTO: La consulta formulada por la Dra. Paola Sayanes en representación del Consejo de Educación Técnico Profesional de la Universidad del Trabajo del Uruguay (UTU), respecto a la comunicación de datos solicitada por la Asociación de Funcionarios (AFUTU).

RESULTANDO:

I) Que AFUTU ha solicitado acceder al listado de los funcionarios que han adherido a los paros realizados durante el año 2015.

CONSIDERANDO:

I) Que la situación encuadra dentro del ámbito de aplicación de la Ley N° 18.331, de 11 de agosto de 2008, y su decreto reglamentario N° 414/009, 31 de agosto de 2009.Que tratándose de datos relativos a experiencia y referencias laborales para el cargo, estamos ante datos personales comunes, cuya recolección aparece justificada y necesaria para el establecimiento de vínculos laborales.

II) Que la ley establece una serie de requisitos para que una comunicación de datos a terceros sea legítima (art. 9° y 17 de la citada Ley) y en este caso no se verifican la conjunción simultánea del interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, salvo las excepciones establecidas en la norma.

III) Que además, en el caso podría considerarse que adherir o no los paros convocados por el gremio, se relaciona con la afiliación sindical del funcionario, que es un dato sensible que sólo puede ser objeto de recolección y tratamiento con el consentimiento expreso y escrito del titular (arts. 4°, 9° y 18 de la citada Ley).

IV) Que en el caso, cada trabajador debería brindar su consentimiento en forma expresa y por escrito, pues en el expediente no se identifica ninguna excepción que habilite o legitime esa comunicación de datos, y de la lectura de los estatutos del sindicato no surge ninguna cláusula, que al ser aceptada por los afiliados, habilite a solicitar esa información a la Institución.

V) Que por otra parte, cabe considerar lo que ya ha expresado la URCDP en el Dictamen N° 16/010 de 20 de agosto de 2010, en relación a una consulta sobre datos sensibles y referencias personales de las empresas de seguridad: la recolección y tratamiento de datos sensibles en el marco de una relación contractual, no abaten la necesidad de obtener el consentimiento expreso y escrito del titular, ni supone dejar de cumplir con los restantes principios y preceptos de la Ley.

ATENTO: A lo expuesto y a lo previsto en las normas aplicables,

LA UNIDAD REGULADORA
Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que de acuerdo con lo previsto por la Ley Nº 18.331, no existe excepción que habilite a la Universidad del Trabajo del Uruguay, a comunicar a la Asociación de Funcionarios el listado de funcionarios que adhirieron a los paros realizados durante el año 2015.

2.- Que para que dicha comunicación sea legítima deberá estarse a lo establecido en el artículo 17 de la Ley, que exige la conjunción simultánea del interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, de lo contrario deberán ser comunicados en forma disociada del titular.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
3/2016	2015-2-10-001235

Montevideo, 2 de marzo de 2016

VISTO: La consulta presentada por la SECRETARIA DE LOS DERECHOS HUMANOS PARA EL PASADO RECIENTE de PRESIDENCIA DE LA REPÚBLICA acerca de la determinación de un criterio para la publicación en la página web de la Institución, de información vinculada al gobierno de facto.

RESULTANDO:

I) Que a modo de ejemplo se adjuntan fichas con información de detenidos desaparecidos y fallecidos.

II) Que las fichas citadas contienen información personal, y se encuentran publicadas en la página web de la Institución, además de encontrarse incluidas en el documento elaborado en el marco del artículo 4° de la Ley N° 15.848 y la Resolución de Presidencia de la República N° 832/006 de 26 de diciembre de 2006.

CONSIDERANDO:

I) Que el artículo 17° de la Ley N° 18.331, de 11 de agosto de 2008 establece que la comunicación de datos personales requiere el cumplimiento de los fines del emisor y destinatario, así como el consentimiento del titular de los datos, salvo excepciones.

II) Que el artículo 9º de la citada ley establece las excepciones al principio del consentimiento, por lo que este no es necesario cuando los datos provengan de fuentes públicas de información, se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, entre otros (literales A y B del artículo citado, respectivamente).

III) Que en este caso, efectivamente existe una comunicación de datos personales, siendo aplicables las normas en materia de protección de datos personales precitadas.

IV) Que sin perjuicio de ello, deben armonizarse estas normas, con las relativas al Acceso a la Información Pública (Ley N° 18.381, en particular su artículo 12°), y otras normas, nacionales y supranacionales, referentes a la investigación y tratamiento de la información de violaciones a derechos humanos durante los gobiernos de facto, o "derecho a la verdad" (Resoluciones N° 47/133 y 55/89 de la Asamblea General de las Naciones Unidas, Ley N° 18.596, entre otros).

V) Que deben ponderarse los derechos en juego, lo que amerita un análisis pormenorizado de las situaciones planteadas a través de criterios objetivos, para lo cual deberá recabarse la opinión de todos los organismos vinculados a la materia.

VI) Que en mérito a lo referido no resulta pertinente indicar criterios que consideren en forma aislada el derecho a la protección de datos personales.

ATENTO: A lo expuesto, y a lo previsto en las normas citadas.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- La publicación de informes vinculados a los gobiernos de facto que contengan información de carácter personal, es una comunicación de datos en los términos del artículo 17 de la Ley N° 18.331.

2.- A los efectos de realizar una adecuada ponderación de los derechos vinculados a la protección de datos personales, acceso a la información pública, y derecho a la verdad procede la elaboración de criterios objetivos para su aplicación a los casos concretos, con la participación de todos los organismos involucrados.

3.- Remítase el presente expediente a la Unidad de Acceso a la Información Pública a los efectos de recabar su opinión, ofreciéndose la colaboración de este Consejo para la elaboración de los criterios objetivos precitados.

4.- Notifíquese, publíquese y oportunamente archívese.

Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
4/2016	2016-2-10-0000105

Montevideo, 2 de marzo de 2016

VISTO: La consulta realizada por la División Epidemiología del Ministerio de Salud Pública (MSP) con referencia a la implementación de un software de registro único de usuarios que padecen VIH, el cual vincula la información clínica, epidemiológica y de laboratorio, con la finalidad de dar tratamiento a la enfermedad y aumentar su vigilancia.

RESULTANDO:

I) Que las características de la epidemia de infección por VIH/SIDA se han modificado con el transcurso del tiempo, pasando a ser un evento transmisible, pero de comportamiento crónico.

II) Que la generalización del tratamiento antirretroviral, el inicio del tratamiento en la etapa no sida de la infección, el mayor acceso a programas de prevención de la transmisión materno infantil y a servicios de consejería y pruebas voluntarias, han permitido incrementar el número de personas que realizan la prueba del VIH, y obtener diagnósticos más tempranos en la historia natural de la infección, por lo que la vigilancia de la enfermedad se ha transformado en un gran desafío para los países.

III) Que el software relacionado en el Visto permite el acceso a la información de los pacientes al MSP, a los laboratorios de análisis clínicos, y a los médicos tratantes.

CONSIDERANDO:

I) Que el artículo 44 de la Constitución de la República dispone que el Estado legislará en todas las cuestiones relacionadas con la salud e higiene públicas, procurando el perfeccionamiento físico, moral y social de todos los habitantes del país, disponiendo también, que todos los habitantes tienen el deber de cuidar su salud, así como el de asistirse en caso de enfermedad.

II) Que el art. 22 de la Ley Nº 18.335, de 15 de agosto de 2008 dispone que las personas tienen la obligación de someterse a las medidas preventivas o terapéuticas que se le impongan, cuando su estado de salud, a juicio del MSP, pueda constituir un peligro público (también el artículo 224 del Código Penal).

III) Que el art. 1 de la Ley Orgánica de Salud Publica, Ley Nº 9202, de 12 de enero de 1934, dispone que compete al Poder Ejecutivo por intermedio del MSP, la organización y dirección de los servicios de Asistencia e Higiene.

IV) Que el art. 2 de la Ley Nº 18.211 de 13 de diciembre de 2007 que regula la creación, funcionamiento y financiación del Sistema Nacional Integrado de Salud (SNIS) establece como competencia del MSP la implementación de dicho sistema y la articulación de los prestadores públicos y privados.

V) Que el art. 4 Lit. B de la referida Ley, consagra como objetivos del SNIS la implementación de un modelo de atención integral basado en una estrategia sanitaria común, políticas de salud articuladas, programas integrales y acciones de promoción, protección, diagnostico precoz, tratamiento oportuno, recuperación y rehabilitación de la salud de sus usuarios, incluyendo los cuidados paliativos.

VI) Que el art. 4 Lit. E), de la Ley Nº 18.331, de 11 de agosto de 2008, define a los datos sensibles como aquellos datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

VII) Que el art. 18 de esta Ley prevé que ninguna persona puede ser obligada a proporcionar datos sensibles, los cuales solo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Asimismo, establece que los mismos, pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo.

VIII) Que el artículo 17 de dicha Ley Nº 18.331 regula la comunicación de datos personales exigiendo que la misma debe contar con el interés legítimo del emisor y del destinatario de los datos, sin perjuicio del previo consentimiento del titular de estos.

IX) Que el Lit. C) de ese artículo 17 prevé que no será necesario el consentimiento del titular cuando se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente.

X) Que por su parte, el art. 19 de la Ley N° 18.331 indica que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la propia Ley Nº 18.331.

XI) Que la Ley Nº 19.286, de 25 de setiembre de 2014 (Código de Ética Médica), dispone en su artículo 22 que el respeto a la confidencialidad es un deber inherente a la profesión médica el cual podrá ser relevado en los casos establecidos por una ley de interés general o cuando exista justa causa de revelación.

ATENTO: A lo expuesto, y a lo previsto en la Ley N° 18.331, su decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que el proyecto objeto de esta consulta prevé el tratamiento de datos de salud, los cuales son datos sensibles en virtud de lo dispuesto por el art. 4 de la Ley 18.331, por lo cual se exhorta al MSP a adoptar todas las medidas de seguridad adecuadas para garantizar la seguridad de la información personal de los usuarios en el sistema.

2.- Que se entiende que la decisión del MSP de solicitar que la información cargada en el sistema sea comunicada sin disociarla de su titular resulta acorde a derecho, ya que la pertinencia exigida por el art. 17 Lit. C de la Ley Nº 18.331, debe ponderarse a la luz de las normas jurídicas que regulan el punto objeto del proyecto y así como el interés general a las que ellas responden, como son los arts. 44 de la Constitución, 22 de la Ley Nº 18.335, y Decreto Nº 409/993, en la redacción dada por el Decreto Nº 255/008, así como las disposiciones internacionales aplicables.

3.- Que la titularidad del sistema y de la base de datos generada por parte del MSP también se entiende acorde a derecho, en función de su calidad de órgano integrante del sistema orgánico Poder Ejecutivo, en ejercicio de los cometidos referentes a la sanidad nacional en cumplimiento de lo dispuesto en el art. 1 de la Ley Orgánica de la Salud Nº 9202.

4.- Que el acceso a la información alojada en el sistema sin restricciones por parte del MSP se entiende legitima, con motivo de ajustarse a lo dispuesto por el inc. 2 del art. 18 de la Ley Nº 18.331, en virtud de mediar razones de interés general por aplicación de lo dispuesto en los arts. 1, 2, 4 Lit. B) ,11 y 49 de la Ley Nº 18.211 que regula el SNIS.

5.- Que la comunicación de datos realizada por los laboratorios de análisis clínicos con la carga de la información del paciente en el sistema también es legítima por encontrarse precedida de interés legítimo del laboratorio como emisor de los mismos, en virtud de la necesidad de dar cumplimiento a la normativa vigente, como son los arts. 4 Lit. B) y 11 de la Ley Nº 18.211; y por el MSP como destinatario de los mismos, en función de lo dispuesto en el art. 4 de la Ley Orgánica de la Salud Nº 9202 y el art. 2 de la Ley Nº 18.211, y no será necesario el consentimiento previo del titular, por aplicación del art. 17 Lit. C).

6.- Que la solicitud de acceso a la información del paciente que solicitan los laboratorios de análisis clínicos, se entiende acorde a lo previsto por el art. 19 de la Ley Nº 18.331, con motivo de que aquel ya ha sido usuario de la entidad, por lo que éstas ya poseen tal información, accediendo en este caso por otra vía. Igualmente corresponde exhortar al MSP extremar las medidas de seguridad y los accesos para que los laboratorios de análisis clínicos no accedan a información que exceda el marco de su actuación.

7.- Que la comunicación de datos realizada por parte de los médicos tratantes del paciente con destino al MSP, también es legítima ya que se encuentra revestida de interés legítimo para ambos: para los médicos, por aplicación de la Ley Nº 19.286 (Código de Ética Médica), y para el MSP por mandato del art. 44 de la Constitución, art. 1° de la ley Orgánica de la Salud Nº 9202 y art. 2° de la Ley Nº 18.211 y tampoco será necesario el consentimiento del titular por aplicación de la excepción prevista en el art. 17 Lit. C).

8.- Que la comunicación de la información médica del paciente por parte del médico tratante con destino al MSP y a otros médicos tratantes que pudieren acceder al sistema en otras instancias del tratamiento, también se realiza acorde a derecho ya que reviste el interés general exigido y no requiere consentimiento previo del titular por aplicación del art. 17 Lit. C) de la Ley Nº 18.331, sin perjuicio de la aplicación del art. 22 de la Ley Nº 19.286 (Código de Ética Médica).

9.- Notifíquese, publíquese y oportunamente archívese.

Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
8/2016	2016-2-10-0000074

Montevideo, 6 de abril de 2016

VISTO: La consulta realizada por la Unidad Nacional de Seguridad Vial (UNASEV) de Presidencia de la República respecto al artículo 126 del Proyecto de Ley de "Contrato de Seguros".

RESULTANDO:

I) Que el artículo mencionado prevé la posibilidad de crear bases de datos comunes entre empresas aseguradoras con fines de: a) liquidación de siniestros, colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora; b) prevenir el fraude de seguros.

II) Que el mismo artículo prevé además una sustitución del consentimiento previo por una comunicación previa a la conformación de las bases mencionadas.

CONSIDERANDO:

I) Que el art. 1° de la Ley Nº 18.331, de 11 de agosto de 2008, establece que el derecho a la protección de datos es inherente a la persona humana, y está comprendido en el artículo 72 de la Constitución. El art. 3° de la Ley por su parte, establece que el régimen será de aplicación a datos personales registrados en cualquier soporte susceptible de tratamiento con excepción de las bases creadas y reguladas por leyes especiales, entre otras.

II) Que a efectos de considerar las bases excluidas del ámbito de la Ley, debe darse el cumplimiento acumulativo de tres requisitos: a) que se encuentren creadas por Ley; b) que se encuentren reguladas por Ley; c) que su creación y regulación resulte de leyes especiales.

III) Que en este caso no se dan los requisitos acumulativos referidos en el Considerando anterior, atento a que no se están creando efectivamente bases, sino habilitando su creación, y porque no existe una regulación completa de esas bases en la norma.

IV) Que por otra parte, atento a que se prevé la conformación de bases comunes para varias entidades, se estima deseable a efectos de asegurar el cumplimiento de los principios y normas previstos en la Ley N° 18.331, que las entidades responsables de la o las bases inscriban Códigos de Conducta, en los términos del artículo 32 de la Ley.

ATENTO: A lo expuesto, y a lo previsto en la Ley N° 18.331, su decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que el artículo 126 del Proyecto de Ley referente a "Contrato de Seguros" no consagra una excepción al registro de Bases de Datos, conforme lo establecido por la Ley N° 18.331, por lo que las bases que se creen a su amparo deberán inscribirse ante esta Unidad.

2.- Que se estima deseable que las empresas que creen las Bases referidas inscriban en forma conjunta Códigos de Conducta, a efectos de garantizar el cumplimiento de las normas y principios de la Ley N° 18.331.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
13/2016	2016-25-3-0000463

Montevideo, 3 de agosto de 2016

VISTO: La remisión de estas actuaciones por parte del Consejo Ejecutivo de la Unidad de Acceso a la Información Pública a efectos de solicitar un pronunciamiento de esta Unidad.

RESULTANDO:

I) Que los presentes obrados refieren a la solicitud de acceso a la información pública recibida por parte de la Administración Nacional de Educación Pública (ANEP) del Señor Tower Urcwiz, vinculada a la entrega de información referente a colegios explicitada en la solicitud correspondiente.

II) Que en concreto se solicita a esta Unidad pronunciamiento respecto a la naturaleza de la información solicitada por el peticionante a efectos de determinar su encuadre en lo dispuesto por el artículo 10 numeral II, de la Ley N° 18.381, de 17 de octubre de 2008, y por ende si la misma reviste el carácter de confidencial por tratarse de datos personales sujetos a previo consentimiento informado.

CONSIDERANDO:

I) Que la libertad de enseñanza se encuentra expresamente consagrada en el artículo 68 de la Constitución de la República.

II) Que ANEP, ente autónomo que rige el servicio de enseñanza preuniversitaria y la supervisión de las entidades de enseñanza privadas, posee determinados cometidos establecidos en la Ley N° 18.437, de 12 de diciembre de 2008, requiriendo para su cumplimiento, la obtención y tratamiento de la información de las referidas entidades.

III) Que esa información es personal, atento a lo dispuesto por el artículo 2° de la Ley N° 18.331, de 11 de agosto de 2008, siendo en consecuencia aplicables los principios de protección de datos personales.

IV) Que no obstante ello, las entidades privadas de enseñanza habilitadas se encuentran reguladas por la Ordenanza N° 14, que determina una serie de condiciones a cumplir en forma previa a su constitución, y mientras revistan tal calidad. En este sentido, se establecen vínculos y contralores específicos por parte de las autoridades de enseñanza pública que garanticen el mantenimiento de aquellas condiciones.

V) Que en función de lo antedicho, ANEP posee el carácter de responsable de la base de datos o de tratamiento, de la información comunicada por las entidades privadas de enseñanza, en la definición dada por el artículo 4 literal K de la Ley N° 18.331.

VI) Que la comunicación de información referente a cada entidad privada de enseñanza coloca a ANEP en la situación de emisor de datos, y al peticionante en el rol de su destinatario, siendo aplicable lo dispuesto por el artículo 17 de la Ley N° 18.331. Dicho artículo requiere la concurrencia de un interés legítimo y del consentimiento previo del titular, o en su caso la aplicación de una excepción a dicho consentimiento.

VII) Que en el presente caso la exigencia del interés legítimo se entiende cumplido por cuanto ANEP es un sujeto obligado a realizar la entrega de la información en cumplimiento de la Ley N° 18.381, y el solicitante posee el derecho a acceder a la misma por lo dispuesto en dicho cuerpo normativo.

VIII) Que en lo que respecta al consentimiento, resulta aplicable al caso concreto la excepción establecida en el literal A del artículo 17 de la Ley N° 18.331 por tratarse la Ley N° 18.381 de una Ley de interés general, lo que se desprende de lo establecido en los artículos 1 y 5 de esta última.

IX) Que no resulta aplicable al caso concreto el principio de reserva establecido en el artículo 11 de la Ley N° 18.331, por ser ANEP un sujeto obligado por la Ley N° 18.381, y por la circunstancia de que el derecho a la información debe primar en el caso frente al deber de reserva de un dato personal de una persona jurídica pública.

ATENTO: A lo expuesto, y a lo previsto en las normas anteriormente citadas.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que la Administración Nacional de Educación Pública debe recabar la información de las respectivas instituciones privadas de enseñanza y dar tratamiento a la misma a efectos de supervisar y fiscalizar su actividad, velando por el cumplimiento de los principios establecidos en la Ley General de Educación N° 18.437.

2.- Que la comunicación de la información de una entidad privada de enseñanza a la Administración Nacional de Educación Pública se encuentra amparada en la Ordenanza N° 14 aprobada por Acta N° 86, Resolución N° 20 de 19 de diciembre de 1994, en el caso de instituciones habilitadas, y en la Ley General de Educación, siendo esta última de interés general.

3.- Que la Administración Nacional de Educación Pública es el responsable de la base de datos o tratamiento de la mencionada información en el sentido dispuesto por el artículo 4° literal K de la Ley N° 18.331 y que la situación planteada ingresa en la hipótesis de comunicación de datos definida por los artículos 4° literal B y 17 de esa Ley.

4.- Que la Administración Nacional de Educación Pública es sujeto obligado a la entrega de la información solicitada en el caso concreto, y el solicitante posee el derecho de acceder a la misma conforme lo dispuesto por el artículo 3° de la Ley N° 18.381, configurándose el interés legítimo previsto en la norma.

5.- Que la comunicación de datos mencionada se encuentra exceptuada del previo consentimiento de los titulares por aplicación de lo dispuesto en el literal A artículo 17 de la Ley N° 18.331 y los artículos 1° y 5° de la Ley N° 18.381.

6.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
14/2016	2016-2-10-0000373

Montevideo, 8 de setiembre de 2016

VISTO: La consulta realizada por Ing. Jorge Forcella, Director del programa Salud.uy, con referencia a la aplicación de la Ley Nº 18.331, respecto al acceso a la información clínica del paciente que luce en su Historia Clínica, en el marco de la asistencia médica brindada por un profesional médico perteneciente a un prestador de salud subcontratado, en el marco de la implementación de la Historia Clínica Electrónica (HCE).

RESULTANDO:

I) Que en la asistencia médica, el factor habilitante de acceso a la Historia Clínica (HC) es el requerimiento de asistencia por parte del paciente o la circunstancia de su condición de salud, lo cual produce el permiso de acceso a la HC para el profesional actuante, mientras dure el episodio de atención.

II) Que la Historia Clínica Electrónica Nacional (HCEN), no cambia los principios expresados, ya que la responsabilidad por la custodia sigue siendo de la institución que presta o prestó los servicios, la cual está impedida de habilitar el acceso a los datos de un paciente fuera del episodio de asistencia.

III) Que el hecho eventual de que el paciente sea asistido en otra institución o prestador, o en un servicio médico subcontratado por el prestador principal, no implica que se compartan los archivos que contienen las HCE, sino que se habilita el acceso electrónico puntual a ella por parte del profesional actuante, cerrándose su acceso finalizada la asistencia del paciente.

CONSIDERANDO:

I) Que el art. 4° Lit. E) de la Ley N° 18.331 define a los datos sensibles como datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

II) Que el artículo 18 de dicha Ley señala que ninguna persona puede ser obligada a proporcionar datos sensibles. Estos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Asimismo dispone que los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares.

III) Que el art. 19 de la referida ley al regular los datos relativos a la salud prevé que los establecimientos sanitarios y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes, respetando los principios del secreto profesional, la normativa específica y lo establecido en esa ley.

IV) Que el art. 18 de la Ley Nº 18.335 dispone que la historia clínica es de propiedad del paciente, será reservada y sólo podrán acceder a ella los responsables de la atención médica y el personal administrativo vinculado y el Ministerio de Salud Pública cuando lo considere pertinente. Asimismo establece que es responsabilidad de los servicios de salud dotar de seguridad a las historias clínicas electrónicas y determinar las formas y procedimientos de administración y custodia de las claves de acceso y demás técnicas que se usen.

V) Que el art. 4° Lit. K) de la Ley Nº 18.331 identifica como responsables de la base de datos o tratamiento a aquella persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento. Por su parte el art. 4 Lit. B) define la comunicación de datos personales como toda revelación de datos realizada a una persona distinta del titular de los datos.

VI) Que la referida comunicación de datos, es regulada por el art. 17 de la propia Ley Nº 18.331, el cual exige que la misma deba ser precedida de interés legítimo del emisor y del destinatario de los datos, sin perjuicio del previo consentimiento del titular de los mismos, salvo aplicación de las excepciones al consentimiento, previstas en los literales A) a D) del propio artículo.

VII) Que con referencia al consentimiento previo del titular el art. 17 Lit. B) de la Ley Nº 18.331 remite a las excepciones al mismo previstas en el art. 9°, el cual en su Lit. D) prevé que el mismo no será necesario cuando el tratamiento de datos, derive de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

ATENTO: A lo expuesto, y a lo previsto en la Ley N° 18.331, su decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que la consulta formulada refiere a datos de salud, los cuales revisten el carácter de dato sensible por aplicación de lo dispuesto en el art. 4° Lit. E), 18 y 19 de la Ley Nº 18.331 de Protección de Datos y Habeas Data.

2.- Que por aplicación de lo dispuesto en el art. 18 de la Ley Nº 18.335 la Historia Clínica es de propiedad del paciente y se encuentra bajo custodia del prestador de salud, el cual a la luz de las disposiciones de la Ley Nº 18.331 califica como responsable de la base de datos o tratamiento, por aplicación de su art. 4° Lit. K.

3.- Que el acceso a la información clínica del paciente por parte del profesional actuante en el marco de la atención médica, así como el acceso por parte de otro prestador de salud subcontratado a los efectos específicos de dicha atención, configura una hipótesis de comunicación de datos personales en función de lo dispuesto por el art. 4° Lit. B) y art. 17 de la Ley Nº 18.331.

4.- Que no se requiere el consentimiento previo del titular por aplicación de la excepción prevista por el art. 9° Lit. D) de la Ley Nº 18.331 en virtud de la remisión dada por el art. 17 Lit. B), con motivo de que la comunicación de datos es necesaria para el desarrollo y cumplimiento de un contrato como el que vincula al prestador con el subcontratante que prestará asistencia.

5.- Que en definitiva el modelo de comunicación de datos descripto en el Visto, se ajusta a lo dispuesto por la Ley Nº 18.331 de Protección de Datos y Habeas Data.

6.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
15/2016	2016-2-10-0000065

Montevideo, 8 de setiembre de 2016

VISTO: la consulta realizada por FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN (FCEA) de la UDELAR con referencia a la solicitud de información al FONDO DE SOLIDARIDAD.

RESULTANDO:

I) Que FCEA, se encuentra creando una Unidad de Evaluación Institucional, la cual dentro de sus objetivos, se plantea el seguimiento, evaluación y comprensión de los factores asociados al abandono o rezago estudiantil insumo para trazar políticas que atiendan dicha situación.

II) Que la UDELAR ha diseñado instrumentos tendientes a mejorar los resultados estudiantiles tales como la descentralización, tutorías entre pares, becas monetarias y alimentarias entre otras.

III) Que por otra parte, el FONDO DE SOLIDARIDAD es otro de los instrumentos previstos por la normativa para fomentar el estudio a nivel terciario.

IV) Que a los efectos, de identificar el impacto de dicho instrumento en los distintos perfiles estudiantiles, resulta relevante para FCEA contar con información de sus beneficiarios.

V) Que en dicho marco, la FCEA realizó una solicitud de información al FONDO DE SOLIDARIDAD para contar con datos sobre sus estudiantes referentes a zona geográfica de procedencia, sexo, nivel educativo del hogar de procedencia, entre otros.

VI) Que la información comunicada complementará la base de datos de FCEA y posteriormente la misma será despersonalizada para ser utilizada con fines estadísticos a los efectos de asociar el desempeño agregado a ciertas características, excluyéndose su uso con la finalidad de un seguimiento individual.

CONSIDERANDO:

I) Que el art. 4° Lit. B) de la Ley N° 18.331 de fecha 11 de agosto de 2008 define a la comunicación de datos como toda revelación de datos realizada a una persona distinta del titular de los datos.

II) Que dicha comunicación es regida por el art. 17 de la propia Ley, exigiendo que la misma debe estar precedida de interés legítimo del emisor y del destinatario de los datos, además de contar con el previo consentimiento informado del titular, sin perjuicio de las excepciones al mismo previstas en los literales A) a D) del propio artículo, así como las previstas en el art. 9°.

III) Que el interés legitimo exigido es reunido por el FONDO DE SOLIDARIDAD tanto emisor de los datos y por FCEA al amparo de lo previsto en la Ley Nº 16.524 de fecha 25 de julio de 1994 en la redacción dada por el art. 752 de la Ley Nº 19.355 de 19 de diciembre de 2015 y la Ley Orgánica de la UDELAR Ley Nº 12.549 de fecha 16 de octubre de 1958.

IV) Que el art. 17 Lit. A) de la Ley Nº 18.331 dispone que el previo consentimiento del titular de los datos no será necesario cuando así lo disponga una Ley de interés general. Por su parte, el Lit. B) del propio articulo remite a los supuestos de excepción previstos en el art. 9°, siendo uno de ellos, el dispuesto en el Lit. D) el cual prevé que no será necesario, cuando los datos deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

ATENTO: A lo expuesto, y a lo previsto en la Ley N° 18.331, su decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que la solicitud de información que realiza FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN perteneciente a UNIVERSIDAD DE LA REPÚBLICA al FONDO DE SOLIDARIDAD, configura una hipótesis de comunicación de datos regulada por el art. 17 de la Ley Nº 18.331.

2.- Que el FONDO DE SOLIDARIDAD en tanto emisor de los datos y FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN en tanto destinataria de los mismos, se encuentran revestidos del interés legítimo exigido en el referido art. 17 de la Ley Nº 18.331.

3.- Que la comunicación de la información referente a los estudiantes de FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN que solicitaron y obtuvieron ayuda económica por parte del FONDO DE SOLIDARIDAD no requerirá consentimiento previo de sus titulares por aplicación de las excepciones al mismo previstas en el Lit. A) del art. 17 de la Ley Nº 18.331 y el Lit. D) del art. 9° de la propia Ley.

4.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
17/2016	2016-2-10-0000360

Montevideo, 14 de setiembre de 2016

VISTO: La consulta vinculada a la aplicación del llamado "derecho al olvido" a la situación que se plantea en obrados.

RESULTANDO:

I) Que se procura obtener opinión de esta Unidad con respecto a la aplicabilidad de la "teoría del derecho al olvido" en relación a publicaciones que a entender de la consultante serían obsoletas.

II) Que la consultante plantea una situación de hecho particular -referida en múltiples publicaciones de internet que adjunta-, que motivó un pronunciamiento judicial archivando la causa por falta de pruebas, e indica que en aplicación del principio de finalidad consagrado en el artículo 8° de la Ley Nº 18.331, de 11 de agosto de 2008, la información en ellas contenida resulta obsoleta y debería de ser eliminada.

III) Que la consultante se funda además en la aplicación del artículo 15 de la Ley Nº 18.331 -que consagra entre otros, el derecho de supresión-, en el entendido de que la información relacionada en las publicaciones de internet habría dejado de ser pertinente.

IV) Que en definitiva, se consulta la opinión respecto de la aplicabilidad de la Ley Nº 18.331 para solicitar la remoción de las referencias personales contenidas en las publicaciones de internet que perjudican el nombre y la reputación de la involucrada en ellas, que son obsoletas y no necesarias para con la finalidad de su recolección, o no pertinentes y excesivas con relación a los fines de su tratamiento.

CONSIDERANDO:

I) Que la publicación de datos personales en internet constituye una hipótesis de comunicación de datos regulada en el artículo 17 de la Ley Nº 18.331.

II) Que el llamado al derecho al olvido puede considerarse como la proyección de otros derechos, entre otros, del de supresión consagrado en el artículo 15 de la Ley Nº 18.331, y en el artículo 13 del decreto Nº 414/009.

III) Que esta Unidad ya se ha pronunciado en otras oportunidades con respecto a la publicación de informaciones vinculadas a personas en internet, tales como en los Dictámenes Nº 12/012 de 7 de junio de 2012, 2/014 de 13 de febrero de 2014 y en las Resoluciones Nº 1040/012 de 20 de diciembre de 2012 y 6/016 de 9 de marzo de 2012, entre otras.

IV) Que en ese sentido, ante la existencia de errores, falsedades o exclusiones en alguna de las informaciones vinculadas a la persona relacionada en las publicaciones, el titular del dato podrá ejercer su derecho de supresión, en principio ante el editor de las páginas web, quien deberá dar una respuesta en el plazo de 5 días hábiles, conforme prevé la norma precitada. En caso de no obtener respuesta, el titular del dato podrá accionar de habeas data ante el Poder Judicial.

V) Que en el caso planteado en la consulta existen otros derechos además de la protección de datos personales -tales como la libertad de expresión y la libertad de prensa- que ameritan una adecuada ponderación, lo que corresponderá se realice por el Juez competente ante una eventual acción judicial como la planteada en el artículo 15 de la Ley Nº 18.331.

ATENTO: A lo expuesto e informado, y a lo previsto en los artículos 15º y 34º de la Ley Nº 18.331, y 13º del Decreto Nº 414/009,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que en la situación planteada por la consultante el titular de los datos incluidos en publicaciones en internet, podrá ejercer el derecho de supresión establecido en el artículo 15 de la Ley Nº 18.331 ante el editor de las páginas web en su calidad de responsable de tratamiento.

2.- Que en caso de incumplimiento por parte del responsable, sin perjuicio de las acciones administrativas ante esta Unidad, el titular de los datos podrá iniciar la acción prevista en el inciso tercero del artículo referido en el resuelve anterior.

3.- Notifíquese y publíquese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
20/2016	2016-25-1-0004762

Montevideo, 23 de noviembre de 2016

VISTO: La consulta realizada por la Dirección Sectorial de Gestión Humana del Consejo Directivo Central de la Administración Nacional de Educación Pública (en adelante ANEP).

RESULTANDO:

I) Que la consultante solicita de esta Unidad un pronunciamiento con referencia a la pertinencia de la comunicación de datos relativos a la salud y certificación de los funcionarios de ANEP entre la base del BANCO DE PREVISIÓN SOCIAL (en adelante BPS) y la propia ANEP.

II) Que la consultante señala que obtendría acceso a la siguiente información contenida en el Sistema Único de Certificaciones de Trabajadores de BPS: CI con dígito verificador, fecha de inicio y de fin de la certificación, diagnóstico, identificación del médico certificador, fecha de certificación, internación y si puede salir del domicilio. Funda su petición en las potestades de contralor del organismo y en los Estatutos Docente y No Docente.

CONSIDERANDO:

I) Que la situación mencionada por la consultante constituye una hipótesis de comunicación de datos regulada en el artículo 17 de la Ley Nº 18.331, por lo que para que proceda deberán de configurarse interés legítimo del receptor y del destinatario y el previo consentimiento del titular de los datos, salvo las excepciones previstas en esa disposición.

II) Que sin perjuicio de lo mencionado, en este caso resulta aplicable el artículo 18 de la citada Ley, por tratarse de datos sensibles, que requieren expresamente mandato legal o razones de interés general para su tratamiento.

III) Que esta Unidad ya se ha pronunciado con respecto al Sistema de certificaciones médicas por Resolución 7/2012 de 10 de mayo de 2012 expresando que la comunicación de datos sensibles -en particular el dato diagnóstico- requiere el consentimiento expreso y escrito del titular.

IV) Que en la situación de marras no se observa un mandato legal ni un interés general en el conocimiento de la información sensible de sus funcionarios, que justifiquen una excepción al previo consentimiento expreso y escrito previsto en las normas para el tratamiento y la comunicación de este tipo de datos.

ATENTO: A lo expuesto e informado, y a lo previsto en los artículos 15 y 34 de la Ley Nº 18.331, y 13 del Decreto Nº 414/009,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que la comunicación del dato diagnóstico requiere del consentimiento expreso y escrito de los titulares por no existir excepciones.

2.- Que con respecto a los restantes datos proveídos por el Sistema Nacional de Certificación Laboral corresponde estar a lo dictaminado por este Consejo en el Dictamen Nº 7/2012 de 10 de mayo de 2012.

3.- Notifíquese y publíquese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
21/2016	2016-2-10-0000521

Montevideo, 29 de diciembre de 2016

VISTO: La consulta formulada por la DIRECCIÓN NACIONAL DE IMPRESIONES Y PUBLICACIONES OFICIALES (en adelante IMPO) respecto de la existencia de un potencial conflicto entre la publicación del Diario Oficial en Internet y el derecho a la protección de datos personales.

RESULTANDO:

I) Que en mérito a lo dispuesto en el artículo 760 de la Ley Nº 19.355, de 19 de diciembre de 2015, el IMPO sustituyó el formato papel por el electrónico e hizo además disponibles las búsquedas por Internet a través de motores de búsqueda, facilitando de esta forma el cumplimiento de los propios fines del organismo, que es dar a conocer a terceros determinados actos jurídicos.

II) Que la publicación electrónica habilitó el acceso a información histórica del Diario, "reviviendo" situaciones que en su momento tuvieron la trascendencia suficiente para ser conocidas por la población, pero cuya vigencia al día de hoy en algunos casos puede resultar discutible.

CONSIDERANDO:

I) Que entre los cometidos del IMPO específicamente se encuentra editar y publicar el Diario Oficial y el Registro Nacional de Leyes y Decretos, en formato papel y electrónico.

II) Que el artículo 9º de la Ley Nº 18.331, de 11 de agosto de 2008 establece que el tratamiento de los datos personales debe efectuarse con el consentimiento del titular del dato o al amparo de algunas de las excepciones a ese consentimiento establecidas en la Ley. Entre estas excepciones se encuentran los casos de datos que provengan de fuentes públicas de información (literal A). El artículo 9° Bis, agregado por Ley Nº 18.996 de 7 de noviembre de 2012, art. 43, por su parte precisa el concepto citado, estableciendo que se entienden como fuentes públicas de información, entre otros, el Diario Oficial y las publicaciones oficiales, cualquiera sea su soporte de registro o canal de comunicación (Literal A).

III) Que de las normas relevadas, y especialmente los artículos 341 de la Ley Nº 16.736, 4º, 9º y 9º Bis de la Ley Nº 18.331, y 760 de la Ley Nº 19.355, surge que las publicaciones en el Diario Oficial cumplen con un fin de interés general y se encuentran además exceptuadas en principio del previo consentimiento informado de los titulares del dato. Esa publicación además debe realizarse in totum, tal y como fue referida al Diario Oficial por parte del organismo obligado a remitir la publicación para su realización.

IV) Que este Consejo en Resolución 6/016 de 9/3/2016, expresó: "Que esta Unidad ya se ha pronunciado (...), señalando especialmente que en las situaciones de simultánea aplicación de los derechos a la protección de los datos personales y el derecho de información, comprensivo del derecho de acceso a la información pública, la competencia resolutiva es de la autoridad responsable de la difusión de que se trate, la que deberá interpretar de manera armónica ambos derechos y, en su caso, procurar el menor sacrificio posible de aquéllos" ("Considerando" I).

V) Que, por otra parte, por Resolución Nº 1.040/012 de 20/12/2012, publicada en el Diario Oficial de 27/2/2014, recomendó "a los responsables de publicar contenidos en los sitios web de los organismos públicos, la adopción de algunos criterios técnicos señalados en la parte expositiva" de ese acto, los "que se desarrollan en el informe del CERT-uy" que se incorporó a dicha resolución.

ATENTO: A lo expuesto e informado, y a lo previsto en el artículo 34 de la Ley N° 18.331, de 11 de agosto de 2008.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- La publicación de informaciones oficiales en el Diario Oficial se encuentra habilitada legalmente en soporte electrónico.

2.- A efectos de minimizar las posibles vulneraciones a las personas en la protección de sus datos personales frente al efecto expansivo de Internet y el rol de los motores de búsqueda, es posible el empleo de herramientas técnicas, cuya procedencia, en casos puntuales, corresponde al Organismo consultante, considerando el tipo de información de que se trate, la pertinencia del mantenimiento de la información, y la afectación a los derechos de las personas involucradas y de la población en general.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

NOTA *de* INTERÉS

DINORAH **ALIFA**

MATILDE **CASABÓ**

VALERIA **COLOMBO**

DINORAH
ALIFA
MATILDE
CASABÓ
VALERIA
COLOMBO

Alifa es Licenciada en Relaciones Internacionales y Casabó y Colombo son Licenciadas en Sociología. Integrantes del Área Ciudadanía Digital de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento de Uruguay.

EDUCANDO EN LA PROTECCIÓN DE NUESTROS DATOS PERSONALES

RESUMEN

En el presente artículo las autoras detallan el proceso que derivó en el reforzamiento de los vínculos entre la Unidad encargada de la protección de datos personales en el Uruguay con la entidad a cargo de la enseñanza pública. Se plantean en el artículo los distintos abordajes para la temática, destacándose el trabajo para generar nuevos materiales específicos vinculados a educación y protección de datos, la inclusión de la materia en la currícula escolar y de formación docente y la creación de un concurso para niños y adolescentes con el objetivo de concientizar en los riesgos derivados de un mal uso de los datos personales.

INTRODUCCIÓN

En Uruguay la Ley de Protección de Datos Personales y Acción de Habeas Data (Ley N° 18.331), que data del 18 de agosto del 2008, crea la Unidad Reguladora y de Control de Datos Personales (URCDP), con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios.

Con la masificación de las Tecnologías de Información (TIC) y su presencia extendida en el entretenimiento, el trabajo, la comunicación y la educación, se torna cada vez más significativo el rol de los adultos (padres, tutores, educadores) en la tarea de ayudar a niños y jóvenes a aprovecharlas de forma efectiva y segura.

Tanto educadores como padres se enfrentan además al desafío de mantenerse informados y actualizados sobre la evolución de estas tecnologías y los riesgos que conllevan.

Sin embargo, considerando la información relevada en algunos estudios realizados -tales como las diferentes ediciones del Estudio de Conocimientos, Actitudes y Prácticas de Ciudadanía Digital[1], cuyos resultados se muestran a continuación- surge la necesidad de reforzar acciones para lograr el conocimiento de la población acerca del derecho de protección de datos personales y las formas de ejercerlo.

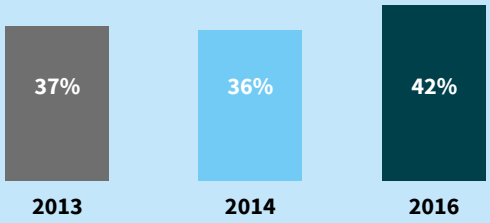
Específicamente en las preguntas relacionadas con el conocimiento y el uso de la Ley de Protección de Datos Personales, los resultados han sido los siguientes:

1 *En el siguiente enlace se podrá encontrar información sobre los principales estudios que se realizan desde la División de Sociedad de la Información y del Conocimiento de AGESIC: http://www.agesic.gub.uy/innovaportal/v/115/1/agesic/estudios-y-mediciones.html?idPadre=20*

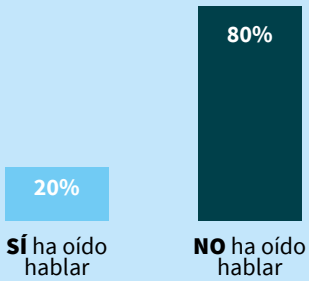
PROTECCIÓN DE DATOS PERSONALES

Base: Mayores de 18 años

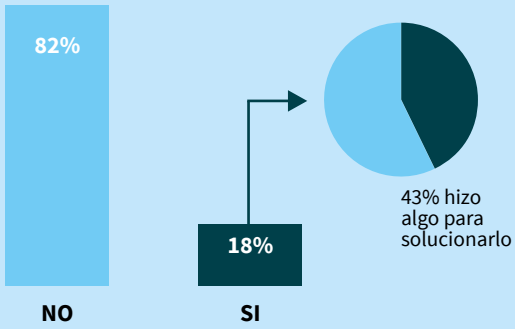
CONOCIMIENTO DEL DERECHO



RECORDACIÓN UNIDAD DE PROTECCIÓN DE DATOS PERSONALES

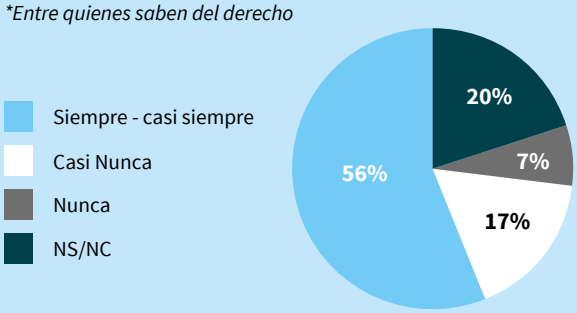


PROBLEMAS CON DATOS PERSONALES



PERCEPCIÓN DEL CUMPLIMIENTO*

**Entre quienes saben del derecho*



Según estos datos, la mayoría de la población uruguaya no sabe que existe una ley que consagra el derecho a la protección de datos personales como un derecho humano fundamental y que brinda garantías y mecanismos para su protección.

Estos resultados nos colocan ante la necesidad de desarrollar una estrategia de sensibilización y formación a la ciudadanía, que permita a todas las personas, conocer, entender y ejercer este derecho, así como las responsabilidades que éste conlleva.

La URCDP, conjuntamente con el área de Ciudadanía Digital de AGESIC, asume el desafío de generar acciones que contribuyan a sensibilizar a la ciudadanía y desarrollar una línea de formación en Protección de Datos Personales.

Entre estas líneas de acción queremos destacar el trabajo realizado en el ámbito educativo formal de Uruguay. En este sentido, desde el año 2013, ANEP y la URCDP han trabajado en conjunto para sensibilizar y capacitar a niños y educadores en la protección de sus datos personales.

En Uruguay la educación primaria es, al igual que los niveles 4 y 5 de inicial, obligatoria. Comienza a los seis años de edad y se organiza en seis grados. Está a cargo de la ANEP (Administración Nacional de Educación Pública) a través del CEIP (Consejo de Educación Inicial y Primaria), que además de gestionar la oferta pública de educación primaria regula y supervisa la oferta privada de este nivel. El objetivo de la educación primaria es *"brindar los conocimientos básicos y desarrollar principalmente la comunicación y el razonamiento que permitan la convivencia responsable en la comunidad".*[2]

La matricula de educación primaria ronda los 325.000 alumnos, distribuidos en 2.131 centros educativos públicos y 413 privados.

EL TRABAJO CONJUNTO DE ANEP Y LA URCDP

A partir de la creciente sensibilidad acerca de la importancia de introducir la temática de Protección de Datos Personales en el ámbito educativo y formar a los niños en el conocimiento y comprensión de su derecho y las buenas prácticas para su protección, es que desde el año 2013, ambas instituciones han desarrollado diversas actividades conjuntas entre las que destacan la capacitación a maestros de todo el país, la elaboración y difusión de una Guía didáctica para el desarrollo de actividades en clase y la realización de un concurso anual.

2 *Ley General de Educacion 18.437, articulo 25*

Para lograr el objetivo de dar a conocer el derecho y generar prácticas y habilidades en los niños, era necesario contar con socios estratégicos que reprodujeran la iniciativa y sus contenidos, aportando el alcance territorial, el contacto directo y la especialidad técnica – didáctica.

Esta iniciativa desarrolla las diferentes dimensiones, que habilitan a transformarse en un modelo replicable:

ABORDAJE INTERINSTITUCIONAL

La iniciativa es liderada por la URCDP, en coordinación con los distintos actores del país que en sumatorio permite generar una sinergia entre educación formal y las políticas públicas. Ellos son Consejo de Educación Inicial y Primaria (CEIP-órgano rector de la Educación Inicial y Primaria en Uruguay-http://www.ceip.edu.uy/), CEIBAL (Ceibal es un plan de inclusión tecnológica y social que ha entregado una computadora por cada niño que asisten a los centros educativos de enseñanza pública-http://www.ceibal.edu.uy/), AGESIC (Agencia para el Desarrollo del Gobierno Electrónico-http://www.agesic.gub.uy) y el IMPO (Centro de Información Oficial-http://www.impo.com.uy/).

PERSPECTIVA INTEGRAL

Se contempla la construcción de capacidades en red, la escuela como institución social que adopta y difunde buenas prácticas en la comunidad en materia de protección de datos personales, el maestro con la capacidad de integrar las temáticas en las actividades curriculares y el niño como agente de cambio social entre sus pares y en su familia a través de la difusión del derecho y la adopción de prácticas responsables.

SOSTENIBILIDAD

Para garantizar la formación de las próximas generaciones es necesaria la integración de la temática en la educación formal de manera permanente. Para eso, entre las actividades que forman parte de la iniciativa, se encuentra la generación en 2017 del 1er Curso de actualización profesional en línea para todos los maestros del país, diseñado en conjunto con CEIP y la creación de una propuesta de integración en la currícula escolar.

Para llevar adelante estas dimensiones se establecieron diferentes líneas de trabajo:

Capacitación presencial a docentes.

Para llegar a nuestro público objetivo que son los niños, necesitamos docentes capacitados y comprometidos en dar a conocer esta temática y trabajarla en cada aula del país.

Se diseñaron y se llevaron a cabo talleres en diferentes localidades del país; procurando llegar a todo el territorio nacional. Estas actividades constan de dos segmentos, el primero a cargo de los abogados de la URCDP, realiza un abordaje teórico capacitando en los siguientes temas: qué es un dato personal, cómo hacemos para cuidarlo, qué derechos y obligaciones tenemos, cuáles son los mecanismos legales que tenemos para denunciar el mal uso de los mismos, etc. El segundo segmento consiste en un taller práctico en el cual se analizan casos reales de la vida docente o del ámbito educativo y los participantes aplican los conocimientos adquiridos a través de propuestas de solución para los mismos.

Elaboración de materiales específicos para docentes.

En conjunto con referentes técnicos de la ANEP diseñamos recursos didácticos para que los docentes pudieran conocer el tema y trabajarlo en clase.

Entre los recursos didácticos diseñados, destaca una Guía para Docentes sobre Protección de Datos Personales, elaborada en base al trabajo de maestros de Primaria y abogados de la Unidad Reguladora.

En esa guía se plantean los contenidos de la ley y diversas maneras de incorporar la temática al aula, de acuerdo al nivel en el que estén los niños.

Para acceder a la guía: https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/5f461508-cef4-4055-a203-379b43183d86/Material+-didactico+para+docentes_Tus+datos+valen.pdf?MOD=AJPERES

Además se generaron videos como recursos didácticos dirigidos a niños y jóvenes, a continuación se presentan algunos ejemplos:

- Video Etiquetado: https://www.youtube.com/watch?v=WXjPtAvN9I0
- Video Datos Personales y Correo Electrónico: https://www.youtube.com/watch?v=AR3P-q6H86FI&t=13s

Inserción de la Protección de Datos Personales en la formación docente.

Desde el año 2016 se desarrollan dos líneas de trabajo conjunto. La primera consiste en incorporar la temática en la formación de los futuros maestros y profesores. En tal sentido, se elaboró con-

juntamente con el Consejo de Formación en Educación[3] en el año 2016 un curso piloto en línea llamado "Educar en la web: manejo responsable de datos y contenidos" en el que participaron 20 docentes y estudiantes. En este año se plantea ampliar la experiencia a más estudiantes en modalidad semi - presencial.

La segunda línea de trabajo se está desarrollando con el Instituto de Formación en Servicio y consiste en desarrollar un curso en línea llamado "La Protección de Datos en la labor docente". El mismo se dirige a docentes, inspectores y directores de centros educativos de todo el país y tiene como objetivo incorporar el conocimiento y las prácticas adecuadas, no solo en el trabajo de los maestros con los niños, sino también en la gestión de los centros educativos.

Concurso anual

Cada año se desarrolla un nuevo concurso, con el objetivo de introducir la temática de protección de datos personales en las aulas de la escuela. Esta iniciativa permite al docente generar un ámbito de trabajo en torno al tema y da la posibilidad que los niños muestren sus conocimientos sobre datos personales mediante el desarrollo de diversas herramientas (afiches, comics, audiovisuales, cuentos). En todos los casos se proponen productos grupales de manera que sea un resultado del trabajo colectivo.

Esta línea de trabajo busca posicionar al niño como agente de cambio en una temática sobre derechos. Considerando al niño como replicador en su hogar y en los espacios en los que participa.

CUATRO AÑOS, CUATRO CONCURSOS, MILES DE NIÑOS DE TODO EL PAIS APRENDIENDO A CUIDAR NUESTROS DATOS PERSONALES

2013

2014

2015

2016

3 *Consejo de Formación en Educación. Tiene a su cargo la formación de maestros, maestros técnicos, profesores, profesores de educación física y educadores sociales, así como de otras formaciones que el Sistema Nacional de Educación requiera.*

CONCURSO 2013
TUS DATOS VALEN, CUIDALOS

CONSIGNA:

Elaborar un afiche donde explique qué son los datos personales.

RESULTADOS:

- *3700 alumnos participaron de la propuesta.*
- *150 afiches presentados.*
- *Participaron 127 escuelas públicas y colegios privados de los 19 departamentos.*

1er PREMIO

Escuela Nº 7, Melo, Cerro Largo

CONCURSO 2014
TUS DATOS, TU DECISIÓN

CONSIGNA:

Elaborar un comic que identifique y resuelva situaciones en las que el uso de los datos personales estén en juego.

RESULTADOS:

- *1100 alumnos participaron de la propuesta.*
- *40 comics presentados.*
- *Participaron 33 escuelas públicas y colegios privados de 11 departamentos.*

1er PREMIO

Escuela Nº 40, Colonia Pintos Viana, Paysandú

MINI-CONCURSO DE VERANO 2015

UNA PROPUESTA EN CONJUNTO CON LOS CENTROS DE ATENCIÓN INFANTIL DE VERANO QUE FUNCIONARON EN EL DEPARTAMENTO DE MALDONADO EN EL VERANO DEL 2015.

CONSIGNA:

Elaborar un afiche, comic o animación que identifique situaciones en las que el uso de los datos personales estén en juego.

RESULTADOS:

- *350 niños participaron de la propuesta.*
- *160 trabajos presentados.*
- *Participaron 21 escuelas públicas del departamento de Maldonado, en el fondo de la foto que aparece a continuación se puede apreciar un mural que difunde el derecho realizado por un grupo de niños.*

CONCURSO 2015
TUS DATOS, TU DECISIÓN. ANIMATE

CONSIGNA:

Elaborar un audiovisual (en 2 categorías: animación y video o filmación) en donde estén en juego la protección de datos personales.

RESULTADOS:

- *900 niños participaron de la propuesta*
- *32 trabajos presentados*
- *Participaron 27 escuelas y colegios del país de 12 departamentos*

1er PREMIO

Escuela N°2, 5º B Vespertino, Paysandú (Capital).

CONCURSO 2016
TUS DATOS CUENTAN

CONSIGNA:

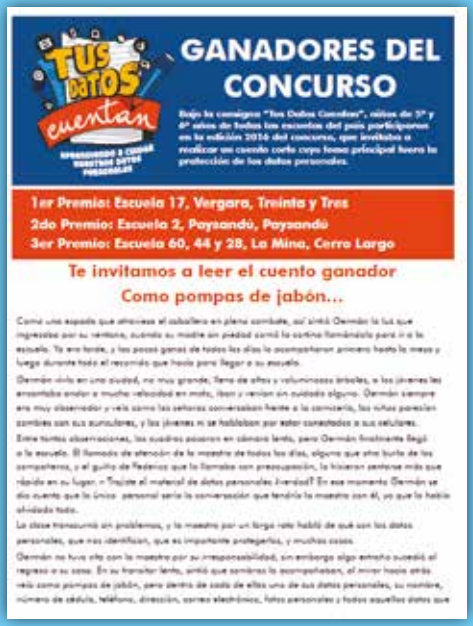
Elaborar un cuento corto colectivo cuyo tema principal fuera la protección de los datos personales.

RESULTADOS:

- *1860 niños participaron de la propuesta*
- *62 trabajos presentados*
- *Participaron 56 escuelas y colegios del país de 14 departamentos*

1er PREMIO

Escuela Nº 17, Vergara, Treinta y Tres


GANADORES DEL CONCURSO

Bajo la consigna "Tus Datos Cuentan", niños de 5° y 6° años de todas las escuelas del país participaron en la edición 2016 del concurso, que invitaba a realizar un cuento corto cuyo tema principal fuera la protección de los datos personales.

1er Premio: Escuela 17, Vergara, Treinta y Tres
2do Premio: Escuela 2, Paysandú, Paysandú
3er Premio: Escuela 60, 44 y 28, La Mina, Cerro Largo

Te invitamos a leer el cuento ganador

Como pompas de jabón...

Y VAMOS POR MÁS...

En junio de 2017, se lanzó la quinta edición del concurso escolar realizado en el marco de la iniciativa "Tus Datos Valen. Cuidalos". Este año el certamen lleva por título: "Me Merezco Datos Protegidos" e invita a niños de 5º y 6º año de las escuelas públicas y privadas del país a crear memes relacionados con la protección de datos personales.


ENTREVISTA

ALESSANDRA PIERUCCI

Es abogada y ha estado trabajando desde hace varios años en la Autoridad de Protección de Datos italiana, en particular en asuntos internacionales y vinculados a la Unión Europea.

Ha estado involucrada activamente en protección de datos a nivel del Consejo de Europa, representando a Italia en el Comité Consultivo del Convenio 108, del que se convirtió en Presidente en 2016.

Trabajó en la División Sociedad de la Información y Medios del Consejo de Europa, donde tuvo a consideración cuestiones tales como la protección de datos y libertad de expresión con referencia a los nuevos medios de comunicación y la sociedad de la información, y la equidad de género y los medios de comunicación.

Colabora regularmente con la actividad del Grupo de Trabajo del Artículo 29 (WP29) de la Unión Europea, en particular a través de la coordinación del trabajo del subgrupo en protección de datos en el sector financiero. Asimismo, colaboró con el Grupo de Trabajo en Seguridad de la Información de la OCDE.

Participó en varios proyectos en protección de datos y prestó asesoramiento legal en esa materia. Como parte de sus actividades de investigación, ha publicado varios trabajos vinculados a cuestiones de derechos fundamentales y protección de datos en revistas jurídicas y libros. Ha enseñado protección de datos en cursos de posgrado en universidades europeas.

1. YOU HAVE RECENTLY BEEN ELECTED CHAIR OF THE CONSULTATIVE COMMITTEE OF CONVENTION 108 (T-PD). WHAT ARE YOUR THOUGHTS ON THE MODERNIZED VERSION OF THE CONVENTION AND WHEN CAN WE EXPECT ITS ENTRY INTO FORCE?

Convention 108 is an extremely valuable instrument for a number of reasons: it is the only legally binding tool for data protection at international level; it is open to any country, as it can be acceded also by non-members of the Council of Europe, it sets forth a high level of protection for fundamental rights by means of flexible standards. Its modernization– which aims at ensuring that the high level of protection provided by the Convention is guaranteed in the new technological and globalized landscape we currently live in - is an historical opportunity we should exploit in the best way.

Its entry into force depends on some remaining controversial issues which are now being negotiated at the Committee of Ministers level.

My strong wish is that negotiating parties will do their best to find appropriate solutions to the outstanding issues, thereby enabling the modernized Convention to enter into force as soon as possible and, in any case, at the latest in May 2018. As the European Data Protection Authorities highlighted in the Resolution adopted at the last Spring Conference in Cyprus, any further delay of the finalization of the modernization will create legal difficulties also in relation to the EU legal instruments, which will ultimately be detrimental for the protection of fundamental rights.

With the application of the EU General Regulation on data protection and the transposition of Directive on Police and Justice (both due by May 2018), it will be even more important to have the new Convention, as it ensures full compatibility with the EU data protection framework.

1. USTED HA SIDO ELEGIDA RECIENTEMENTE PRESIDENTE DEL COMITÉ CONSULTIVO DEL CONVENIO 108 (T-PD). ¿QUÉ PIENSA USTED DE LA VERSIÓN MODERNIZADA DE LA CONVENCIÓN Y CUÁNDO PODEMOS ESPERAR QUE ENTRE EN VIGOR?

El Convenio 108 es un instrumento extremadamente valioso por varias razones: es el único instrumento jurídicamente vinculante para la protección de datos a nivel internacional, está abierto a cualquier país, en tanto puede ser adherido también por no miembros del Consejo de Europa, y establece un alto nivel de protección a los derechos fundamentales a través de estándares flexibles. Su modernización -que tiene como objetivo garantizar el alto nivel de protección que ofrece el Convenio en el nuevo entorno tecnológico y globalizado en que actualmente vivimos - es una oportunidad histórica que deberíamos explotar de la mejor manera posible.

Su entrada en vigor depende de algunos temas polémicos pendientes que se están negociando actualmente a nivel del Comité de Ministros.

Mi mayor deseo es que las partes negociadoras hagan todo lo posible por encontrar soluciones adecuadas a las cuestiones pendientes, permitiendo así que el Convenio modernizado entre en vigor lo antes posible y, en cualquier caso, a más tardar en mayo de 2018. Tal y como destacaron las Autoridades Europeas de Protección de Datos en la Resolución aprobada en la última Conferencia de Primavera en Chipre, cualquier retraso adicional en la finalización de la modernización generará dificultades legales también en relación con los instrumentos jurídicos de la UE, lo que en última instancia será perjudicial para la protección de los derechos fundamentales.

Con la aplicación del Reglamento General de la UE sobre la protección de datos y la transposición de la Directiva sobre Policía y Justicia (ambas previstas para mayo de 2018), será aún más importante tener el nuevo Convenio, en tanto éste garantiza la plena compatibilidad con el marco de referencia sobre protección de datos de la UE.

2. WHAT DO YOU WOULD LIKE TO ACCOMPLISH DURING YOUR TIME AS CHAIR OF THE T-PD? DO YOU HAVE ANY SPECIFIC GOALS OR OBJECTIVES?

Although the Consultative Committee has accomplished its task in respect of the technical revision of Convention 108, my biggest hope is to see the finalization of the new Convention during my mandate.

The revised Convention provides for a strengthened role for the future Committee which will be called upon to evaluate candidates for accession and to follow-up the implementation of the Convention by the Parties to the Convention. One of the T-PD's objectives for the next future is therefore to work on the modalities and mechanisms for the purposes of evaluating and following-up the implementation of the Convention to ensure effective protection of personal data.

Other objectives of the Committee will be to accomplish the revision process of other CoE's instruments such as the Recommendation (97)5 on health data (again, to react to the manifold challenges for data protection coming from new technologies), and to prepare practical guidance for data processing in the police sector. What is also in the goals of the Committee is to evaluate new frontiers and challenges for data protection such as in the context of artificial intelligence.

3. WHY SHOULD A NON EUROPEAN COUNTRY ACCEDE TO CONVENTION 108?

A non-European country should accede Convention 108 because it is a set of flexible but substantive principles for the protection of fundamental rights with regard to processing of data.

The respect for data protection standards is now a pre-requisite for exchanges of any sort (including commercial) and the adhesion to Convention 108 represents a serious commitment by the Party which can be spent in its relationship with other international interlocutors.

An additional and very significant value of the accession is also acknowledged by the EU GDPR. Recital 105 of the GDPR says that in the assessment carried out by the European Commission on the adequacy of a third country (without which the transfer from EU to such country would be in principle prohibited), the third country's accession to Convention 108 is an element to be (positively) considered.

2. ¿QUÉ LE GUSTARÍA LOGRAR DURANTE SU TIEMPO COMO PRESIDENTE DE LA T-PD? ¿TIENE METAS U OBJETIVOS ESPECÍFICOS?

Aunque el Comité Consultivo ha cumplido su tarea con respecto a la revisión técnica del Convenio 108, mi mayor esperanza es ver la finalización del nuevo Convenio durante mi mandato.

El Convenio revisado proporciona una futura Comisión con un rol fortalecido, la que será llamada a evaluar a los candidatos a la adhesión y a dar seguimiento a la implementación del Convenio por las Partes del Convenio. Por lo tanto, uno de los objetivos del T-PD para el futuro próximo es trabajar en las modalidades y mecanismos para evaluar y hacer un seguimiento a la aplicación del Convenio que asegure una protección eficaz de los datos personales.

Otros objetivos del Comité consistirán en llevar a cabo el proceso de revisión de otros instrumentos del Consejo de Europa, como la Recomendación (97) 5 sobre datos de salud (nuevamente para responder a los múltiples desafíos que plantean las nuevas tecnologías para la protección de datos) y para preparar guías prácticas para el procesamiento de datos en el sector policial. Otros de las metas del Comité es evaluar nuevas fronteras y desafíos para la protección de datos, como es en el contexto de la inteligencia artificial.

3. ¿POR QUÉ UN PAÍS NO EUROPEO DEBERÍA ADHERIRSE AL CONVENIO 108?

Un país no europeo debería adherirse al Convenio 108 porque se trata de un conjunto de principios flexibles y al mismo tiempo sustantivos, para la protección de los derechos fundamentales en lo que respecta al tratamiento de los datos.

El respeto a las normas de protección de datos es hoy un requisito previo para los intercambios de cualquier tipo (incluido el comercial) y la adhesión al Convenio 108 representa un compromiso serio de una Parte que puede ser usado en sus relaciones con otros interlocutores internacionales.

Un valor adicional y muy significativo de la adhesión también es reconocido por el Reglamento General de Protección de Datos de la UE. El considerando 105 del Reglamento afirma que en la evaluación realizada por la Comisión Europea sobre la adecuación de un tercer país (sin la cual, en principio, se prohibiría la transferencia de la UE a dicho país), la adhesión del tercer país al Convenio 108 es un elemento a ser (positivamente) considerado.

4. WHAT ARE THE BENEFITS OF BECOMING A MEMBER OF THE CONVENTION FROM THE PERSPECTIVE OF TRANSBORDER FLOWS OF INFORMATION?

The main idea of the Convention is that free flow of information is ensured among the Parties, therefore being member of the Convention is already an advantage in this respect. Becoming a member of the Convention means entering a community which provides for appropriate safeguards and towards which transfers will be more easily considered legitimate.

Generally speaking, the perspective of the Convention is not to limit the flow of information but to ensure that such flows are carried out while guaranteeing data subjects' rights.

5. THE NEW GENERAL DATA PROTECTION REGULATION WILL ENTER INTO FORCE IN 2018, BRINGING IMPORTANT CHANGES IN THE WAY DPAS, CONTROLLERS AND PROCESSORS ADDRESS THIS ISSUE. DO YOU THINK THAT THEY ARE PREPARED FOR THE CHANGES THAT THE REGULATION IMPLIES? HOW HAS THE ITALIAN DPA BEEN PREPARING?

The entering into force of the GDPR is a revolution for controllers and processors but also for regulators, although well-founded on a core of principles already included in Directive 95/46.

Generally speaking, I see a lot attention paid by many sectors towards the novelties of the Regulation, and this is a positive sign as the implementation of the principles of the GDPR has to be prepared with a certain margin of time.

Our DPA is actively working on the GDPR, in particular by focusing on two main actions: on the one hand, the elaboration of guidance for data controllers/data processors that will help them in getting ready for the compliance with most of the GDPR rules before May 2018. In parallel, our DPA is carrying out an assessment on the validity - in the light of the GDPR- of the many decisions which have been adopted over the years. Our DPA has just celebrated its 20th anniversary and we of course have an important heritage we would like to preserve, where consistent with the new EU framework.

4. ¿CUÁLES SON LOS BENEFICIOS DE CONVERTIRSE EN MIEMBRO DEL CONVENIO DESDE LA PERSPECTIVA DE LOS FLUJOS TRANSFRONTERIZOS DE INFORMACIÓN?

La idea principal del Convenio es que se garantice la libre circulación de información entre las Partes, por lo que ser miembro del Convenio ya es una ventaja a este respecto. Convertirse en miembro del Convenio significa entrar en una comunidad que provee salvaguardas apropiadas y hacia la cual las transferencias serán más fácilmente consideradas legítimas.

En términos generales, la perspectiva del Convenio no es limitar el flujo de información, sino asegurar que dichos flujos se realicen garantizando al mismo tiempo los derechos de los titulares de los datos.

5. EL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) ENTRARÁ EN VIGOR EN 2018, INTRODUCIENDO IMPORTANTES CAMBIOS EN LA FORMA EN QUE LAS APD, LOS RESPONSABLES Y LOS ENCARGADOS ABORDAN ESTA TEMÁTICA. ¿CREE USTED QUE ESTÁN PREPARADOS PARA LOS CAMBIOS QUE IMPLICA EL REGLAMENTO? ¿CÓMO SE HA ESTADO PREPARANDO LA APD ITALIANA?

La entrada en vigor del RGPD es una revolución para los responsables y encargados, pero también para los reguladores, aunque esté basada en un conjunto de principios fundamentales ya incluidos en la Directiva 95/46.

En términos generales, veo que muchos sectores prestan mucha atención a las novedades del Reglamento, lo cual es positivo, ya que la aplicación de los principios del RGPD debe prepararse con un cierto margen de tiempo.

Nuestra APD está trabajando activamente en el RGPD, en particular centrándose en dos acciones principales: por una parte, la elaboración de directrices para los responsables de tratamiento / encargados de tratamiento que les ayudarán a prepararse para el cumplimiento de la mayoría de las reglas del RGPD antes de mayo de 2018. Paralelamente, nuestra APD está llevando a cabo una evaluación de la validez -a la luz del RGPD- de las numerosas decisiones que se han adoptado a lo largo de los años. Nuestra APD acaba de celebrar su 20 aniversario y, por supuesto, tenemos una importante herencia que nos gustaría preservar, en consonancia con el nuevo marco de la UE.

6. THE T-PD HAS RECENTLY ISSUED GUIDELINES ON BIG DATA WITH RECOMMENDATIONS FOR CONTROLLERS AND PROCESSORS AS A FIRST STEP TOWARDS A STRONGER PROTECTION FOR INDIVIDUALS. CAN YOU TELL US WHAT ARE THE FUTURE PLANS OF THE COMMITTEE TO ADDRESS THIS ISSUE?

As expressly stated in the Guidelines adopted by the T-PD, such document provides for a first general guidance for controllers/processors but also for legislators to apply appropriate policies and measures to make effective the principles of Convention 108 in the context of Big Data.

These Guidelines may however be revised in the future in light of the evolution of technologies and complemented by further guidance and tailored best practices within specific fields of application of Big Data. The T-PD will evaluate whether to intervene again in such sector. However, the current work of the Committee – such for example on the Recommendation on health data – is already taking into due account the issues raised by Big data and the principles set forth in this respect by the Guidelines.

7. IN REGARD TO THE "RIGHT TO BE FORGOTTEN" AND ITS APPLICATION IN EUROPE, THE ITALIAN DPA DECLARED RECENTLY THAT CERTAIN JUDICIAL CASES WHERE EXCLUDED FROM ITS APPLICATION WHEN THEY REFERRED TO SERIOUS MISDEMEANORS OR POSED A SOCIAL ALARM. WHAT ARE IN YOUR VISION THE LIMITATIONS TO THE SO CALLED "RIGHT TO BE FORGOTTEN"?

The case you probably refer to concerns a decision by the Italian DPA which denied to an ex-terrorist the delisting from search engines of news concerning his crimes. Such example shows that the balancing between the right to be informed and the right to privacy is a sensitive issue which must be carried out on a case by case basis. In the example you mentioned such news was still actual and the crimes had relevant repercussions on the society and even on the history of our country.

The conclusions of our DPA may have been different if, for example, the request concerned a crime committed many years before but with no persistent relevance for the public opinion. In that case the right to be forgotten and to renew the person's identity could have prevailed.

6. EL T-PD HA PUBLICADO RECIENTEMENTE DIRECTRICES SOBRE "BIG DATA" CON RECOMENDACIONES PARA RESPONSABLES Y ENCARGADOS COMO UN PRIMER PASO HACIA UNA MAYOR PROTECCIÓN PARA LAS PERSONAS. ¿PUEDE DECIRNOS CUÁLES SON LOS PLANES FUTUROS DEL COMITÉ PARA ABORDAR ESTE ASUNTO?

Como se indica expresamente en las Directrices adoptadas por el T-PD, dicho documento proporciona una primera orientación general a los responsables/encargados, pero también a los legisladores para que apliquen políticas y medidas adecuadas para hacer efectivos los principios del Convenio 108 en el contexto de "Big Data".

Sin embargo, estas Directrices pueden ser revisadas en el futuro a la luz de la evolución de las tecnologías y complementadas con posteriores directrices y mejores prácticas adaptadas dentro de campos específicos de aplicación de "Big Data". El T-PD evaluará si debe intervenir nuevamente en dicho sector. Sin embargo, el trabajo actual del Comité - por ejemplo, en la Recomendación sobre datos de salud - ya está teniendo debidamente en cuenta las cuestiones planteadas por el "Big Data" y los principios establecidos a este respecto por las Directrices.

7. EN LO QUE SE REFIERE AL "DERECHO AL OLVIDO" Y A SU APLICACIÓN EN EUROPA, LA APD ITALIANA DECLARÓ RECIENTEMENTE QUE ALGUNOS CASOS JUDICIALES QUEDARON EXCLUIDOS DE SU APLICACIÓN CUANDO SE REFERÍAN A DELITOS GRAVES O QUE SUPONÍAN UNA ALARMA SOCIAL. ¿CUÁLES SON EN SU VISIÓN LAS LIMITACIONES AL LLAMADO "DERECHO AL OLVIDO"?

El caso al que probablemente usted se refiere tiene que ver con una decisión de la APD italiana que negó a un ex terrorista su exclusión de los motores de búsquedas de las noticias sobre sus crímenes. Este ejemplo demuestra que el equilibrio entre el derecho a la información y el derecho a la privacidad es un asunto sensible que debe llevarse a cabo caso por caso. En el ejemplo que usted mencionó esa noticia era real y los crímenes tuvieron repercusiones relevantes en la sociedad e incluso en la historia de nuestro país.

Las conclusiones de nuestra APD pudieron haber sido diferentes si, por ejemplo, la solicitud se refería a un delito cometido muchos años antes, pero sin una relevancia persistente para la opinión pública. En ese caso, podría haber prevalecido el derecho al olvido y a la renovación de la identidad de la persona.

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay