Revista Uruguaya de Protección de Datos Personales

No. 5 - Año 2020

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Uruguay Presidencia

agesic

CONTENIDOS





Sección Doctrina

Explicabilidad: hacia una IA confiable

M. Àngels Barbarà Fondevila

Autoridad catalana en protección de datos. Licenciada en Derecho por la Universidad de Barcelona. Máster por ESADE en Función Gerencial en las Administraciones Públicas. Diplomada por la Universidad Menéndez Pelayo sobre Participación de las Comunidades Autónomas en las decisiones del Estado. Diplomada por el Ministerio de Asuntos Exteriores sobre "Las Comunidades Europeas". Diplomada por ESADE sobre Función Directiva en las Organizaciones Públicas y Privadas.En el ámbito profesional, desde julio de 2012 es la directora de la Autoridad Catalana de Protección de Datos Ha sido secretaria general del Departamento de Gobernación y Relaciones Institucionales de la Generalitat de Cataluña, en dos legislaturas distintas, cargo desde el que dirigió la creación de la Agencia (hoy Autoridad) Catalana de Protección de Datos. Ha sido presidenta de la comisión ejecutiva de la Administración Abierta de Cataluña, presidenta de la Agencia Catalana de Certificación, presidenta de la comisión para el Impulso de los Medios Electrónicos en la Administración, vicepresidenta del consejo de administración del Centro de Telecomunicaciones y Tecnologías de la Información, miembro de la comisión bilateral Estado Generalitat de Cataluña, miembro de la comisión parlamentaria para el Pacto Fiscal y miembro del consejo general de la Feria de Barcelona, entre otros cargos.

Resumen

En los últimos años se ha extendido el uso de la Inteligencia Artificial a todo tipo de aplicaciones. Si bien los beneficios son indiscutibles, también hay que tener en cuenta los riesgos, sobre todo en aquellas aplicaciones que tienen un impacto significativo sobre las personas. Necesitamos una Inteligencia Artificial confiable. En esta, la explicabilidad de las decisiones es un elemento fundamental; no solo sirve para entender el porqué de las decisiones, sino que nos permite determinar si la decisión es correcta y justa. Todas estas cuestiones son muy importantes desde un punto de vista legal pero ético, como es el caso de las limitaciones y condiciones que pone a las decisiones automatizadas el Reglamento General de Protección de Datos de la Unión Europea.

Lamentablemente la complejidad de gran parte de los modelos utilizados hoy en día hace que sean una caja negra. En los últimos años hay un renovado interés por explicar las decisiones de los sistemas de Inteligencia Artificial. Se espera que la tercera oleada de Inteligencia Artificial nos traiga sistemas que se adapten al contexto, abstrayendo de la experiencia y razonando, y que sean fácilmente explicables. Entre tanto se está desarrollando la Inteligencia Artificial explicable. Esta es más pragmática, no busca superar las técnicas actuales, solo quiere darnos una explicación para las decisiones. Veremos que esta es una tarea ardua y con muchas limitaciones.

Introducción

Desde sus inicios a mediados del siglo pasado, la Inteligencia Artificial (IA) ha vivido una sucesión de períodos de grandes expectativas seguidos de otros de pérdida de interés. Ha sido la incapacidad de dar respuesta a las expectativas del momento lo que la lleva al desánimo, a la cancelación de proyectos y a la reducción drástica de la inversión; son los conocidos inviernos de la IA .[1]

En la última década hemos vivido el período más brillante de esta disciplina. El incremento en el poder computacional, el desarrollo de nuevas técnicas y, sobre todo la gran abundancia de datos, ha permitido multitud de nuevas aplicaciones. La IA se ha democratizado; han llegado con fuerza a toda la sociedad. Desde cosas tan inocuas como recomendar películas o libros, hasta otras tan delicadas como la conducción autónoma o el diagnóstico de enfermedades. Nuestra sociedad es, cada vez más, una sociedad dominada por algoritmos.

Esta gran socialización de la IA ha puesto sobre la mesa el próximo gran reto a que se enfrenta: una IA ética y confiable. Este es un reto de una gran magnitud, no solo por su complejidad técnica, sino principalmente por los profundos efectos que puede tener sobre nuestra sociedad. Es una cuestión que no se puede postergar si queremos que la IA mantenga el firme desarrollo que tiene actualmente.

La necesidad de una IA confiable, que actúe siguiendo unos parámetros éticos, es obvia cuando observamos el gran impacto que tienen sobre las personas algunas de sus aplicaciones. En los coches autónomos, en la gestión de recursos sanitarios o en el diagnóstico de enfermedades la decisión que toma un sistema IA puede marcar la diferencia entre la vida y la muerte.

Hasta ahora, la IA está sujeta únicamente a las regulaciones sectoriales que aplican a cada uso concreto y, en la medida en que usa datos personales, a las regulaciones de protección de datos. Es particularmente relevante el artículo 22 del Reglamento General de Protección de Datos [2], que evita el problema de las decisiones automatizadas que puedan tener un impacto significativo sobre las personas exigiendo la intervención humana.

Sin embargo, el gran impacto de algunos sistemas IA, ha hecho que muchos países estén considerando la necesidad de una regulación específica que promueva el desarrollo de una IA confiable. Por la variedad de aplicaciones de la IA, este es un tema muy complejo y parece razonable una regulación para aquellas aplicaciones o sectores más críticos. En la Unión Europea se ha hecho un trabajo muy significativo en estos últimos cuatro años[3] [4] [5] . Todo este trabajo debe culminar en una regulación para la IA prevista para el último trimestre de 2020. Aunque no hay que olvidar la fuerza de algunos grupos de presión que claman por una IA desregulada para no limitar su desarrollo. Argumentan que es una tecnología disruptiva y que el país que la lidere tendrá una gran ventaja competitiva.

Entre las propiedades que comúnmente se asocian a la AI confiable, este artículo se centrará en la explicabilidad. Este es un campo en el que las tecnologías actuales son deficientes. La Inteligencia Artificial explicable[6] persigue el desarrollo de modelos sofisticados que sean inherentemente explicables. Mientras estos no están disponibles, se impone un enfoque pragmático: buscar maneras de abrir la caja negra, aunque sea de manera parcial.

Explicabilidad en el contexto de una IA confiable

Desde un punto de vista técnico un sistema IA es un algoritmo cuyo objetivo es cumplir ciertas ecuaciones matemáticas. En este sentido no se diferencia de un algoritmo que se use, por ejemplo, para diseñar un puente. La diferencia está en el uso que les vamos a dar y en como este uso afectará a las personas.

En general, decimos que un sistema es confiable cuando se comporta consistentemente de la forma esperada. Mientras que en caso de un puente esto quiere decir que se cumplen los parámetros de resistencia para los que se diseñó, en el caso de la IA, la gran diversidad de aplicaciones hace que las propiedades sean muy variadas: precisión, robustez, equidad, responsabilidad, explicabilidad y comportamiento ético, entre otras.

---

1. D. Crevier. "AI: The Tumultuous Search for Artificial Intelligence", New York, BasicBooks, 2013.
2. 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.
3. Grupo independiente de expertos de alto nivel sobre Inteligencia Artificial. "Directrices para una IA fiable", 8 de abril de 2019.
4. Expert group on liability and new tecnologies. "Liability for artificial intelligence and other emergint digital technologies", 21 de noviembre de 2019
5. European Comission. "White paper on artificial intelligence - A european approach to excellence and trust", 19 de febrero de 2020, COM (2020) 65 final.
6. DARPA. "Explainable Artificial Intelligence (XAI)", 2017.

Precisión

Los sistemas de IA se entrenan sobre un conjunto de datos de entrenamiento, pero el objetivo es que se ejecute sobre datos nuevos (desconocidos). La precisión mide como de bien se comporta el sistema sobre estos datos desconocidos.

Robustez

Como cualquier otro sistema, la IA también puede ser atacada. Por ejemplo, la capacidad de estos sistemas de continuar aprendiendo mientras funcionan puede ser aprovechada por un atacante para alterar progresiva e intencionadamente las decisiones que toma. Cuanta más resistencia tenga un sistema a estos ataques, más robusto es un sistema IA.

Equidad

Un sistema es equitativo cuando no discrimina. Los sesgos de un sistema IA tienen orígenes diversos: un modelo inapropiado, unos datos sesgados o, incluso, la noción concreta de lo que es justo.

Responsabilidad

Es inevitable que los sistemas IA cometan errores. Cuando las consecuencias de estos errores son significativas es importante determinar quién de entre todos los actores que intervienen tiene la responsabilidad. Por ejemplo, ¿quién es el responsable si un coche autónomo circula en sentido contrario porque han cambiado el sentido de circulación en una calle y el mapa no está actualizado?

Explicabilidad

En general, no creemos ciegamente en médico que no puede razonar su diagnóstico. Lo mismo pasa con la IA. A medida que las decisiones de la IA incrementan su impacto sobre las persones, se hace más necesaria una explicación de las mismas.

Comportamiento ético

La IA es una tecnología con un gran potencial, pero no debemos olvidar que no es ajena a la sociedad. Ya que su impacto puede ser muy alto, tiene que respetar los valores éticos de la sociedad en la que actúa. Los problemas éticos pueden ser muy variados y de difícil solución, pero hay que afrontarlos para evitar que la respuesta venga dada por sesgos en el diseño o en los datos. Por ejemplo, ¿debe un coche autónomo evitar un coche frontal si en la maniobra se pone en riesgo a unos peatones?.

Conceptos clave

Inteligencia Artificial (IA). Es un término que engloba todos aquellos algoritmos que buscan dotar a los ordenadores de un comportamiento inteligente.

Caja negra (black box). Cada aplicación de la IA se basa en un modelo de representación del conocimiento, que puede ser muy variado (desde un sencillo conjunto de reglas hasta una compleja red neuronal). Cuando este modelo es tan complejo que aun conociéndolo somos incapaces de entender el porqué de las decisiones que toma, se dice que actúa como una caja negra. Esta caja negra recibe unas entradas y produce una salida, pero la relación entre entradas y salida es desconocida.

Primera oleada (First wave). El desarrollo de la IA se ha producido en diferentes oleadas. En la primera, los sistemas IA se basaban en conjuntos de reglas que eran introducidas manualmente. El objetivo era introducir en el sistema todo el conocimiento que había sobre un tema para que este fuera capaz de aplicarlo usando razonamiento lógico. La gran limitación de estos sistemas era su incapacidad de aprender a partir de la experiencia; tampoco gestionaban bien la incertidumbre. Si bien esta es una tecnología antigua que tuvo un ámbito de desarrollo eminentemente académico, sigue habiendo aplicaciones concretas en las que resulta muy útil. Por ejemplo, el sistema Mayhem[7] , que ganó la competición de ciberseguridad Cyber Grand Challenge organizada por la DARPA.

Segunda oleada (Second wave). Es el momento actual de la IA. La disponibilidad de datos y el suficiente poder computacional para procesarlos han permitido el uso de modelos de IA que extraen el conocimiento de la experiencia (de los datos); es el conocido aprendizaje

7. D. Brumley. "Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them", IEEE Spectrum, 29 Jan 2019

automático. En esta segunda oleada, el poder de la IA de clasificar y predecir se ha incrementado mucho. Aún así sigue habiendo muchas limitaciones: no hay una noción del contexto (el sistema solo ve casos particulares), la complejidad de muchos de los modelos utilizados hace que muchas veces sea una caja negra (un caso paradigmático es el aprendizaje profundo, que simula una red neuronal compleja), los sistemas son precisos, pero poco fiables (lo hacen bien una y otra vez, pero ocasionalmente tienen errores que nadie espera), etc.

Tercera oleada (Third wave). En el futuro se espera mejorar la adaptación contextual de la Inteligencia Artificial. Por muy sofisticadas que sean las aplicaciones de la IA actuales, están restringidas al contexto concreto para el que se han diseñado. Por ejemplo, el software que conduce un modelo concreto de coche autónomo es inútil en otro coche diferente. No es así en el caso de las personas, que una vez han aprendido, pueden conducir cualquier coche. Esto se debe a que la capacidad de abstracción y razonamiento de las personas les permite adaptarse al contexto. En la tercera ola se espera que la IA tenga la capacidad de abstraer el conocimiento obtenido de la experiencia y aplicarlo en otros contextos. Desde el punto de vista de la protección de datos, esto ha de permitir reducir la cantidad de datos necesaria para entrenar a los sistemas IA (ya no será necesario que el sistema sea entrenado teniendo en cuenta todas las situaciones posibles) y mejorar la explicabilidad.

Explicabilidad en el desarrollo de la IA

La explicabilidad de los sistemas IA no es una novedad: se empezó a estudiar en los años 70 del siglo pasado, en el contexto de los sistemas expertos. Estos sistemas buscaban incorporar el conocimiento de expertos humanos en un tema en base a una serie de reglas que se introducían manualmente. El hecho de ser sistemas basados en reglas hacía que tuvieran intrínsecamente un alto grado de explicabilidad, ya que se podía seguir el rastro de las decisiones en función de las reglas aplicadas.

En la última década hemos vivido el boom del aprendizaje automático y del aprendizaje profundo. La capacidad de aprendizaje de estas tecnologías en base a unos datos de entrenamiento ha sido revolucionaria. Unida a la gran disponibilidad de datos, ha permitido aplicaciones de IA que poco antes eran ciencia-ficción: la traducción automática, el reconocimiento de imágenes, la redacción de textos, etc. Para estas tareas no hay un algoritmo conocido y, por tanto, no es posible dar unas reglas para llevarlas a cabo. El aprendizaje automático nos permite que el sistema aprenda ajustando su funcionamiento a los ejemplos usados en el entrenamiento. La versatilidad de estos sistemas conlleva, en muchos casos, una gran complejidad en su funcionamiento interno, que hace que incluso el acceso al modelo entrenado no dé pautas significativas sobre su funcionamiento.

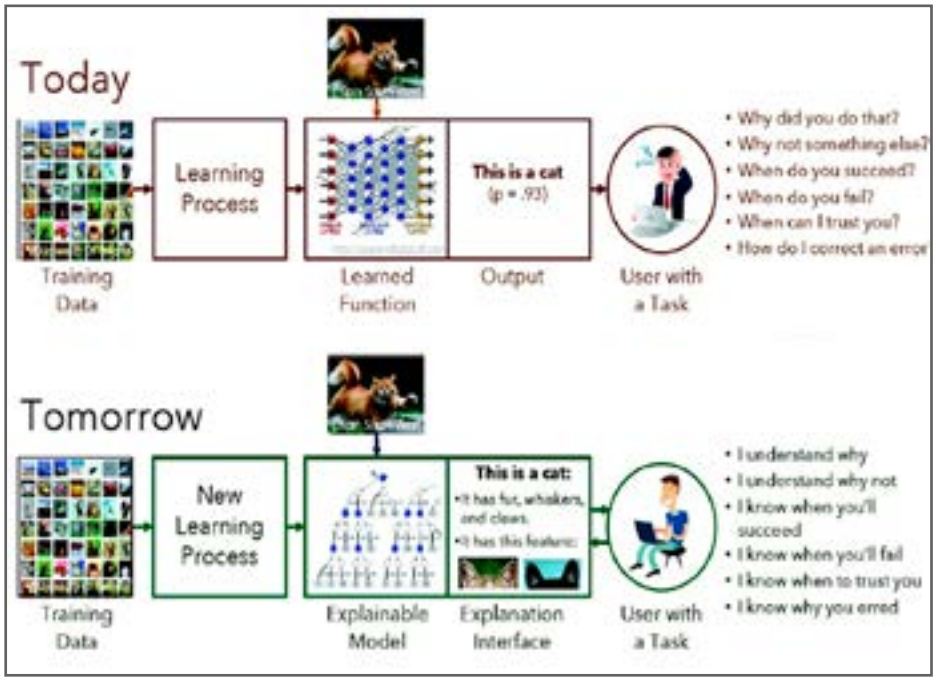

Ilustración 1.
Con la IA actual no sabemos el porqué de la decisión, cosa que conlleva diferentes problemas. En el futuro, se espera que las decisiones de la IA sean más fácilmente interpretables (Fuente: DARPA XAI program Update 2017).

De hecho, con el boom del aprendizaje automático, el foco se ha centrado en extender el uso de la IA a todo tipo de aplicaciones, poniendo énfasis en la precisión de estos sistemas y dejando de lado la explicabilidad de las decisiones. Ahora bien, ha sido el gran éxito del aprendizaje automático que, ante el impacto de algunos de sus usos, ha puesto de nuevo en relieve la importancia de la explicabilidad. Y ha dado lugar a lo que se conoce como Inteligencia Artificial explicable (XAI). **Ver Ilustración 1**.

¿Para qué queremos una IA explicable?

Desde el punto de vista de la protección de datos, la utilidad principal de una IA explicable es que las personas que la utilizan puedan entender el porqué de las decisiones y evaluar si son correctas y justas. Pero su utilidad no se limita a esto:

Explicar para justificar. Las controversias por trato discriminatorio son una constante en muchas de las aplicaciones de la IA. Por ejemplo, la discriminación por razón de sexo en los sistemas de selección de personal, o la discriminación por razón de origen racial en sistemas de reconocimiento facial. Poner a disposición del usuario final una explicación del porqué de la decisión es una manera de mostrar al usuario que se le está dando un trato justo.

Explicar para controlar. Tener una explicación de las decisiones tomadas permite a los operadores del sistema revisar si las decisiones son adecuadas, detectar los fallos con mayor rapidez y solucionarlos antes de que tengan consecuencias importantes.

Explicar para mejorar. Las explicaciones de un sistema IA nos permite detectar aquellas decisiones que no son óptimas y, así, mejorar el sistema.

Explicar para descubrir. Es cierto que la IA no ha llegado al nivel de la inteligencia humana, capaz de interactuar en todo tipo de entornos. Ahora bien, en algunos campos concretos las capacidades de la IA superan a las humanas. En estos campos, tener una explicación de las decisiones tomadas por el sistema IA es una fuente de conocimiento que no hay que desaprovechar.

Explicabilidad, complejidad y precisión del modelo

La explicabilidad de un sistema IA es inversamente proporcional a su complejidad. Así, la forma más fácil de conseguir explicabilidad es usar modelos que sean sencillos; es decir, que sean intrínsecamente interpretables. Por ejemplo, modelos basados en reglas [8] o modelos lineales [9].

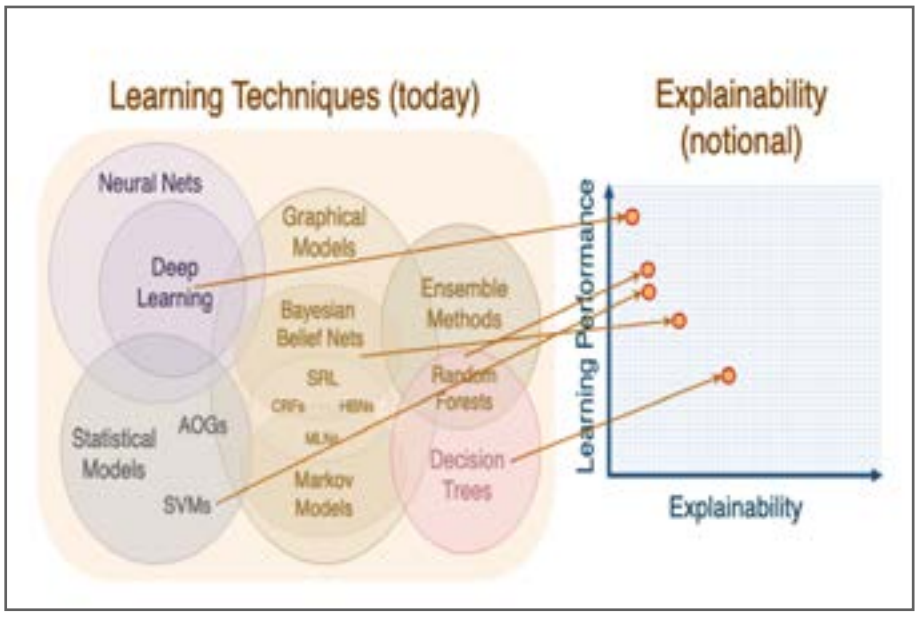

Ilustración 2.
Relación entre la precisión y explicabilidad en las técnicas AI actuales. A mayor complejidad del modelo, mayor precisión, pero menor explicabilidad de las decisiones (Fuente: DARPA XAI program Update 2017).

Ahora bien, es bien conocido que el poder de un modelo (es decir, la capacidad que tiene para modelar una situación concreta) está directamente relacionado con su complejidad [10].

Por tanto, los modelos sencillos (e interpretables) serán útiles solamente para tareas de baja complejidad. El uso de modelos sencillos para tareas de alta complejidad comporta un alto coste en términos de precisión. Ver Ilustración 2.

8. B. G. Buchanan y R. O. Duda. "Principles of rule-based systems", Standford University Report STAN-CS-82-926, 1982
9. G. James, D. Witten, T. Hastie y R. Tibshirani. "An Introduction to Statistical Learning", Springer Texts in Statistics.
10. S. Sankar. "Accuracy and interpretability trade-offs in machine learning applied to safer gambling". In Proceedings of the International Conference on Machine Learning (ICML), 2015, pp. 1–10.

La alternativa al uso de modelos sencillos es utilizar modelos complejos (tipo caja negra), que tienen alta precisión, combinados con técnicas para explicar las decisiones. Más adelante se describen algunas de estas técnicas.

Conviene no confundir la descripción de la lógica del modelo de IA usado con la explicabilidad. Conocer el funcionamiento abstracto de un tipo de modelo de IA es bueno para la transparencia en un tratamiento de datos, pero no nos indica el porqué de las decisiones.

Explicabilidad en el RGPD

El RGPD es una referencia a nivel mundial en lo que a protección de datos se refiere. Es especialmente interesante el artículo 22 que regula la toma de decisiones automáticas cuando intervienen datos personales. Este tipo de regulación no es una novedad del reglamento, la Directiva de protección de datos 95/46/EC ya regulaba la toma de decisiones automáticas. Esto puede parecer sorprendente para una directiva cuya propuesta inicial data de 1992, un tiempo en que la tecnología y las posibilidades de recolectar datos sobre las personas eran mucho más limitadas. El RGPD refuerza las limitaciones que imponía la Directiva 95/46/EC respecto la toma de decisiones automáticas y refuerza el control de las personas sobre este tipo de decisiones cuando están permitidas.

Actualmente hay cierta controversia respecto a si el RGPD reconoce el derecho a obtener una explicación de las decisiones automáticas[11] [12]. Aunque no es el objetivo de este trabajo ahondar en el debate, es necesario exponer los hechos.

Cuando habla de los derechos que tienen las personas interesadas respecto las decisiones automáticas, el considerando 71 dice:

"dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión."

Por tanto, en los considerandos se reconoce el derecho a recibir una explicación.

Ahora bien, los considerandos tienen únicamente valor interpretativo y el en la redacción de los artículos el derecho a obtener una explicación no queda fijado.

Por otra parte, cuando se regula el derecho a la información (artículos 13 y 14) y el derecho de acceso (artículo 15), el reglamento exige que se dé información significativa sobre la lógica aplicada. En concreto, exige que la persona responsable facilite información sobre:

"...la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado."

Al final, gran parte del debate sobre la existencia del derecho a obtener una explicación se basa en determinar qué se entiende por "información significativa sobre la lógica aplicada" y hasta qué punto esa información puede constituir una explicación.

Técnicas para explicar un modelo

No es el objetivo de este artículo profundizar en las técnicas que se usan actualmente para dar explicaciones ad-hoc de las decisiones de los sistemas IA que funcionan como una caja negra. Ahora bien, una breve descripción de algunas de ellas puede ser útil para tener entender el tipo de explicaciones que podemos obtener actualmente y sus limitaciones.

Modelo suplente. Es un modelo sencillo que se usa para explicar uno de mayor complejidad. En concreto, es un modelo interpretable (como un árbol de decisión o un modelo lineal) que se entrena con las predicciones de un modelo de caja negra. Como es obvio que un modelo sencillo es más limitado, el modelo suplente acostumbra a modelar solo un área concreta de la caja negra; aquella cercana a la decisión que se quiere explicar. Aún así, no se puede garantizar que no haya discrepancias entre ambos; es decir, no se puede garantizar que la explicación sea correcta.

Importancia de las entradas. Esta técnica busca cuantificar la importancia de cada variable de entrada en la decisión concreta. Es decir, que

11. G. Malgieri y G. Comandé. "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", International Data Privacy Law, 7(4), pp. 243-265, 2017
12. L. Edwards y M. Veale. "Enslaving the Algorithm: From a Right to an Explanation to a Right to Better Decisions?" IEEE Security & Privacy 16(3), pp. 46-54, 2018

peso tiene cada una de las variables concretas de entrada en el resultado obtenido.

Explicaciones contra fácticas. Se busca explicar el funcionamiento del sistema IA dando el mínimo cambio en las variables de entrada que hace que cambie la decisión del sistema. Por ejemplo, en el caso de un algoritmo que ha denegado un crédito bancario sabríamos cuanto tiene que cambiar el sueldo, la edad, etc., para que el crédito fuese concedido.

Cabe destacar que estas son explicaciones locales, parciales y poco fiables. Sirven para que la persona interesada tenga una idea de lo que ha afectado a su decisión concreta, pero distan mucho de lo que se espera para la tercera oleada de IA.

Conclusiones

Este artículo es una breve introducción a la explicabilidad en sistemas IA. Hemos visto como el gran desarrollo de la IA ha puesto en relieve la necesidad de disponer de un IA confiable y que la explicabilidad es un componente esencial de esta IA confiable. También se han analizado diferentes usos de la explicabilidad (justificar, controlar, mejorar y descubrir) y sus limitaciones (pérdida de precisión con el uso de modelos intrínsecamente explicables, e interpretaciones poco precisas o incorrectas en las técnicas para explicar modelos de caja negra).

El objetivo del artículo es transmitir la relevancia que tiene la explicabilidad en conseguir una IA que sea compatible con los valores de la sociedad en la que actúa.

Referencias

B. G. Buchanan y R. O. Duda. "Principles of rule-based systems", Standford University Report STAN-CS-82-926, 1982.

B. Goodman y S. Flaxman. "European Union Regulations on Algorithmic Decision-Making and a Right to Explanation", AI Magazine 37, pp. 50–57, 2017.

DARPA. "Explainable Artificial Intelligence (XAI)", 2017.

D. Brumley. "Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them", IEEE Spectrum, 29 Jan 2019.

D. Crevier. "AI: The Tumultuous Search for Artificial Intelligence", New York, BasicBooks, 2013.

European Comission. "White paper on artificial intelligence - A european approach to excellence and trust", 19 de febrero de 2020, COM (2020) 65 final.

Expert group on liability and new tecnologies. "Liability for artificial intelligence and other emergint digital technologies", 21 de noviembre de 2019.

G. James, D. Witten, T. Hastie y R. Tibshirani. "An Introduction to Statistical Learning", Springer Texts in Statistics.

G. Malgieri y G. Comandé. "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", International Data Privacy Law, 7(4), pp. 243-265, 2017.

Grupo independiente de expertos de alto nivel sobre Inteligencia Artificial. "Directrices para una IA fiable", 8 de abril de 2019.

L. Edwards y M. Veale. "Enslaving the Algorithm: From a Right to an Explanation to a Right to Better Decisions?" IEEE Security & Privacy 16(3), pp. 46-54, 2018.

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.

S. Sankar. "Accuracy and interpretability trade-offs in machine learning applied to safer gambling". In Proceedings of the International Conference on Machine Learning (ICML), 2015, pp. 1–10.

S. Wachter, B. Mittelstadt y L. Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", 7(2), pp. 76–99, 2017.

Estado de la protección de Datos Personales a comienzos de la segunda década del Siglo XXI

Leonardo Cervera Navas[1]

Director de la Oficina del Supervisor Europeo de Protección de Datos (SEPD), la autoridad de protección de datos de la Unión Europea.

Licenciado en Derecho por la Universidad de Málaga y en Derecho Europeo por la Universidad de Granada. Fue profesor en la Universidad Duke de Carolina del Norte (EE.UU.) como parte del Programa Europeo de Becas de la Comisión Europea (US Fellowship Programme). Posee un diploma de postgrado en Gestión de Recursos Humanos en la Universidad de Kingston (Reino Unido). Es miembro de la Academia de Ciencias de Málaga (corresponsal en Bruselas).

Leonardo se incorporó a la Comisión Europea en 1999 y desde entonces ha estado trabajando en el ámbito de la protección de datos en las instituciones de la UE. En 2010 se unió al SEPD como jefe de la Unidad de Recursos Humanos, Presupuesto y Administración y en 2018 fue nombrado Director. Como jefe de la Secretaría, es miembro del Consejo de Administración del SEPD: es responsable de asesorar sobre legislación y política de protección de datos, así como de la coordinación y aplicación de las estrategias y políticas de la institución.

Resumen

El Supervisor Europeo de Protección de Datos ha publicado su estrategia para los próximos cinco años[2] tan sólo unos días después de la publicación del primer informe sobre la aplicación del Reglamento General de Protección de Datos por parte de la Comisión Europea y unos días antes de la sentencia Schrems II que ha invalidado el acuerdo de Privacy Shield entre la Unión Europea y los Estados Unidos.

El presente artículo, escrito durante la pandemia del Covid-19, es pues una reflexión en voz alta sobre el estado de la protección de datos personales a comienzos de la segunda década del siglo XXI tomando como referencia principal el documento estratégico del Supervisor Europeo.

El Supervisor Europeo de Protección de Datos

El derecho a la protección de datos personales está considerado como un derecho fundamental recogido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea [3].

El control por una autoridad independiente constituye un elemento integrante de este derecho fundamental y, en consecuencia, el Supervisor Europeo de Protección de Datos (en adelante "El Supervisor") es la autoridad independiente de supervisión de las instituciones de la Unión Europea, lo cual incluye a las agencias del denominado "tercer pilar" tales como Europol, Eurojust y EPPO (La Oficina del Fiscal Europeo).

Al mismo tiempo, de conformidad con lo previsto en el Reglamento (EU) 2018/1725, que aplica los principios del Reglamento (EU) 2016/679 (en adelante "el RGPD") a las instituciones europeas, el Supervisor actúa como asesor imparcial de la Comisión Europa, el Parlamento Europeo y el Consejo de la Unión en materia de protección de datos, a la vez que como centro de excelencia en el análisis del interfaz entre la tecnología y el derecho desde la perspectiva de su impacto en la privacidad de las personas.

El Supervisor lleva a cabo estas funciones en estrecha colaboración con las demás autoridades de protección de datos de los países miembros de la Unión Europea y con el Comité Europeo de Protección de Datos [4] (en adelante "el Comité"), del cual es a la vez miembro y proveedor de su secretariado.

1. Todas las opiniones vertidas en este artículo son de naturaleza estrictamente personal, sin que puedan considerar en ningún caso, de manera directa o indirecta, como las opiniones del Supervisor Europeo en la materia
2. Dando forma a un futuro digital más seguro: una nueva estrategia para una nueva década
3. Carta de Derechos Fundamentales de la Unión Europea
4. Sitio de la Junta europea de protección de datos

Problemas endémicos agravados por la pandemia

La irrupción de la pandemia de coronavirus y la crisis sanitaria que han traído aparejada, aceleraron la digitalización de nuestra economía y de nuestras sociedades, pero esto no debe hacernos perder de vista que mucho antes de que surgiera el virus nuestras sociedades tecnológicas ya afrontaban una serie de problemas endémicos que no sólo persisten, sino que se han visto amplificados por la pandemia.

A comienzos de la década de los años 20 del siglo XXI, el funcionamiento de Internet sigue anclado en modelos de negocio, que a veces operan en situación cuasi-monopolística, basados en la vigilancia permanente de las personas y la recolección masiva e indiscriminada de datos personales en clara contravención de los principios básicos de la normativa de protección de datos. El modelo publicitario del micro-targeting o muchas de las aplicaciones que centenares de millones de personas llevan instaladas en sus teléfonos móviles, recopilando y compartiendo infinidad de datos personales sin el conocimiento de las personas, son un buen ejemplo de esta situación.

Además de esta realidad preexistente y que nada tiene que ver con la pandemia de Covid-19, el uso de algunas aplicaciones tecnológicas para controlar la expansión del virus como las aplicaciones de rastreo o los controles de temperatura en los lugares públicos, podrían ser la antesala de un uso generalizado de herramientas de seguimiento y control por parte de las autoridades. Algo similar sucedió tras los ataques del 11 de septiembre del año 2001, cuando la irrupción de un fenómeno terrorista sin precedentes justificó la introducción de medidas de vigilancia en principio excepcionales y temporales que, veinte años después, siguen ahí sin visos de que vayan a ser desactivadas.

El mundo en que vivimos

La humanidad se encuentra en los albores de una cuarta revolución industrial que, como ha ocurrido en anteriores revoluciones tecnológicas, transformará nuestro mundo y nuestro modo de vida. La combinación de avances tecnológicos como la computación quántica o la Inteligencia Artificial, es decir, la suma de una mayor capacidad de computación sobre máquinas cada vez más autónomas, tiene un enorme potencial en términos de progreso y bienestar.

De la misma manera que los avances de la tercera revolución industrial, con la generalización de Internet y las tecnologías de la información, ha permitido a una gran parte de la población de los países desarrollados sobrellevar la crisis sanitaria del coronavirus con distanciamiento social y altos niveles de confort, parece razonable pensar que los avances de la cuarta revolución industrial ayudarán también a la humanidad a afrontar los grandes retos a los que se enfrenta en la actualidad que en el caso de la emergencia climática amenazan incluso la propia supervivencia de nuestra especie.

En consecuencia, es fundamental q que como profesionales de la protección de datos mantengamos siempre una actitud positiva y constructiva frente a los avances tecnológicos. Quienes que piensen que ella persona responsable de protección de datos pone las cosas más difíciles a profesionales de ingeniería o a las personas responsables del tratamiento, no habrá entendido bien la finalidad última de nuestra disciplina. Nuestro papel no debe ser nunca obstaculizar el avance tecnológico de una organización sino asesorar y persuadir a quines son responsables del tratamiento de que la protección de la privacidad de las personas no está reñida con otros objetivos y que es perfectamente posible encontrar un justo equilibro, en particular mediante la introducción de la privacidad por diseño y por defecto.

En el mismo sentido, la responsabilidad de las autoridades de protección de datos no puede ser poner reparos a la innovación o el progreso tecnológico sino concienciar a a quienes son responsables públicosde la necesidad de respetar la ley y también de que existan políticas públicas encaminadas a contrarrestar los impactos negativos del cambio tecnológico que son tan predecibles como sus potenciales avances. La protección de datos nació precisamente durante la tercera revolución industrial, para amortiguar el impacto sobre la privacidad de las personas que supuso la irrupción de las computadoras y el Internet, y el RGPD no es otra cosa que la necesaria actualización de esa normativa en los albores de la cuarta revolución industrial.

Los datos personales y los datos en general son la materia prima con la que se alimentan esas máquinas cada vez más autónomas e inteligentes de la cuarta revolución industrial que van a reemplazar a las personas que conducen vehículos, a los recepcionistas o a muchos trabajadores industriales y a personas que trabajan en la industria o el sector servicios. Por tanto, la próxima batalla industrial va a ser la batalla de los datos, y en nuestras sociedades libres y democráticas tendremos que buscar un justo equilibrio entre la competitividad y la sostenibilidad, la innovación y el respeto a la dignidad de las personas, abrazando siempre el progreso y la innovación, pero dejando bien claras cuáles son las líneas rojas que nunca se pueden cruzar.

Hoy, la protección de datos es prácticamente inexistente allí donde existen regímenes totalitarios, pero la mayoría de los países democráticos

del planeta ya cuentan con legislación en materia de protección de datos, algunos todavía con importantes lagunas como es el caso de los Estados Unidos de América. Habida cuenta de que las tecnologías de la información permiten recolectar los datos personales en países con protección para que sean tratados en países sin protección, conceptos como la geolocalización de los datos y soberanía digital están emergiendo con fuerza. La sensación de indefensión experimentada por la ciudadanía durante la pandemia de Covid-19 cuando se ha puesto de manifiesto que la deslocalización de la producción de mascarillas, respiradores y otros materiales esenciales han dificultado la lucha contra el virus, contribuye sin lugar a dudas a amplificar estas tendencias.

Agencias de inteligencia y fuerzas del orden público pueden tener acceso a esos datos personales recolectados por propósitos comerciales y transferidos a países sin protección, lo que acrecienta la preocupación. La anulación por parte del Tribunal de Justicia de la Unión Europea de los acuerdos Safe Harbor y Privacy Shield con los Estados Unidos es un buen ejemplo de esta preocupación que es lógicamente mucho mayor si los datos son accesibles para las autoridades públicas de gobiernos no democráticos. Esto se ha puesto recientemente de manifiesto con las empresas chinas Huawei y Tik-Tok no sólo en la Unión Europea, también en los Estados Unidos y en otros países.

La estrategia del Supervisor

El Supervisor, en su estrategia para los próximos cinco años, trata de dar respuesta a estos desafíos globales desde su responsabilidad como autoridad de control y asesor de las instituciones europeas.

El punto de partida es su configuración como una administración inteligente que pone su conocimiento al servicio de las instituciones de la Unión, destacando un enfoque de prospectiva, siguiendo muy de cerca los desarrollos tecnológicos y tratando de anticipar su impacto sobre la privacidad de las personas.

Un buen ejemplo es el "tech-dispatch" [5] que prepara regularmente la unidad de Tecnología y Privacidad del Supervisor. Las dos publicaciones del año 2020, sobre las aplicaciones de contact-tracing para el control de la pandemia de Covid-19 y sobre la computación cuántica, son muy significativas de la ambición de esta iniciativa.

Otra prioridad del Supervisor y en la misma línea de compartir el conocimiento con las instituciones europeas, es la aprobación de opiniones de gran impacto, a solicitud de otras instituciones o de motu propio, sobre las cuestiones más candentes en materia de protección de datos. Las opiniones adoptadas el mes de junio del 2020 sobre el Papel Blanco de la Comisión Europea sobre la Inteligencia Artificial [6] o sobre la Estrategia Europea sobre los Datos son un buen ejemplo de ello. Conviene mencionar a este respecto, a título orientativo, que otras áreas no estrictamente relacionadas con desarrollos legislativos en materia de protección de datos en las que el Supervisor Europeo se propone centrar sus esfuerzos en los próximos años son el sector E-health, el paquete legislativo del Digital Services Acto,[7] el interfaz entre la protección de datos, la protección de quienes consumen y el derecho de la competencia, tanto a través de la plataforma del Digital Clearing House [8] como en el marco del Comité Europeo, por ejemplo en relación al análisis de la reciente adquisición de Fitbit por Google [9] en la que el Supervisor ha participado muy activamente.

En lo que se refiere a la actividad del Supervisor como autoridad de control, la próxima creación de un módulo básico de formación en línea sobre protección de datos para cada persona que recién llega a la administración europea es un buen ejemplo de la ambición de fomentar una fuerte cultura de protección de datos a todos los niveles. Igualmente, las acciones en marcha para asegurar que los contratos que suscriben las administraciones europeas con los proveedores de servicios tecnológicos, en su mayor parte estadounidenses, cumplen con la normativa europea de protección de datos son un buen indicador del enfoque práctico del Supervisor. Un ejemplo de lo anterior es el denominado "Foro de la Haya"[10], una plataforma informal promovido por nuestra pequeña institución en la que se intercambian buenas prácticas y se coordinan acciones para mejorar la capacidad de negociación de las administraciones europeas y nacionales con los grandes proveedores de servicios digitales.

En clave más regional, además de la labor de supervisión y asesoramiento en materia de cooperación policial y judicial entre los Estados Miembros, una prioridad del Supervisor para los próximos años es contribuir en el seno del Comité Europeo a un enforcement transfronterizo

5. TechDispatch" en el sitio del Supervisor europeo de protección de datos
6. Dictamen del SEPD sobre el Libro Blanco de la Comisión Europea sobre inteligencia artificial: un enfoque europeo hacia la excelencia y la confianza en el sitio del Supervisor europeo de protección de datos
7. El paquete de la Ley de servicios digitales en el sitio de la Comisión europea
8. Big Data y cámara de compensación digital
9. Declaración sobre las implicaciones para la privacidad de las fusiones.
10. Statement on privacy implications of mergers

más eficiente del RGPD, facilitando investigaciones conjuntas y proponiendo la creación de un Support Pool of Experts que asista a las autoridades nacionales de control en casos particularmente difíciles o gravosos desde la perspectiva de los recursos disponibles. El enforcement del RGPD ha sido construido sobre el principio de la proximidad con la persona interesada que puede acudir así a su autoridad local y comunicarse con ella en su propio idioma, pero esto plantea algunas dificultades para la cooperación transfronteriza, en particular por las diferencias que existen en el derecho administrativo y en las leyes procesales en los Estados Miembros de la Unión Europea.

Reflexiones finales

La década de los años 20 del siglo XXI presenta algunas similitudes con los denominados "locos años 20" del siglo XX, que también comenzaron con la irrupción de otra pandemia, la denominada "gripe española" y terminaron con la gran depresión del año 1929 y la irrupción de los totalitarismos.

En nuestros "locos años 20 del siglo XXI", los movimientos populistas y nacionalistas que se aprovechan del descontento creciente de las clases medias constituyen una seria amenaza a las conquistas de progreso y derechos humanos logradas con gran sacrificio de nuestros padres y abuelos. Para comprobar la fragilidad de nuestras democracias y del estado de derecho basta con asomarse cada día a las redes sociales y ser testigos de la creciente desinformación y radicalidad de sus participantes. Esto no es solo el resultado de la acción irresponsable de dirigentes políticos instalados en la mentira y la manipulación sino también de algoritmos desarrollados con motivaciones mercantiles que premian la máxima difusión y el ingreso publicitario sobre la veracidad de la información. Sólo muy recientemente se están observando algunos intentos de corregir esta situación cuyas consecuencias en términos de polarización de nuestra sociedad son tremendamente dañinas.

La crisis económica provocada por la crisis sanitaria del Covid-19 se cebará con los más débiles y vulnerables de nuestra sociedad y la respuesta no puede ser el "sálvese quien pueda" o "nosotros primero" sino la unión y la solidaridad como se ha puesto de manifiesto recientemente en el acuerdo histórico alcanzado por los líderes de la Unión Europa [11] para hacer frente a las consecuencias económicas del coronavirus. No tendremos una vacuna que pueda protegernos contra la emergencia medioambiental motivada por el cambio climático, que amenaza la supervivencia misma de nuestra especie, y la única solución para este problema de índole planetario pasa por la cooperación internacional de dirigentes políticos que guíen sus pasos con altura de miras y responsabilidad trans-generacional.

Corresponde a la ciudadanía exigir a las autoridades públicas que estén a la altura de las circunstancias frente a estos retos planetarios trascendentales, también en lo que se refiere a las nuevas tecnologías y a la protección de la privacidad de las personas. Afortunadamente, la protección de datos ha dejado de ser una preocupación netamente europea y la región iberoamericana es un buen ejemplo de ello. Iniciativas como la Red Iberoamericana de Protección de Datos que ha recibido un impulso considerable gracias el liderazgo de su presidente Felipe Rotondo y de la secretaría permanente de la Agencia Española de Protección de Datos, son un instrumento muy útil para hacer realidad esta visión compartida.

El RGPD ha recibido muchos elogios desde su aprobación hace ya más de cuatro años, pero en realidad es sólo la punta del iceberg de una visión europea, que afortunadamente comparten en lo esencial otras regiones del planeta que abrazan también los principios democráticos y el imperio de la ley, de que la dignidad del ser humano es inviolable y, por tanto, incompatible con una tecnología que sirva únicamente o principalmente al beneficio empresarial. La tecnología debe amoldarse al ser humano y no al revés y los poderes públicos tienen la responsabilidad de regular, cuando no prohibir directamente, un uso de la tecnología claramente dañino para la dignidad de las personas. En este sentido, el Supervisor pide en su estrategia para los próximos cinco años una moratoria del uso de las tecnologías de reconocimiento facial en espacios públicos.

En definitiva, el reto para los próximos años es sentar las bases de una tecnología más sostenible y respetuosa con las personas a medio y a largo plazo pues a medida que nuestra existencia se haga más digital, más importante será que los derechos y libertades que ya disfrutamos en el mundo off-line se hagan también una realidad palpable en el mundo on-line. No hay vuelta atrás en este camino.

11. "Líderes de la Unión Europea logran un acuerdo «histórico» de US$ 2 billones para reconstruir la economía del bloque" en el sitio de CNN

A glass half full look at de brasilian data protection authority

Leonardo Parentoni

PhD in Corporate Law at USP. Master of Laws at UFMG. Member of Attorney General's Office (Advocacia-Geral da União/ AGU).

Researcher and Tenured Law Professor at UFMG and Full Professor at The Brazilian Institute for Capital Markets - IBMEC/ MG. Founder and Coordinator of the research area on Law, Technology and Innovation at UFMG Law School PhD Program. Founder and Scientific Advisor to the Research Center on Law, Technology and Innovation - DTIBR (www.dtibr.com). Former Research Fellow at the University of Texas in Austin and Visiting Professor at the Uruguay Data Protection Authority. Key Technology Partner (KTP Program) at the University of Technology Sydney. Team Mentor in Law Without Walls - LWOW. Publications available for download.

SUMMARY

ABSTRACT

Purpose: In any data protection system, the regulatory institution - called the National Data Protection Authority - plays a substantial role. In Brazil, this institution was created in a different way from what had originally been expected. Therefore, the legal literature started to criticize it and to doubt its ability to satisfactorily exercise its regulatory powers. Even before the Brazilian general data protection act came into effect, a major opinion was formed around the idea that, in its current structure, the Brazilian Data Protection Authority (BDPA) would fail. The author of this paper intends to provide a different view on the subject. Amid the uncertainty, he opted for looking at the glass "half full" instead of seeing it "half-empty". He highlights that even in its current format the BDPA is remarkable progress and could be very useful to the Brazilian personal data protection system.

Method: To provide this text with a scientific basis, the author conducted a structuralist analysis drawing a comparison between the Brazilian Data Protection Authority and the equivalent institution in Uruguay (URCDP), which has a very similar structure and has been carrying out its duties with success for over a decade. After all, more important than the structure of the regulatory body are its capacities and how they will be exercised in practice.

Results: In the end it was possible to demonstrate that the initial structure of the BDPA is not a barrier that could prevent it from carrying on its duties. Therefore, it is prudent to trust the BDPA and monitor how it will operate.

Contributions: As far as the Author knows, this is the first paper in Brazil drawing a structuralist comparative analysis between the Brazilian and Uruguayan data protection bodies.

Keywords: Privacy; Personal Data Protection; Brazilian Data Protection Authority - BDPA; Uruguay Data Protection Authority - URCDP.

Observando a Autoridade Nacional de Proteção de Dados brasileira na perspectiva do copo "meio cheio".

RESUMO

Objetivo: Em qualquer sistema de proteção de dados pessoais, a instituição reguladora - em vários países denominada Autoridade Nacional de Proteção de Dados (ANPD) - desempenha papel destacado. No Brasil, esta instituição foi criada de forma diferente do previsto. Por isso, a literatura especializada passou a criticá-la e a duvidar de sua aptidão para exercer satisfatoriamente o papel de órgão regulador. Antes mesmo da entrada em vigor da lei geral de proteção de dados pessoais, formou-se opinião majoritária de que, no formato atual, a ANPD iria fracassar. O autor deste texto procurou fornecer uma perspectiva diferente sobre o tema. Diante da incerteza, optou-se por enxergar o copo "meio cheio"

ao invés de "meio vazio". Ou seja, considera-se que mesmo no atual formato a ANPD é sim um grande avanço e pode ser muito útil ao sistema brasileiro de proteção de dados. Afinal, mais importante do que a estrutura são as funções do órgão regulador e como elas serão exercidas na prática.

Metodologia: Para embasar cientificamente o texto, realizou-se uma análise estruturalista comparando a ANPD brasileira com a instituição equivalente do Uruguai (URCDP), que tem formato semelhante e vem atuando com sucesso há mais de uma década.

Resultados: Ao final, foi possível demonstrar que a estrutura inicial da ANPD não é, por si só, um óbice intransponível ao bom exercício de suas funções. É preciso dar um voto de confiança à ANPD e monitorar como ela irá de fato desempenhar as suas atribuições.

Contribuições: Até onde se sabe, este é o primeiro artigo científico do Brasil que realizou uma análise estruturalista comparada entre as autoridades de proteção de dados do Brasil e do Uruguai.

Palavras-chave: Privacidade; Proteção de Dados Pessoais; Autoridade Nacional de Proteção de Dados (ANPD); Autoridade Uruguaia de Proteção de Dados (URCDP).

1. INTRODUCTION: THE BDPA AND ITS MISSION

In every personal data protection system, there must be an institution responsible for its regulation which plays a major role. In some countries, this institution accumulates the protection of personal data with other assignments, eventually very different ones. This is the case for the Federal Trade Commission - FTC in the United States of America, whose main mission is to "protect consumers and competition"[1], but also to protect personal data (privacy)[2] On the other hand, there are countries in which a public institution is specifically in charge of protecting personal data. That is what happens in the member's states of the European Union since its Charter of Fundamental Rights (CFREU Section 8, 3) considers as mandatory the existence of an independent authority for this purpose in each country, as well as a European agency for harmonizing this theme inside the Union [3].

In the Brazilian legal tradition, personal data protection has been sparsely addressed in various laws, from the Brazilian Telecommunications Code of the 60s and its decree to more recent laws such as the Brazilian Consumer Defense Code (CDC) and the "Positive Credit Reporting Act". In this context, the institution responsible for overseeing market compliance with each of these laws also acted partially in the mission of protecting personal data. But there was no authority in place exclusively focused on this subject.

The legal landscape has deeply changed with the advent of Law nº 13709/2018 - Brazilian General Data Protection Law (BGDPL), which having been strongly influenced by the European model (General Data Protection Regulation - GDPR)[4] has created the Brazilian Data Protection Authority (BDPA)[5] , a public institution dedicated specifically to "ensure the protection of personal data in accordance with the law" (Law Section 55-J, I). In other words, Brazil has finally come to own a central regulatory institution such as the European model[6] .

It turns out that there is a lot of suspicion regarding the potential of the BDPA to effectively act in a technical, impartial and efficient manner.

2. BRIEF LEGISLATIVE HISTORY OF THE BDPA

The original House of Representatives Bill nº 4060/2012, which would later become the BGDPL, did not foresee the creation of the BDPA. It was first outlined in the Executive Bill nº 5276/2016 (Section 53), as an administrative body. As such, it was not a legal entity nor had its budget or personnel. However, still during the legislative process, a parliamentary amendment proposed to change its format to a regulatory agency by the terms of Section 55 of Bill nº 53/2018, a movement encouraged by the opinion of legal experts, according to whom this new structure would be

1. THE UNITES STATES OF AMERICA - FEDERAL TRADE COMMISSION: 2019/a; p. 01.
2. An aspect reinforced by the fact that in July 2019, the FTC applied to Facebook the largest fine in history, amounting to USD 5 billion for violating previous recommendations of FTC itself, dating back to 2012, regarding measures that should have been adopted by Facebook for greater protection of US users personal data of. (THE UNITES STATES OF AMERICA - FEDERAL TRADE COMMISSION: 2019/b; p. 01).
3. For a detailed study on the similarities and cultural differences between the US and the EU in terms of personal data protection, see the text by James Whitman: (WHITMAN: 2004).
4. The justification of the Law nº 4060/2012 did not explicitly mention the GDPR's influence. However, such aspect has become clear in later bills such as Law nº 5276/2016, which stated that: "the debate on privacy and personal data dealt with in this Preliminary Draft Bill was also heavily influenced by the international context." (BRAZIL - CÂMARA DOS DEPUTADOS: 2016).
5. The troubled legislative history that culminated on the creation of the BDPA will be addressed in the next section
6. Even though there are substantial differences between the format of the BDPA and its European counterpart, this aspect goes beyond the purpose of this study

the only one able to provide the authority with the independence to perform its regulatory duties, mirroring similar international organizations[7]. However, due to this new structure the creation of the authority was vetoed by the President based on two grounds: 1) a parliamentary amendment could not lead to an increase in expenses for bills proposed by the Executive[8] and 2) Brazilian laws forbid the proposal of bills that could increase current expenditures during the last few months of a presidential term[9]. The conjuncture of a severe economic crisis in the country (demanding great efforts to contain public spending and reduce staff) has significantly contributed to the veto. As a consequence of this veto, the BGDPL finally published on August 14, 2018, did not foresee the creation of the BDPA.

To fill that gap, on December 27, 2018, the Executive itself has handled the presentation of the Provisional Measure nº 869/2018, which had as one of its core aspects the creation of the BDPA, structured as an administrative body, without increasing expenses (Section 55-A), in the same way as it was originally outlined in 2016. Once again, an intense debate over this structure took place. Many voices highlighted its possible shortcomings, especially the lack of independence when exercising regulatory duties against the State itself. Shortly after, on July 18, 2019, Law nº 13844/2019 (Section 2: VI and Section 12) has formally inserted the BDPA into the structure of the Presidency as an administrative body. This structure was finally consolidated on July 8, 2019, when the Provisional Measure nº 869/2018 was converted into Law nº 13853/2019, keeping the BDPA as an administrative body inside the structure of the Presidency, in accordance with the previous provisions.

This brief history demonstrates that the creation of the BDPA was one of or the most - if not the most - sinuous aspects of the legislative process that gave rise to the BGDPL. Besides those many legislative turnarounds, the structure of the BDPA was also subject to an intense discussion, on both public and private forums, as to which structure it should have. In the end, the Executive's position to create the authority as an administrative body inside the structure of the Presidency without incurring in additional costs has prevailed. The government is fully aware that this structure is not the ideal model but the only one possible in the current context of the country. So much so that BGDPL itself (Section 55-A, 1st and 2nd Paragraphs) recognize this structure as transient, providing that it should be re-evaluated after two years for a possible conversion into a legal personhood in the form of an authentic regulatory agency with its budget and personnel.

3. CRITICISM ABOUT THE CURRENT STRUCTURE OF THE BDPA

The choice of structuring the BDPA as an administrative body instead of a special regime autarchy (an agency) was subjected to intense criticism from both the legal community and the press[10]. Some of this criticism are listed below. Even though the author does not agree with all of them, he considers it important to describe these arguments as a basis for the antithesis built in the following topics.

The first criticism is that the BDPA was not structured as a regulatory agency. This aspect is reinforced by the fact that the BDPA is not included in the 2nd Section of Law nº 13848/2019, which lists some of the main regulatory entities operating in the country [11]. As a result, the "European model" that inspired the BGDPL was left aside [12]. Moreover, the rules of Law nº 13848/2019 on interaction with other regulatory agencies and public bodies do not apply to the BDPA. These rules could be of paramount importance in complementing the few dispositions of the BGDPL around this subject, helping to solve potential conflicts of attribution.

The second criticism is related to the first. Had it been structured as an autarchy, the BDPA would have a "decentralized administrative and financial management" according to the Decree-Law nº 200/1967, Section 5, I. However, being structured as an administrative body resulted in the lack of a budget of its own, remaining basically linked to - and dependent of - the general budget of the Presidency. Especially because the other sources of income provided for the BDPA on Section 55 of the BGDPL tend to be insufficient. This could jeopardize its financial autonomy. This aspect is aggravated by the fact that the BDPA also may not collect fees for services rendered such as the approval of binding corporate rules and other documents.

A third criticism says that the current structure of the BDPA makes it harder to organize its staff with specialized personnel. After all, to achieve

7. (DONEDA: 2006; p. 385-386): "The use of an administrative authority for the protection of personal data, in the model of an independent authority, is a trend strongly rooted in some legal systems. After its conception and adoption in countries such as Germany and Sweden, its creation was deemed mandatory to all countries members of the European Union (...) turning it into a core feature of the so-called 'European model' of personal data protection. It is not, however, a phenomenon restricted to the geographical and political European spaces, since similar organizations can be found in countries such as Argentina, Australia, Canada, Japan, Israel, Hong Kong, New Zealand and Taiwan

8. BRAZIL - PRESIDÊNCIA DA REPÚBLICA: 2018

9. For example, Section 42 of the Brazilian Law of Fiscal Responsibility (Supplementary Law nº 101/2000) and Section 359-C of the Brazilian Criminal Code (Decree-Law nº 2848/1940).

10. Summarizing these arguments: (BIONI: 2019).

11. Nor was it structured as a regulatory agency in the BGDPL, what could make applicable the provision of the 2nd Section, Sole Paragraph, of Law nº 13848/2019: "Except from what is envisaged in the specific legislation, the provisions of this law should be applied to special autarchies characterized in terms of such law as regulatory agencies and created from its effective date."

12. (SOPRANA: 2018; p. 01): "Provisional Measure 869 founds an administrative body connected to the Presidency of the Republic and not an independent authority as provided in the original bill. (...) Representatives of the Academy and civil society involved in the debate also criticized the BDPA's connection to the Executive." See also Section 52 of the GDPR.

greater specialization it would be advisable to create a career of its own, made up of members selected through a specific public tender that would test knowledge in the field of personal data protection. However, this is definitely not going to happen since the staff of the BDPA will be composed of public employees from other fields, already admitted into the administration, in addition to those appointed to positions of trust.

The fourth criticism concerns the BDPA's possible lack of technical autonomy, because its directors could suffer all sorts of political pressure, especially when the authority has to exercise its regulatory duties against the government itself [13].

Even if all this criticism is overcome and the current structure of the BDPA is eventually considered acceptable, one more question remains: where to allocate it?

Some scholars suggested[14] placing this new administrative body within the Ministry of Justice, similar to what has been done to CADE (The Brazilian Administrative Council for Economic Defense) during its first years. However, the choice to allocate it within the Presidency of Republic prevailed.

All this criticism led to the conclusion that in its current structure the BDPA would lack the independence to satisfactorily perform its regulatory duties, especially to supervise the government itself [15].

Some of these arguments are not technically grounded, while others have been overcome by changes that occurred during the legislative process of converting the Provisional Measure nº 869/2018 into law. Furthermore, even the pertinent criticism does not mean that the BDPA is doomed to fail. After all, just as important as its structure - if not far more important - is how it will exercise its regulatory powers [16].

4. WHY THE COMPARISON WITH URUGUAY?

It is notorious that Brazil and Uruguay are countries substantially different in many aspects: territorial extent, number of inhabitants, gross domestic product, climate, vegetation, official language, etc. [17]. So what would be the reason for comparing them? The answer is that the Uruguayan Data Protection Authority (URCDP) has a structure very similar to the Brazilian one. Moreover, the Uruguayan URCDP has been very successful in carrying out its regulatory duties. Thus, it is possible to learn from the Uruguayan experience and extract useful insights for Brazil.

First, Uruguay already has in place a specific law addressing personal data protection since 2004 (Ley nº 17838/2004) [18]. And since 2008 it has adopted a General Law on the subject (Ley nº 18331/2008)[19]. Therefore, Uruguay has regulated personal data protection with specific laws more than a decade before Brazil.

Secondly, Uruguay has obtained adequacy decision[20] from the European Union in August 2012, after proving that the country provides an adequate level of protection for data transfers in its legislative system similar to those prevailing in Europe until Directive 95/46/CE. As much as having the URCDP as an independent authority [21].

---

13. (VALENTE: 2019; p. 01): "The Secretary of State for Consumer Defense of the Ministry of Justice, Luciano Benetti Timm, has expressed his concerns about the risks of capture of the agency."
14. (VENTURA: 2019; p. 03): "Another point that has resulted in discussions and controversies was about which part of the government would host the BDPA. Officially the Ministry of Justice has manifested interest in encompassing the authority, arguing that among other reasons that Ministry has the successful experience of CADE, the Administrative Council of Economic Defense, which has emerged in the MJ and today is completely independent
15. (PSCHEIDT: 2019; p. 02): "The agency suffers direct political and partisan influence because it is connected and committed to government and political party plans. (...) With the creation of a 'simple' agency, the Executive will have full regulatory control, which will establish guidelines on Data Protection according to the governmental plan. It will reduce some frictions but also will make any future regulation even more politically affected, which raises great concern.
16. (BOBBIO: 2007; p. 112): "[functional analysis] here understood as a general theory that seeks the characterization of element of law not in the specificity of the structure, as had occurred so far by some of the greatest theoretical scholars, but in the specificity of the function (...)."
17. For detailed statistics regarding Uruguay, it is recommended the reading of: (URUGUAY - INSTITUTO NACIONAL DE ESTADÍSTICA: 2019).
18. "Artículo 1º.- El presente Título tiene por objeto regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos, u otros medios similares autorizados, sean éstos públicos o privados, destinados a brindar informes objetivos de carácter comercial."
19. " Artículo 3. Ámbito objetivo. El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.
20. (TIKKINEN-PIRI; ROHUNEN; MARKKULA: 2018; p. 145): "The GDPR builds on DIR95 regarding the European Commission's possibility to make an adequacy decision about the level of data protection of a third country (or a territory or a processing sector in that country) or an international organization. To make the decision, the commission has to assess the level of protection regarding the rule of law, the independent supervisory authority and the international commitments entered into by the third country or the international organization. (...) If an adequacy decision has been made, a transfer may take place, and any further authorization to transfer is not required from the supervisory authority." Along the same lines: (SARMENTO E CASTRO: 2005; p. 281).
21. (THE EUROPEAN UNION - COMISSÃO EUROPEIA: 2012): "Section 1. For the purposes of Section 25, no. 2, of Directive 95/46/CE, it is considered that the Eastern Republic of Uruguay ensures an adequate level of protection for personal data transferred from the European Union." See also recital 10

In other words, while Brazil is still working to harmonize with the European model[22] Uruguay has already obtained official recognition in this regard. It is also worth mentioning that Uruguay was the first non-European country to accede to Treaty nº 108/1981[23] of the Council of Europe, in August 2013[24].

Uruguay is still the only South American State member of the Digital 9, a select group of 9 countries that call themselves "the world's most advanced digital nations" [25]. It was even chosen to host this group's annual meeting in 2019.

Finally, in 2019 a national survey noted that 92% of interviewees had access to the internet, as well as 100% of requirements to the Federal Administration can be initiated online, while 70% of them can be fully processed and solved in this manner. Even more surprising is the result that 53% of the population has affirmed to be completely aware of their data protection rights[26].

Those numbers illustrate the expressive results Uruguay has been reaping by investing in digital development. All of it, plus the fact that its national authority is structured similarly to the BDPA, justifies the comparative analysis hereby conducted.

5. DRAWING A COMPARISON BETWEEN THE URUGUAYAN URCDP AND THE BRAZILIAN BDPA

It is worth mentioning that the author does not mean to draw a complete analysis of comparative law. Instead, the aim is just narrow down the scope of this research to a structuralist analysis intending to spot common institutional guarantees [27] of the data protection authorities in Brazil and Uruguay. This kind of investigation is more qualitative than quantitative and can clarify what to expect from the Brazilian authority when it effectively starts to operate[28].

The Uruguayan data protection authority is called Unidad Reguladora y de Control de Datos Personales (URCDP), which can be translated to the Unity of Regulation and Control of Personal Data. It is worth noting that the name does not even mention the term "authority" traditionally used in the European model.

Operating for over a decade, the URCDP has already achieved significant results [29]. Some information about its accomplishments are listed below.

Dozens of events to make people aware of their data protection rights have been put in place, involving varied audiences such as children, high school teachers, employees that work directly with personal data, public officers, and the elderly. Moreover, more than 1,800 consultations were answered in 2017 alone, of which 642 had been made in person, 692 by telephone, and 540 by e-mail. Online courses were offered on the website of the URCDP, as well as academic events hosting national and international specialists, such as "charlas de café" (monthly meetings in which this author had the opportunity to participate in 2019). Regarding the regulatory activities 122 resolutions were issued in 2017 to implement legal provisions. Internationally the URCDP has participated in meetings of the Ibero-American Data Protection Network, of the Inter-American Legal Committee of the Organization of American States (OAS), of the International Association of Privacy Professionals (IAPP) and of the Advisory Committee of Treaty nº 108/1981 of the Council of Europe. Regarding the number of databases, from a total of 9000 databases registered until 2017 more than 150 were effectively audited that year alone, 30 of which were public, 13 controlled by individuals, 107 controlled by legal entities, and 1 controlled by a parastatal organization. From 2009 to 2017, more than 20 codes of conduct were reviewed and approved. Finally, regarding the sanctions in 2017 8 warnings and 17 fines were imposed.

After properly highlighting the positive numbers of the URCDP it is time to demonstrate how its structure and function are similar to the Brazilian authority.

22. The European model of data protection works in fact as the standard model adopted by many countries (de facto standard). Some exceptions to this model are the United States, China and Russia. (LYNSKEY: 2015; p. 41): "Data protection is one of the rare fields in which the EU could be said to exercise global regulatory supremacy; the EU rules have now been used as a blueprint for regulatory regimes across the Western world.
23. The Council of Europe is an international organization that promotes human rights including personal data protection: (COUNCIL OF EUROPE - COOPERAÇÃO INTERNACIONAL: 2019). It was responsible for the creation of Treaty 108 in January 1981, the very first international treaty about personal data protection that was open to accession by interested countries, whether European or not. For further information, see: (TENE: 2013; p. 1221).
24. COUNCIL OF EUROPE - CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA: 1981).
25. DIGITAL 9: 2019.
26. URUGUAY - AGENCIA PARA EL DESARROLLO DEL GOBIERNO DE GESTIÓN ELECTRÓNICA Y LA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO: 2019.
27. (MENDES: 2019; p. 142): "(...) institutional guarantees represent those juridical institutions created by and dependent on the legal framework."
28. (HOPT: 2009; p. 10): "Try to see what is useful for your own continent and for your country. This is the essence of Comparative Law: learning from others' mistakes and good experiences."
29. (URUGUAY - UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES: 2019/a).

The URCDP was created by the Uruguayan General Data Protection Law[30] in 2008, as an administrative body inside the structure of the Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), a governmental agency in charge of coordinating actions for the development of the "e-Government" in Uruguay [31], according to Section 72 of Law nº 17930/2005. Hence, the URCDP is structured as an administrative body such as the Brazilian authority.

Its internal structure comprehends a Board of Directors composed of 3 members. Therefore, even smaller than the equivalent structure of the BDPA, which has 5 Directors, according to Section 55-D, caput, of the BGDPL. Members of the Board of Directors at RCDP have a fixed mandate of 4 years admitting re-election. The same period is foreseen for directors of the BDPA as provided in Section 55-D, Third Paragraph of the BGDPL.

In addition, members of the Board of Directors at URCDP may only be compulsorily removed from their positions at the end of the mandate or by decision of the Executive, in case of ineptitude, omission or practice of illicit act, always respecting the due process of law. On that topic, the BDPA provides even more guarantees, since the definitive removal of its Directors may only occur based on "a final court decision or a dismissal decided in an administrative process" under Section 55-E, caput, of the BGDPL. Last but not least, the BDPA has an additional safeguard: the preventive removal of a Director can only be imposed by the President of the Republic himself/herself after the recommendation of a special committee, as stated in Section 55-E, 2nd Paragraph of the BGDPL. In other words, only the highest authority of the Executive can remove the Directors before a definitive administrative decision or a final judicial decision.

To continue, both URCDP and BDPA have technical and operative autonomy to exercise their regulatory powers, an aspect provided by law clearly and unambiguously (in Brazil according to Section 55-B, caput, of the BGDPL). It is well-known that there are laws that become repeatedly unobserved even though they are in force ("non-binding laws") [32]. However, it cannot be presumed that the technical and operative autonomy of the BDPA will suffer that sad end. On the contrary, the very purpose of law itself as a regulatory system for life in society mandates to presume that the law will be respected. Especially at the current moment, when the BDPA has not even started to operate, and therefore it is not yet possible to evaluate the technicality and impartiality of its decisions.

The attributions of the URCDP are also very similar to those of the Brazilian authority. For example, to develop guidelines, to consider petitions of data subjects, to conduct studies and educate the population, to regulate, to supervise and possibly to impose sanctions[33] .

To conclude it is worth mentioning that the author of this paper has visited the URCDP in 2019, as a guest researcher, when he heard in person one of the "mantras" of this regulatory body repeated by both late and current directors which is the fact that there has never been any political interference in their decisions. Amid the uncertainty, it seems better to look at the glass "half full" instead of seeing it "half-empty". Therefore, instead of disbelieving the BDPA ab initio why not believe - and surveil for - that it indeed fulfills its capacities? After all, in law good faith is presumed, and bad faith must be evidenced.

6. BDPA'S ADDITIONAL GUARANTEES AND SOME QUESTIONS STILL LEFT OPEN

Besides all the aspects already mentioned in the previous section the BGDPL provides other guarantees to the BDPA, to equip it with enough instruments to perform its regulatory duties. Much of these guarantees were inserted during the legislative process of conversion of Provisional Measure nº 869/2018 into Law nº 13853/2019. Therefore, they are subsequent to some of the criticism already mentioned and they were included in law precisely in response to these criticisms, to minimize the risks that had been identified.

Firstly, the role of the BDPA and its capacities was one of the most amended parts during the legislative process. While in Section 53 of Executive Bill nº 5276/2016 (the first to propose the creation of the BDPA) there were only 13 capacities for that authority, in the conversion to Law nº

30. Ley n. 18.331/2008. Art. 31. "CAPITULO VII - ORGANO DE CONTROL. Artículo 31. Órgano de Control. - Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos. A excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso. Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico."

31. For further reading on the Uruguayan initiative of an electronic government (e-government), see: (BRUNET: 2015).

32. (RIPERT: 2002; p. 268): "The constant violation of law gets men used to consider that what is not respected is not respectable. Legal provisions fall into disuse or survive only at the expense of successive amendments. But by being constantly amended, it cannot acquire the prestige that turn institutions into long traditions. It is no longer respected by default. Moreover, the change of rules is many times expected. What was illegal yesterday becomes lawful a few months later."

33. For a detailed analysis of the URCDP's assignments and how they have been carried out since its creation, see: (URUGUAY - UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES: 2019/b; p. 97): "La URCDP ha desarrollado desde sus inicios una gestión enfocada en el cumplimiento de metas anuales - y en ocasiones quinquenales - asociadas a proyectos específicos vinculados a la promoción, difusión y evolución del derecho a la protección de datos personales."

13853/2019 these capacities were expanded up to 29 (BGDPL Section 55-J). In other words, its list of powers was more than doubled.

Another important amendment was the introduction of Section 55-D, 2nd Paragraph of the BGDPL, demanding that the nominees for the Board of Directors of the BDPA should be previously approved by the Senate ("sabatina" in Portuguese). A process stricter than, for example, the appointment of Ministers of State. Subsequently, 2nd Paragraph of the same Section reinforces the technical profile of the Directors by providing that only "Brazilians who have an unblemished reputation, higher level of education and high concept in the field of specialty" may be nominated to that position. And yet, it also imposes on former Directors a period of "quarantine" of 6 months without engaging in any activities related to personal data protection after they leave the board, to prevent possible conflicts of interest (BGDPL, Section 55-F).

Therefore, in the author's view there are enough guarantees in the BGDPL for the BDPA to perform its duties as an independent authority [34]. As a consequence, this authority and its members should get a vote of confidence. Other public bodies were initially structured similarly or even in a less protective manner than the BDPA and today are quite respected, such as the Administrative Council for Economic Defense - CADE[35] . So, it should only be expected that the BDPA can also follow the same path.

Heading out to the end of this text, it is worrisome that other issues, perhaps even more relevant than the structure of the BDPA, have not yet been treated as hot topics in the debate. One of them stands out: the potential conflict of attributions between the BDPA and other public bodies and entities ruled by ordinary law[36].

On the one hand, the BGDPL categorically states that the power to interpret its provisions and eventually impose sanctions belongs exclusively to the BDPA (Section 52, caput, Section 55-J, XX), emphasizing that "this power shall prevail over correlated competences of other public administration entities or administrative bodies in matters of personal data protection" (Section 55-K, caput). On the other hand, the same BGDPL encourages the BDPA to perform its regulatory duties "in accordance with other administrative bodies and entities with powers to sanction and regulate matters related to personal data protection" (Section 55-J, XXIII and Section 55-K, sole Paragraph). After all, under what circumstances will the BDPA have the final word on a particular issue if a consensus is not reached?

This question is much more complex than it seems at first sight. It is wrong to simply assume that the BDPA position will always prevail. Indeed, the interaction between regulatory bodies is partially disciplined in Law nº 13848/2019 and long before that, it had already been subject of intense administrative struggle, which was later converted into the judicial matter well-known as case BACEN (Brazil's Central Bank). CADE (Administrative Council for Economic Defense)[37] . That case discussed which of these public agencies would have the final word in analyzing the lawfulness of a merge involving financial institutions. The opinion of the Federal Attorney General, later confirmed by the Superior Court of Justice, stated that the principle of specialty must be applied. Therefore, BACEN had the final word in deciding whether the merger was lawful as it is a more specialized institution in the National Financial System than CADE, which analyzes the competition as a whole, encompassing a variety of economic sectors and players.

Following this reasoning, in the context of personal data protection, one can imagine that in case of a conflict between the BDPA and sectoral regulatory agencies, decisions of the latter will prevail. And this is not just hypothetical or far from reality. On the contrary, in the case of cloud banking [38], for example, a linear application of what was ruled would lead to the conclusion that the final decision would be BACEN's instead of the BDPA's. The issue involves deepening insights and important distinctions that could affect the conclusion, but it is not the case of addressing them here for the sake of brevity.

Another issue of paramount importance and that still lacks proper studies is the relationship between the BGDPL and other laws that sparsely address personal data protection, such as the Consumer Protection Code and the Brazilian Civil Framework of the Internet [39].

---

34. Considering as independence the sum of four factors highlighted by specialized literature: (MOREIRA NETO: 2003; p. 165): "The independence necessary to ensure that the exercise of regulatory powers is politically neutral should be understood as a content strict related to four aspects: technical, normative and managerial, budgetary and financial independence of managers."

35. Recalling that the CADE was created in 1962 by Law nº 4173/1962 as an administrative body inside the Ministry of Justice, being transformed into an autarchy (agency) only in 1994 by Law nº 8884/1994, which was latter repealed by Law nº 12529/2011, currently in effect.

36. This kind of conflict does not pose a problem in case one of the institutions involved is provided for in the Constitution itself, since the constitutional rules must prevail. The same cannot be said about institutions provided for only in regular laws. See: (BOBBIO: 1999)

37. See also: STJ, 1st Section, Special Appeal no 1.094.218/DF, j. 25.08.2010, Rel. Ministra Eliana Calmon.

38. In short, cloud banking is the transference of personal data controlled by financial institutions from their traditional data processing and storage centers, where each institution is responsible for its own center, to a cloud storage service run by third parties. This subject is currently regulated by BACEN Resolution nº 4658/2018.

39. On this topic, see the paper written by this author in January 2019, which, as far as it's known, was one of the first - if not the first Brazilian author - to address this subject: (PARENTONI: 2020).

7. FINAL REMARKS

It is indisputable that the BDPA does not have the ideal structure inspired by the European model. For this reason, it was subjected to intense criticism as if doomed to fail. This study intended to provide a different and more optimistic overview, demonstrating that the BDPA already has enough guarantees to act as an independent authority. The author opted for looking at the glass "half full" instead of seeing it "half-empty". Accordingly, the effectiveness and success of the BDPA will depend more on the ability of its first Directors than on the statically structure provided by law. In this context, more important than criticizing the BDPA's structure is to contribute to its functioning - and watch over it -, to ensure that it will, in fact, fulfill its important mission. Especially in the current scenario of economic crisis, where the solutions adopted are usually not the ideal ones but those that are feasible.

To come to this conclusion, the author has carried out a structuralist analysis comparing the Brazilian BDPA with its Uruguayan equivalent, the URCDP. He demonstrated that the URCDP is very similarly structured to the Brazilian authority and it has been acting for over more than a decade quite successfully. This corroborates with the assumption that even more important than structure is how the authority performs its duties in practice. And at this point, at least for now, there are not enough scientific basis to question the BDPA, since it has not even started performing its activities.

What everyone hopes is that the BDPA will be a success and contribute decisively to the improvement of the culture of personal data protection in Brazil. To achieve that goal, it deserves an initial vote of confidence. As the Brazilian writer Ariano Suassuna once said: "the optimist is a fool; the pessimist is dull; the good thing is to be hopefully realistic."

Finally, since the current structure of the BDPA is already consolidated it would be advisable to broaden the debate to other issues of paramount importance, although not yet in the spotlight. For example, the potential conflict of attributions between the BDPA and other public bodies and entities ruled by ordinary law, such as the relationship between the BGDPL and other laws that sparsely address personal data protection, such as the Consumer Defense Code and the Brazilian Civil Framework of the Internet.

REFERENCES

BIONI, Bruno Ricardo. Privacidade e proteção de dados pessoais em 2019. Jota, 28 jan. 2019. Available at: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/privacidade-e-protecao-de-dados-pessoais-em-2019-28012019>. Access: 29 Jul. 2019.

BOBBIO, Norberto. Da Estrutura à Função: Novos Estudos de Teoria do Direito. Tradução: Daniela Beccaccia Versiani. Barueri: Manole, 2007.

Teoria do Ordenamento Jurídico. 10. ed. Brasília: Universidade de Brasília, 1999.

BRAZIL. Câmara dos Deputados. Projeto de Lei nº 5.276/2016. Available at: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Access: 08 Dec. 2018.

Presidência da República. Mensagem de Veto n. 451/2018. Available at: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Access: 07 Dec. 2018.

BRUNET, Laura Nahabetián. Del Gobierno Electrónico al Gobierno de la Información. Montevideo: Amalio M. Fernández Editorial y Librería Jurídica, 2015.

COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: 28 jan. 1981. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>. Access: 30 Jul. 2019.

Cooperação internacional. Available at: <https://edpb.europa.eu/international-cooperation_pt>. Access: 31 Jul. 2019.

DIGITAL 9. About the D9. Available at: <https://www.digital.govt.nz/digital-government/international-partnerships/the-digital-9/>. Access: 31 Jul. 2019.

DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção e dados pessoais. Rio de Janeiro: Renovar, 2006.

HOPT, Klaus. Uma Conversa sobre Direito Societário Comparado com o Professor Klaus Hopt. Cadernos Direito GV. São Paulo: Direito GV, v. 6, n.º 2, mar. 2009.

LYNSKEY, Orla. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

MENDES, Laura Schertel; et al. Methodology for Comparative Law Analysis on Personal Data Legal Protection. Proceedings of the 2019 Communication Policy Research Latin America - CPRLATAM. Cordoba: Americas Information and Communications Research Network. p. 141-162, Jul. 2019.

MOREIRA NETO, Diogo de Figueiredo. Direito Regulatório. Rio de Janeiro: Renovar, 2003.

PARENTONI, Leonardo. Protection of Personal Data in Brazil: Internal Antinomies and International Aspects. In: LIMA, Cíntia Rosa Pereira de (Coord.). Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020.

PSCHEIDT, Kristian. Lei de Proteção de Dados: de agência para órgão, a mudança é muito maior, analisa Kristian Pscheidt. Poder 360, 28 jul. 2019. Available at: <https://www.poder360.com.br/opiniao/governo/lei-de-protecao-de-dados-de-agencia-para-orgao-a-mudanca-e-muito-maior-analisa-kristian-pscheidt/>. Access: 29 jul. 2019.

RIPERT, Georges. Aspectos Jurídicos do Capitalismo Moderno. Campinas: Red, 2002.

SARMENTO E CASTRO, Catarina. Direito da Informática, Privacidade e Dados Pessoais. Coimbra: Almedina, 2005.

SOPRANA, Paula. Temer cria autoridade de proteção de dados vinculada à Presidência. Folha de São Paulo, 28 dez. 2018. Available at: <https://www1.folha.uol.com.br/mercado/2018/12/temer-cria-autoridade-de-protecao-de-dados-vinculada-a-presidencia.shtml>. Access: 29 Jul. 2019.

TENE, Omer. Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. Ohio State Law Journal. Columbus: Moritz College of Law. v. 74, n. 06, p. 1217-1261, Nov. 2013.

THE EUROPEAN UNION. Comissão Europeia. Decisão de Execução da Comissão. Bruxelas: 21 ago. 2012. Available at: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32012D0484>. Access: 30 Jul. 2019.

THE UNITED STATES OF AMERICA. Federal Trade Commission - About the FTC. Available at: <https://www.ftc.gov/about-ftc>. Access: 27 Jul. 2019.

Federal Trade Commission - News & Events. Available at: <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>. Access: 27 Jul. 2019.

TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. Amsterdam: Elsevier. v. 34, n. 01, p. 134-153, Feb. 2018.

URUGUAY. Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento - AGESIC. Available at: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevos-datos-resultados-de-la-5a-encuesta-de-conocimientos-actitudes-y>. Access: 01 Aug. 2019.

Instituto Nacional de Estadística. Available at: <http://www.ine.gub.uy/inicio>. Access: 31 Jul. 2019. In relation to Brazil see: BRAZIL. Instituto Brasileiro de Geografia e Estatística. Available at: <https://www.ibge.gov.br/>. Access: 31 Jul. 2019.

Unidad Reguladora y de Control de Datos Personales - Estadísticas. Available at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/datos-y-estadisticas/estadisticas>. Access: 01 Aug. 2019.

Unidad Reguladora y de Control de Datos Personales. Informe a 10 años de la Ley de Protección de Datos Personales. Revista Uruguaya de Protección de Datos Personales. Montevideo: URCDP. n. 03, p. 85-98, Oct. 2018. Available at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/revista-de-proteccion-de-datos-personales-3era-edicion-2018>. Access: 01 Aug. 2019.

VALENTE, Jonas. Autoridades e pesquisadores debatem adoção da lei de proteção de dados. Agência Brasil, 18 jun. 2019. Available at: <http://agenciabrasil.ebc.com.br/politica/noticia/2019-06/autoridades-e-pesquisadores-debatem-adocao-da-lei-de-protecao-de-dados>. Access: 29 Jul. 2019.

VENTURA, Ivan. Entenda como será a futura Autoridade Nacional de Proteção de Dados. Consumidor Moderno, 05 abr. 2019. Available at: <https://www.consumidormoderno.com.br/2019/05/01/entenda-futura-autoridade-nacional-protecao-dados/>. Access: 30 Jul. 2019.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. Yale Law Journal. Yale: The Yale Law Journal. v. 113, n. 06, p. 1151-1221, Apr. 2004.

Los Datos Personales en tempos de Coronavirus o COVID-19

Mtra. Elsa Bibiana Peralta Hernández

Es magíster en Administración Pública por el Instituto Nacional de Administración Pública, con Mención Honorífica, y Licenciada en Derecho por la UNAM, actualmente cursa el Doctorado en Administración y Políticas Públicas. Cursó la especialidad en Preparación para aspirantes al cargo de Juez (IEJ del Poder Judicial de la CDMX), así como el curso de Especialización Judicial del Poder Judicial Federal y el Seminario de Capacitación a Servidores Públicos Mexicanos por el Ministerio de Comercio de la República Popular China en el Centro de Capacitación de la Academia Nacional de Gobernación de China en Beijing.

Cuenta con diversos Diplomados, entre los que destacan: Transparencia y Acceso a la Información Pública (INFODF y UAM); Diplomado en Administración y Gestión Pública (IBERO) y Diplomado en materia de Protección de Datos Personales (INFODF y EAPDF), así como la especialidad en Derechos de la Niñez (UAM-SCJN). Actualmente cursa el Diplomado en Derecho de las Tecnologías en la Barra Mexicana Colegio de Abogados.

A la fecha, se encuentra en su 5° año de gestión como Comisionada Ciudadana del INFO CDMX, donde está a cargo de la Coordinación de la Dirección de Datos Personales. Es enlace y representante del INFO ante diversos Organismos Internacionales como la RED IBEROAMERICANA de PDP, la Asociación Latinoamericana de Archivos (ALA) y el International Council on Archives (ICA). Durante sus 32 años como Servidor Público de 1988 al 2014 colaboró en diversos Órganos Jurisdiccionales, destacando su nombramiento como primera Contralora General del TSJDF y Asesora y Secretaria Técnica de la Presidencia del Consejo de la Judicatura del DF. Cuenta con amplia experiencia por más de 14 años en los ámbitos de Transparencia, PDP y Anticorrupción, impartiendo conferencias para distintas Instituciones de Gobierno Locales, Nacionales e Internacionales en países como Argentina, Colombia, Uruguay, El Salvador, Perú y España. Colaboró en los procesos de armonización de las Leyes de Transparencia, Protección de Datos Personales, Archivos y Anticorrupción, así como durante su gestión sola al frente del INFO se publicó la Ley de Transparencia comentada.

En el Sistema Nacional de Transparencia, es Coordinadora Nacional de la Comisión de Rendición de Cuentas (2019-2020). Fungió como Secretaría Técnica del 2018 al 2019, y de la jurídica del 2017 al 2018; ha sido la única comisionada en ocupar dos secretarías, en dos comisiones al mismo tiempo, por dos periodos seguidos, en la de PDP y en la de Archivos, del 2015 al 2017. Ha integrado también las de Tecnologías de la Información y Plataforma Nacional de Transparencia, y Derechos Humanos, Equidad de Género e Inclusión Social.

En materia de Equidad de Género es autora del libro de poesía Reflexiones Femeninas (2012) e integrante del Comité Interinstitucional de Igualdad de Género de los Órganos Impartidores de Justicia. Además, integra el Observatorio de Participación Política de las Mujeres en la CDMX y la Comisión de Género de la Barra Mexicana de Abogados; es miembro fundador, y primera Coordinadora del Comité de Género del INAP.

Es miembro de la Barra Mexicana Colegio de Abogados, e integrante activo de las Comisiones de Derecho Constitucional, Derecho Administrativo y Protección de Datos.

Participa habitualmente en diversas capsulas de RADIO (IMEFI y RADIO UNAM) y TV (Capital 21), entre muchos otros. Colabora como columnista invitada en Contra Réplica y otros diarios, así como ha realizado y publicado diversos artículos en materias como Responsabilidades, Anticorrupción, Transparencia y Armonización Contable y Administrativa, Género, y otros, en publicaciones auspiciadas por el INAP, la Comision de Derechos Humanos de la CDMX, el Colegio de Contadores Públicos y el Tribunal Superior de Justicia del DF, entre otros.

Cuando fui invitada a escribir un artículo para esta prestigiada Revista, llegué a pensar en innumerables títulos y temas sobre los cuales trabajar. La materia de datos personales y su protección ofrecen una amplia gama sobre la cual escribir. De hecho, cada uno ofrece, a su vez, muchos otros tópicos sobre los cuales aportar.

El tiempo transcurrió y de la mano de él las ideas fueron surgiendo. Sin embargo, cuando decidida estaba a escribir sobre un tema, venían a mi mente otros que desplazaban al que se había posicionado. Así, el tiempo siguió pasando hasta que llegamos a una situación de tintes inimaginables en el mundo; o no, de alguna manera sí lo habían imaginado aquellos realizadores de literatura o cine apocalíptico, cuyas mentes vieron limitadas frente a lo que verdaderamente vivimos; y hablo en presente porque, cuando por fin me senté a escribir, aún nos encontrábamos dentro del confinamiento, al que fuimos sometidos por la llegada de un virus a nuestras vidas que trastocó, por completo, la

vida en el planeta como la veníamos ejerciendo.

En efecto, mientras la imaginación se quedó pequeña, pues no vinieron marcianos ni seres malignos a destruirnos, así como tampoco amenazas del espacio o guerras mundiales con poderoso armamento, que según serían las formas más posibles de extinguir la vida en la tierra; llas personas de este planeta nos vimos afectadas por un diminuto virus, que puso fuera de control a la población de la mayoría de los países, principalmente aquellos de los denominados del primer mundo como superpotencias, tales como China y Estados Unidos, Reino Unido, Alemania, Francia, España, Italia, etc.; lo cual, afectó en mayor medida al resto, como los de América Latina, entre los que destacan por el número de contagios y efectos, Brasil, México, Argentina, Ecuador, Perú, Chile, Colombia, etc.

Mientras escribía estas líneas, me di cuenta de que el impacto era fuerte, pues un diminuto e imperceptible virus, había logrado lo que hasta ahora nadie pudo hacer en temas de control social, económico, político y tecnológico. A través de una enfermedad, que provoca la muerte por afectar algo tan esencial como respirar, se generó una psicosis que hizo que nos confináramos en nuestras casas, dejando todo lo que creímos que era imposible: nuestra vida social y sus diversas interacciones.

Antes de que se propagara la epidemia, el mundo se encontraba demasiado convulso. En todas partes se desarrollaban no sólo guerras, que de alguna manera ya estábamos acostumbrados a ellas; sino también, numerosas revueltas internas contra la economía, la política interna y los gobiernos, cuyas elecciones se cuestionaban en redes sociales y diversos medios, por la manipulación electrónica que suscitó escándalos tales como el de Cambridge Analytics, o de manera económica por la trascendencia corrupta que implicó, como el de Panamá Papers, por mencionar los más sonados.

El internet y las comunicaciones, la tecnología en un desarrollo inimaginable, la Inteligencia Artificial y el denominado 5G, cobraron tal relevancia en nuestras vidas, que lo prioritario era estar conectados en el mundo de todas las formas posibles, de tal manera, que podíamos ser activos en todos los frentes que quisiéramos participar, con cualquiera de las intenciones, dándonos a conocer por la simple influencia o impacto generado en el resto del sector social. Esta interacción con el mundo generó influencias, con efectos sociales positivos o negativos, que hacían imprescindible existir virtualmente, más que físicamente, sin importar que ello tuviese para la humanidad una utilidad derivada del ejercicio de algún talento, como sucedía con los aportes históricamente documentados; sino sólo por el hecho de llegar a la mayor cantidad de población en el mundo.

Ese impacto se volvió tan imprescindible, que las personas físicamente podían estar en un lugar, pero llegar fácilmente a cualquier otro; realizando multiplicidad de acciones no controladas por nadie, salvo, en cierta medida, por quienes ofertan los servicios tecnológicos; los cuales también se volvieron incontrolables (y ahora lo son más), frente a la cantidad de información que se recopila y el valor de ésta en una economía globalizada y una población mundial en todo momento conectada.

En los últimos 20 años, con ese avance tecnológico, la vida de las personas se vio inmersa en una vorágine de actividades, en la que nadie paraba por nada, ni siquiera los gobiernos lo podían controlar; las fronteras se derrumbaron de manera virtual, frente al inútil esfuerzo de algunos gobiernos, de construir muros físicos para detener la migración virtual y física de las personas. En este contexto, el control político y económico se debilitó frente al embate de las masas tecnológicas, propiciado por el desarrollo comercializado por grandes empresas de tecnología, cuyas posibilidades de organización se volvieron incontrolables, en ambos casos, como muy bien lo explica Manuel Castells en su libro ¨Redes de indignación y Esperanza¨.

La posibilidad de acceder a información y servicios ofertó tantas cosas que el tiempo y el dinero adquirieron una dimensión y valor insuficiente. Con el temor de ser obsoleto o estar fuera del contexto social virtual, la necesidad tecnológica creciente generó la obligación de consumir, de tal manera que el planeta también entró en crisis. La necesidad de conexión generó la creencia de poseer lo último en aparatos y tecnología, pues de lo contrario, el nivel ¨humano¨ desciende, olvidando que la tecnología se creó en función del ser humano, lo cual cambió para convertirlo de usuario a mercancía. En efecto, la gran cantidad de información que las personas vierten con el uso de la tecnología se volvió tan valiosa que generó la idea de mayores necesidades. Aparece así el internet de las cosas, con la idea de facilitarnos la vida, cosificándonos aún más. Las ciudades y sus edificios se volvieron inteligentes, controlados por mecanismos recopiladores de información con la intención de gestionar los servicios urbanos y su infraestructura, lo cual, no siempre funciona ni se utiliza para esos fines; generando con todo eso la percepción errónea de vivir en un mundo conectado, cada día más desconectado.

De esa manera, la vida en los últimos años se volvió una carrera en la que la vida y la salud se volvieron una mercancía más, como muchas de las necesidades humanas, que sentíamos satisfechas por efecto de la publicidad, por adquirir tal producto o aplicación. La salud se volvió secundaria. No obstante contar con aparatos que ahora nos miden todo, resultaban prioritarias otras cosas en ese ir y venir de la vida, menos

la vida misma y la salud, pues el tiempo para atenderlas era lo que hacía falta. ¿Cuántas personas no dejamos de lado un padecimiento por ocuparnos de actividades que consideramos más relevantes? Yo lo hice muchas veces.

Pero, de repente, un día, lo que no tenía freno, paró.

Frente al temor, primero receloso y después obligatorio, por diversos medios, la pandemia consiguió lo que más de una autoridad hubieran deseado: guardarnos en nuestra casa. El temor de enfermar y morir logró detener la vida que considerábamos normal, frente al embate de una epidemia incontrolable respecto de la cual, paradójicamente, la tecnología, aun con sus avances, no puede (al menos mientras escribía estas líneas no había una cura y espero que al publicarla ya exista). Lamentablemente, hasta este momento, a corto plazo no se ve una posible solución o cura para la enfermedad; por lo que, el retorno se visualiza con nuevos esquemas de convivencia física, en los que el contacto humano no puede ser.

Sin embargo, aún cuando el confinamiento logró paralizar física y presencialmente a la población en el mundo; no logró evitar que tecnológicamente sigamos en contacto. En efecto, si bien es cierto, en la historia de la humanidad hubo epidemias y males que mermaron significativamente el número de habitantes del planeta; también lo es, que nada se compara con lo que ahora nos sucede, pues somos más población que nunca y contamos con tecnología, que, aunque físicamente estemos resguardados, virtualmente seguimos navegando y haciendo vida social en el ciberespacio.

La tecnología es lo que genera una gran diferencia con anteriores hechos históricos. Esa parálisis física vino a significar que las actividades convulsas se detuvieran. De esa manera, las protestas pararon, los ataques terroristas, pues ya no hay gente afuera a quien matar; ciertos conflictos bélicos también frenaron, pues los países que suelen financiarlos tuvieron que destinar los recursos a atender la emergencia sanitaria generada. En ese contexto, la pandemia puso en evidencia también que, pese a los avances tecnológicos, lo peor de los sistemas de salud en todo el mundo quedó evidenciado, pues no han avanzado de la misma manera, ante la carencia de infraestructura que pudiera resultar mínimamente suficiente para atender a la población en caso de un contagio masivo. Ni siquiera los mencionados países del primer mundo o superpotencias se vieron preparados frente a esto. El avance tecnológico manifestó que los gobiernos se han preocupado por invertir en armamento y tecnología para controlar el poder, dejando de hacerlo en lo que realmente importa para el bienestar de las personas, como la vida, la salud y el bienestar social.

Lo anterior, si bien les preocupó, resultó ser la mejor forma de control. Las medidas de confinamiento, ante la incertidumbre de poder atender al grueso de la población frente a una infraestructura de salud escasa y deficiente, logró resguardar a las personas y restringir sus protestas. Esta medida resultó un buen mecanismo de control, primero por sanidad y después por resultar eficiente como control social, lo que se cuestiona, pues el miedo a la muerte siempre se ha manipulado con información y cifras que logran que las personas por temor se replieguen ante la incertidumbre.

Al margen de un control social, necesario dada la efervescencia en el mundo, previa a la emergencia sanitaria decretada por la pandemia, había que sostener el confinamiento y algunas actividades consideradas esenciales, como salud, alimentación, educación, trabajo, seguridad y militares, transporte y comunicaciones, entre otras. Satisfacer esos rubros motivó que se generarán una gran cantidad de servicios y aplicaciones para poder atenderlas. Para contener la epidemia se decretan medidas en todos los países, que van desde mecanismos coercitivos hasta voluntarios, dependiendo del tipo de gobierno. En la mayoría de los países, se desarrollan mecanismos de información, pero también de monitoreo, con aplicaciones de geolocalización y contacto, que resultan intrusivas en la privacidad de las personas, bajo el argumento de detectar y contener puntos de contagio. Se recopila gran cantidad de información sobre los pacientes, tanto por los servicios de salud públicos como privados. Las estadísticas alarman y con ello la pandemia se alarga de diferentes formas en países que influyen de manera decisiva en los continentes en los que se ubican.

Lo mismo sucede con la industria de alimentos que, al ser prioritaria, genera que se desarrollen mecanismos de abastecimiento en los lugares de confinamiento, por lo que las aplicaciones para todo tipo de compra y venta de bienes y servicios generan una demanda sin precedentes. Transportar, transitar y trasladarse se restringe a lo local y los servicios por aplicación se hicieron indispensables por un factor más que resguardaba del contagio, con cierta seguridad en el traslado, por lo que aplicaciones de ese tipo se disparan; la aviación comercial paró, excepto para transporte de insumos necesarios para la pandemia, medicamentos y alimentos; y la industria en general se detuvo, salvo la de alimentos que siguió operando con restricciones al igual que todo tipo de centros de abasto, pero todas aquéllas encargadas de satisfacerla continúan apoyadas en la gran cantidad de información que generan las necesidades aportadas en las plataformas que cuentan con la infraestructura para competir.

La mensajería y reparto continuó operando, pues los servicios en línea para abastecer se volvieron esenciales, las aplicaciones al respecto cobraron gran relevancia al convertirse en el medio para allegarse de todo tipo de insumos; la demanda en este sentido también se volvió un hecho sin precedentes, al ser un mecanismo que permite a las personas obtener todo tipo de bienes o servicios sin salir de casa. El comercio cambió para transitar de un flujo físico a un flujo virtual. Los negocios se transforman y sobreviven todos aquellos que encuadran en estos rubros. Poco a poco se advierte la extinción de todos aquéllos que no lo hacen o los que no resultan prioritarios.

La industria del entretenimiento se volvió esencial a través de múltiples plataformas: las de cine, televisión por cable e internet; mientras que las aplicaciones de redes sociales se desbordaron ante el ingenio de quienes, confinados, deseaban ser vistos por los demás o tratar de estar cerca de todos aquellos a quienes pudiendo visitar antes, nunca lo hicieron por falta de tiempo, tratando de resolver un poco el alejamiento y soledad que el confinamiento acentúo.

La necesidad de mantener activo el aspecto laboral, frente al desempleo que resultó una enfermedad igual o peor que el mismo virus, obligaron a crear figuras y modelos de organización para mantener muchos empleos; entre otros, el denominado HOME OFFICE. Las actividades, antes esencialmente personales, se volvieron remotas con aplicaciones que permiten a un gran número de personas conectarse para una reunión, clases y cátedras, conferencias y conciertos. La interacción humana cambió para volverse más receptiva que nunca, modelos en los que la presencia física resultaba imprescindible, se transformaron para lograr el objetivo a distancia, por lo menos para continuar generando fuentes de empleo, pero, aunque las plataformas permiten la interacción, no es igual que en persona, por lo que no es completa. La educación también cambió para dar paso a clases virtuales en las que no se puede realizar un monitoreo real de lo aprendido, dado que los padres se han vuelto no sólo tutores sino coactores con los hijos, de lo que son sus responsabilidades escolares; lo que tiende a generar un déficit difícil de medir aún, pero que, ante la emergencia logró salvar el proceso educativo, en la cual también se pusieron en evidencia, las enormes deficiencias que en muchos países ha generado la falta de inversión en un modelo educativo que forme verdaderamente a las personas.

En resumen, la economía mundial se paralizó y cambió sus parámetros por una epidemia global, sin precedentes en la historia de la humanidad. Sin embargo, paradójicamente, los inversores de todos aquellos bienes y servicios que se evidenciaron como esenciales en la pandemia, resultaron beneficiados con ese drástico giro en la economía; lo mismo que los dueños de aplicaciones, servicios en línea, redes sociales y corporativos que desarrollaron plataformas para continuar conectados llevando a cabo las actividades descritas.

Los mercados económicos como funcionaban anteriormente también han sufrido enormes cambios. Los valores monetarios cambiaron para dar paso a otros basados en información, particularmente en datos de las personas, que revelan sus necesidades de consumo, cautivas ahora por un tema de confinamiento, que vino a confinar también sus necesidades al uso de plataformas, que las transforman en información imprescindible para los proveedores de esos bienes y servicios. Esto nos lleva a pensar, que en la economía también las cosas cambiaron, pues mientras antes dominaban el mundo los grandes productores de petróleo porque controlaban el mercado energético; así como, después los especuladores de capital; ahora las industrias mencionadas, entre ellas las de procesamiento de datos e información, se han convertido en el Mercader de Venecia, dada la trascendencia e importancia que cobra el manejo de la información en un mundo encerrado, cuyas ventanas son la tecnología e información que esas empresas procesan, en donde las personas son la mercancía y sus datos la materia prima. Saber y conocer los perfiles de necesidades de la gran cantidad de población confinada, es lo que determina y determinará en el futuro la vida de la industria y comercio, en tanto que esa información establece los patrones de consumo conforme a las nuevas necesidades de la población y, por ende, de las inversiones que se hagan para satisfacerlas.

Durante el confinamiento, la idea de satisfacer todas las necesidades humanas, aparte de las ya mencionadas, ha puesto de manifiesto que el hombre es un ser social, por lo que estar comunicado también ha sido indispensable durante su resguardo. Por ello, como ya dijimos, a diferencia de otras pandemias, ésta se distingue por la tecnología que ha permitido al ser humano sobrellevarla hasta donde la brecha digital lo permiten. El internet y las redes sociales se han convertido en el mecanismo de información (y de desinformación) dominante, así como en fuentes virales de distracción pues, a pesar del triste panorama de la crisis sanitaria, el humor y la risa, como a menudo ocurre en estos casos, han sido la conexión entre el mundo exterior, con familiares y amigos, y hasta con personas extrañas, por el sólo hecho de que los demás adviertan que seguimos existiendo. Empresas de video llamadas han tenido un crecimiento exponencial con motivo de la pandemia. Diversos autores señalan que antes de la expansión del coronavirus, las acciones de empresas de video llamadas costaban alrededor de 70 dólares; y que para el mes de marzo valían el doble, aumentando su valor conforme el confinamiento se ha ido alargando, convirtiendo a sus principales accionistas en las personas más ricas del mundo. Por su parte, grandes empresas digitales que ya eran líderes en el mercado accionario, antes de la pandemia, han incrementado exponencialmente su valor, en contraste con otras industrias cuyos inversionistas nunca pensaron que tendrían problemas, tales como el turismo, entretenimiento no virtual y muchas más, que ante el confinamiento perdieron clientela física que era el sustento de su modelo de negocio, el cual, conforme se advierte, necesariamente debe transitar a un modelo híbrido de negocio entre

presencial y virtual. Lo preocupante es que esos grandes capitales no parecen ahora ocupados en ello.

Ante este escenario nos preguntamos si estamos avanzando hacia un nuevo esquema mundial y orden económico y la respuesta es sí. De no hacerlo, se generará una crisis económica mundial que es posible que nos enfrente a la muerte del capitalismo como lo conocemos, y ni hablar de otros modelos políticos o económicos, que de por sí ya estaban muertos. La experiencia está revelando que dentro de nuestro confinamiento somos cautivos de quienes controlan el mercado que produce lo necesario para atender la pandemia y el confinamiento; como ya sucede con los países que se encargan de abastecer estos insumos, desde los más básicos, como medicamentos, test, mascarillas, guantes, respiradores; hasta las grandes empresas de tecnología, cuyas sedes se encuentran en países que ejercen un dominio económico, las cuales, con el gran potencial que representa la información recopilada con la pandemia, resultan ser los nueves jeques de los datos y la información. No pugno por ningún modelo económico ni apoyo a ningún país, pero sí ante momentos de crisis lo importante es aprender a transformarse, yo voltearía los ojos al modelo chino, que conocí durante una especialidad que curse en ese país, que continúa en un esquema social, no socialista, en tanto pretende generar igualdad en la prestación de bienes y servicios, en un modelo de economía de mercado, en el que todos deben trabajar por igual para mantener un nivel de vida en común. Si alguien se ha transformado, pese a todo tipo de adversidad, durante más de cinco mil años, son los chinos.

No obstante, eso no gusta a quienes a lo largo de la historia de la humanidad la han controlado política y económicamente. Veamos si lo permiten pues los gobiernos que deben luchar en dos frentes: el externo, en un contexto internacional en el que el Internet y las comunicaciones dificultan mantener a las personas confinadas al interior de su país; pero también en el interno, cediendo a la tentación que puede generarse en un entorno en el que el populismo y el fantasma del absolutismo acechan, tratando de limitar el ejercicio de los derechos más esenciales, como el acceso a la información y la libertad de expresión, dentro de los que se regulan las comunicaciones y la tecnología. Antes de que surgiera el brote viral, el mundo se convulsionaba con múltiples protestas contra la globalización financiera y sus efectos, que llevaban a la población del planeta a condiciones de pobreza, incluso en los países más desarrollados, en los que las personas comenzaron a ver mermada la calidad de vida a la que estaban acostumbradas. Los movimientos de indígenas, migrantes y género cobraron gran relevancia.

Con la pandemia se reprimieron dado el confinamiento, y no obstante los movimientos en redes sociales, la fuerza que da la presencia física se perdió. La globalización en un sentido positivo nos mantenía conectados y en intercambio constante; ahora, con el confinamiento, se evidencia un aspecto negativo, en tanto que favorece los egoísmos, las fracturas y el ultranacionalismo, con la idea de combatir la pandemia los gobiernos se cierran, lo hacen también con sus fronteras, controlando el flujo de las personas y con ello, condenándolas a un doble confinamiento. Ejemplo de esto, son algunos líderes políticos, como el de Gran Bretaña, el de EU y el de Brasil, entre otros, que insisten en cerrarse para protegerse internamente, pero con una visión intervencionista; lo cual, estiman los que saben, no resuelve nada y el proteccionismo sólo aísla; lo que con el confinamiento se ha agudizado, poniendo en evidencia, como nunca, que tales gobiernos y sus políticas resultan contrarias a todo ejercicio que genere un orden mundial sano, no sólo económicamente hablando; sino también por temas de sanidad y salubridad; pues no por nada, son los países que mayores contagios y muertes propiciaron en su región, poniendo en evidencia cómo la práctica extrema de políticas neo liberales y absolutistas debilitó la inversión pública en sectores prioritarios como la salud, llevándolos a la crisis de atención que se puso en evidencia también ahora con la pandemia. La mayoría de los gobiernos han sido severamente criticados por no estar a la altura de las circunstancias en el combate y control de la emergencia sanitaria, pues no han propiciado la protección que sus gobernados esperan. En este sentido, el actuar negligente de los dirigentes se ha evidenciado de muchas formas, aunque todos tienen un esquema en común: informar a las personas; lo único que ha sucedido es que se dedican a bombardearlas con gran cantidad de datos, con la finalidad de emitir el mensaje de ¨control¨ sobre la situación; lo que no sucede así, ante la confrontación de datos y estadísticas que no coinciden con la realidad, que se refleja por las redes sociales y los medios de comunicación, los cuales también han jugado un papel preponderante ante la situación. La OMS ha definido este fenómeno como infodemia, pandemia de info-falsedades. a la par, los sistemas de mensajería móvil se han convertido en verdaderas fábricas continuas de engaños y mentiras, muchos elaborados de tal manera que dan la impresión de seriedad y credibilidad para que llas personas los viralicen.

En ese sentido, de la mano de malas políticas de información, la desinformación favorece, particularmente a los gobiernos que con ello controlan a las personas. La gran cantidad de datos, que se recopilan de las personas por motivos de salud, geolocalización y contacto, frente al embate de las plataformas, como las que hemos mencionados, que recaban gran cantidad de información de bienes y servicios, no puede arrojar que no se cuente con información precisa, particularmente de la pandemia. Sin embargo, no proporcionarla, controla a las personas, por lo que el manejo de sus datos personales, en este sentido ha revelado también que el control de los datos y la estadística que genera ya sea anonimizado o no, también es el oro de los gobiernos, quienes de esa manera controlan a la población, que continúa confinada ante el riesgo de no saber y no entender realmente qué está pasando.

Aunado a ello, los medios de comunicación no ayudan mucho a mantener esa información, dado que dependiendo de los intereses a los que atienden, propician información tendenciosa y poco confiable, factores que favorecen la proliferación de noticias falsas que derivan de la confianza existente entre personas que comparten información en una misma red y la repiten, reiterando los mensajes de idéntica matriz, sin estar seguros de lo que comparten. Ese entorno, en el que la desinformación juega un papel controlador, algunos desarrolladores implementan políticas que tienden a contribuir, queremos pensar que tal vez sin proponérselo; o proponiéndoselo; tal es el caso de los mensajes de texto por WhatsApp, que durante la pandemia implementó una restricción que ya no te permite reenviar los mensajes e inclusive sólo puedes compartir alguno hasta cinco contactos. Estas restricciones se venían aplicando con antelación y con el tema de la pandemia se agudizaron; lo cual, también puede interpretarse como restricción a las capacidades organizativas, que la aplicación tenía para las personas. El peligro de esto es un control, que visto de manera positiva evita que circulen noticias falsas, aparentemente ciertas, que en ocasiones pueden afectar la salud; pero visto en sentido negativo, restringe tu derecho a compartir lo que desees, que era una de las libertades absolutas de que gozabas en internet y en este tipo de aplicaciones, que se distinguían por la facilidad con que contaban para compartir información.

Frente a la desinformación o exceso de ésta, lo cual también desinforma, algunos minimizan los efectos de la pandemia; otros, niegan la gravedad de la situación, como si el coronavirus se tratara de una gripe cualquiera. Muchos se han centrado en dar respuestas locales, nacionales, gestionando la pandemia de manera independiente, sin verdadera coordinación internacional. Pero todos coinciden en dos cosas: la primera, en proporcionar gráficas y cifras sobre contagios, número de casos, casos positivos, negativos, activos, sospechosos, defunciones, nuevos contagio; y la segunda, en que ningún país puede darle solución al problema de manera pronta, no se sabe si porque no es posible aún o porque, ante la evidencia del control que representa sobre la población mundial, es mejor mantenerla, resultando la generación de emergencias sanitarias, mucho más lucrativo económica y políticamente como control social, que las guerras. Tal vez estamos entrando en una era de guerras biológicas, donde de cualquier manera se están generando muchas bajas en cualquiera de los bandos. En este sentido, la imaginación de los autores de libros y guiones de películas o series, siguen quedando cortos de imaginación, como lo referí en un principio.

Lo que es un hecho, es que la mayoría de los gobernantes han manejado la situación, bajo esquemas obsoletos tanto política como administrativamente hablando. Es indispensable que se documenten los gastos, la transparencia y la rendición de cuentas son muy importantes; siendo importante destacar que en momento como los que nos ocupan, han brillado por su ausencia. Si bien es cierto, la mayoría de las autoridades han transparentado diariamente datos e información sobre la propagación del virus y las acciones implementadas, la emergencia demanda una amplia e inmediata disposición de recursos, por tanto, la transparencia y rendición de cuentas cobran especial relevancia, para evitar conductas que propicien corrupción y desvío de recursos con fines electorales o de otra índole. Las grandes tragedias siempre crean fondos de apoyo y figuras económicas que se convierten en verdaderos sacos de riqueza que, con el pretexto de atender el problema, son difíciles de fiscalizar, perdiéndose el camino del dinero una vez agotado el problema. Esto está sucediendo en todo el mundo, en el que, ya pasada la contingencia, comenzarán a surgir las voces pidiendo cuentas, las cuales nunca se rinden.

Transparentar esta información es necesario y urgente, para dar seguimiento a los recursos públicos, desde su origen, uso y destino final como herramienta para mitigar la corrupción en aspectos como: Diagnóstico de necesidades, Compras, Contrataciones, Padrones de personas beneficiarias de apoyos económicos y sociales, Medidas fiscales, financieras y redirección del gasto público, Atención a grupos vulnerables, Protección al empleo y centros de trabajo, y en general todo el seguimiento de recursos públicos durante y después de la emergencia.

Este punto es muy importante, pues de la mano de la transparencia y la rendición de cuentas, deben existir las voluntades de generar toda la información necesaria y que se estime que la población necesita para estar informada, a través de ejercicios de transparencia proactiva y adecuada defensa de los derechos humanos de todas las personas. Insto a hacer transparencia proactiva como una buena práctica para poder contar con información. Lo importante, es que el tema de salud no sea el pretexto para evadir la rendición de cuentas y sí para salvar vidas. Si bien en estos momentos el bien jurídico mayor es la vida y la salud, el Estado no debe obrar con enfoques totalitarios ni excesivamente proteccionistas que vulneren los derechos humanos de las personas en aras de salvar su vida o preservar su salud. Las democracias han crecido y en regímenes como los nuestros en América Latina ha costado muchas sangre y vida implementar el respeto pleno de los derechos humanos.

En este sentido, en un esfuerzo desesperado para combatir la pandemia, los gobiernos y los particulares, muchas veces en colaboración, por la infraestructura que los segundos ofrecen a los primeros, dadas las carencias presupuestales de que éstos adolecen; los gobiernos han implementado el uso de tecnología para dar seguimiento y monitoreo a la pandemia; así, se elaboraron aplicaciones y mecanismos de control para dar seguimiento a las personas infectadas, pues darle rostro a los beneficiados, en un adecuado cruce de datos personales, genera certeza del destino de los recursos. Para ello, es importante generar bases de datos personales debidamente resguardadas, cuyas transferencias permitan atender por todos los sectores involucrados el tema.

Mediante diversas aplicaciones se conoce quiénes son las personas infectadas y las que estuvieron cerca; se puede ordenar el confinamiento de todas ellas y en caso de no cumplirse tal confinamiento, se establece algún tipo de sanción. Mediante la geolocalización a través del uso de dispositivos móviles y videocámaras se conoce y controla a llas personas. Diversos países como España e Italia lo implementaron. Empresas como Google y Apple anunciaron que trabajan conjuntamente para desarrollar una tecnología que permitirá a los dispositivos móviles intercambiar información a través de conexiones Bluetooth, para alertar a las personas cuando hayan estado cerca de alguien que dio positivo por el nuevo coronavirus. El COVID-19 se volvió la primera enfermedad global contra la que, si bien no se tiene cura, pese a los avances médicos; si se está combatiendo digitalmente a través de los mecanismos más avanzados para ello, no sin destacar, que ello debe hacerse sin violar la privacidad de las personas y algunos otros derechos humanos, ponderando la vida y la salud frente a la privacidad, sin olvidar que ésta no pierde vigencia frente a la necesidad de salvaguardar las primeras. Las excepciones al principio del consentimiento que se dan por cuestiones sanitarias y emergencias como la que nos ocupan, no consideran la indiferencia total de la voluntad de las personas, ni de los demás principios que rigen la protección de datos, los cuales continúan vigentes y deben ser observados en todo el mundo.

Dada la implementación de todos estos mecanismos, es que nos atrevemos a afirmar que los gobiernos y los particulares involucrados, cuentan con información que han estado recabando de manera constante; no obstante la aplicación de toda esta tecnología, geolocalización y el rastreo de la telefonía móvil, sumados al uso de los algoritmos de predicción, las aplicaciones digitales sofisticadas y el estudio computarizado de modelos estadísticos; concluimos que los resultados no han sido suficientes para controlar totalmente la pandemia. Y es que, aunado a malas políticas implementadas, la tecnología no puede todavía (y esperemos que eso no pase) contra la conducta humana. Aun cuando es cierto, que medidas sencillas como el uso obligatorio de la mascarilla, desinfectarnos las manos y frenar el avance del virus mediante la ciencia del confinamiento y del aislamiento social, pueden marcar una vital diferencia; lo cierto es que, el mundo no puede parar del todo. La propagación del virus, a pesar de la tecnología de ubicación, no logra hacer que las personas, dependiendo de sus diversas necesidades afectivas, laborales o económicas, entiendan que deben confinarse y, ello, en gran medida al descontrol del que ya hablamos. La propagación se ha dado por que las personas no dejan de moverse y no lo harán porque muchas de ellas obedecen a circunstancias en las que está más allá de toda posibilidad, o no creen del todo ante la falta de información precisa o desinformación.

La pandemia puso en evidencia todas estas vulnerabilidades para mantener el confinamiento o como consecuencia del confinamiento. En el primer caso, nos encontramos a todos aquellos que, por pertenecer laboralmente a los rubros prioritarios como la salud, la seguridad, la milicia y el comercio, necesariamente deben trasladarse y aun cuando observen todas las medidas de higiene y sanidad, sin embargo, están expuestos. Los repartidores, los ambulantes, los productores de comida, los campesinos y los proveedores de bienes y servicios como son telefonía, luz, agua, gas, etc. Estas personas saben que están siendo ubicadas, pues inclusive su servicio mismo los ubica o en razón de su celular. Sin embargo, poco o nada le importa frente a la necesidad de sobrevivir, pues, aunque saben que están expuestos, la necesidad de conservar el trabajo para sobrevivir se vuelve mayor que la propia subsistencia misma, por lo que el que se viole su privacidad y se les exponga como población vulnerable no resulta relevante para vivir. Lo importante es sobrevivir.

Otra vulnerabilidad que se evidencia, que violenta mayormente otros derechos, no sólo la privacidad; es el relativo a las personas indigentes, grupos vulnerables en general y ancianos. Los primeros, dependen totalmente del Estado y sus políticas, las cuales, en situaciones como éstas, los dejan correr su suerte dado que se vuelve prioridad salvar a los demás, aunado al hecho de que por su misma situación no cuentan con ningún tipo de tecnología que los ubique y se trasladan sin control por todos lados. Esta población no es escasa y abunda en las grandes ciudades, que han sido de las más golpeadas por la pandemia, dados los focos de concentración. Tristemente se vuelven población desechable que ni siquiera importa localizar, por lo que menos aún importará que sus datos personales se recaben y sean motivo de resguardo.

Otro grupo vulnerable es el de la gente trabajando en las calles, limpiando edificios, conduciendo autobuses, desinfectando hospitales, atendiendo supermercados, manejando taxis, repartiendo paquetes, etc. todos ellos no sólo corren riesgo por su necesidad de salir y conservar su empleo o sustento; sino enfrentan otros riesgos que la localización no les remedia o protege. Aunado al riesgo de infección que enfrentan en sus barrios marginados, se suman los riesgos que corren en los transportes públicos y en sus empleos. La vida se torna difícil pero la idea de sobrevivir es más fuerte que cualquier temor, en donde no cabe pensar ni siquiera preocuparse por lo que está sucediendo con sus datos personales. En algunas ciudades del mundo, ese tipo de trabajadores son migrantes, lo que en su calidad de ilegales e indocumentados, acosados y extorsionados por las autoridades, es impensable para ellos acudir a los servicios de salud, por miedo a que los detengan. Contar con un aparato que permita localizarlos, a riesgo de morir, prefieren obviarlo, pues ello implica ponerse al descubierto de las autoridades que los deportaran, dejando de lado el camino difícil que han tenido que recorrer. Esta población no sólo no es localizable, sino invisible, por lo que el riesgo de contagio respecto de ella es aún mayor y al respecto debería haber políticas que protejan su salud y su integridad, amén de sus datos personales, que, de ser recopilados, sirven para ubicarlos con fines de deportación o repatriación de sus restos. Por tanto, frente a la necesidad de sobrevivir, el cuidado de los datos personales no resulta esencial sino peligroso. En México, me tocó presenciar por televisión, la

repatriación de un grupo importante de migrantes indocumentados que murieron por el virus en EU, cuya ubicación se logró gracias a una base de datos personales de oficinas que los apoyan.

Otra población que ha resentido los efectos de esta pandemia, no sólo porque sus características como la edad y sus padecimientos, los hacen más proclives al contagio; sino porque se les discrimina, son los ancianos. La mayoría de ellos aun cuando cuenta con tecnología, por no ser parte de su formación, no siempre la dominan, por lo que dentro de la vorágine de aplicaciones y usos están en desventaja frente a las generaciones más jóvenes, lo cual se convierte en un primer factor que los hace vulnerables ante la falta de información, ignorando muchas veces los efectos de compartirla, lo cual los puede ubicar como una persona adulta, motivando ser objeto de discriminación, abandono o fraudes. Una de las notas más tristes que hemos visto en estos días, ha sido la información que sobre la propagación del virus en los asilos o casas de retiro se han dado, en las que el número de muertos por contagio es mayor, por lo sensible de su salud; de la mano del hecho, de que mueren solos o sólo acompañados por sus cuidadores, porque, debido al confinamiento, su familia, que en la mayoría de los casos ni los visita, por la pandemia menos. A este escenario se suma otro más triste aún, el de algunos casos documentados en los que se ha llegado a estimar que, en caso de que los contagios sobrepasen la capacidad hospitalaria será necesario elegir y la población de ancianos no está considerada dando preferencia a las generaciones más jóvenes. Que aberración. En ese sentido se vuelve un tema de vida o muerte proporcionar la edad, pues es un dato personal que de conocerse implica discriminación y el riesgo de perder la vida.

Frente a estos escenarios, la tecnología sirve para ubicar y precisar estos casos, muchas veces sin que las personas lo sepan o entiendan de manera precisa los efectos, simplemente porque en algún momento proporcionaron esa información, que los coloca en esos supuestos para ser localizados y con ello resultar vulnerables en esta emergencia. En ese sentido, las bases de datos personales deben potenciar su uso y aplicación evitando en todo momento cualquier vulneración de derechos humanos. De no hacerse, las decisiones que se tomen respecto de esas personas serán también ignoradas por ellas, en franca violación a sus derechos humanos más elementales, no sólo la privacidad; la cual cobra especial relevancia si por razón de su ubicación, diagnóstico, situación laboral, migratoria, edad, está en juego su vida. En este sentido, las políticas de gobierno deben considerar el máximo respeto a la dignidad humana, pero para ello, tendrán que haber instalado la suficiente capacidad sanitaria que permita atender al grueso de la población, sin necesidad de actos de discriminación derivados de diversas condiciones obtenidas de su vida privada; lo que no sucede. De ahí, que consideramos que la capacidad de los gobiernos para contener la pandemia no sólo depende del uso de tecnología, sino de una capacidad sanitaria instalada y políticas efectivas implementadas con antelación, que hagan más efectivo el uso de la tecnología en pro de las personas, nunca para ubicar sus circunstancias para realizar algún tipo de depuración genocida, como ya ha sucedido en otros contextos en la historia de la humanidad.

La razón de estado ha cobrado mayor fuerza y se impone tratando de mantener un control, que actualmente ya no tenía del todo, y que a través de la tecnología y el manejo de los datos personales puede volver a tener; pero que debe aplicar en aras de preservar los derechos de los sectores más desprotegidos, como son los indigentes, los ancianos, los migrantes, y en general, la gente económicamente desfavorecida, quienes son los más afectados; que son víctimas de una serie de desventajas sociales y tecnológicas, que poco o nada les importan frente a la necesidad de supervivencia, ya ni que decir de sus datos personales, los cuales, tampoco resultan de gran atractivo para quien los comercia, pues no son del grueso de la población que implique un consumo importante, lo cual también se refleja en sus hábitos, que van dejando por ahí, sin que lo sepan. Al respecto, el gobierno debe evitar la tentación de manejar y manipular fuera de toda ética y buen gobierno, las bases de datos que se generen durante la pandemia, utilizándolas aplicando los principios rectores universales para la protección de datos personales y los derechos humanos, siempre ponderando la vida y particularmente aún más, la vida privada de las personas.

Cuando decidí escribir este artículo, me di cuenta de que había muchos temas técnicos sobre protección de datos personales sobre los cuales hablar. Pero la vulneración, en todos los casos que decidí abordar, resultó para mí el tema más evidente. La protección de los datos personales durante la crisis del coronavirus puso en evidencia lo vulnerable del derecho a la privacidad, no sólo en todos las formas y casos de los que he hablado; sino también para la población más vulnerable de todas, aparte de los grupos que ya mencioné, que es la que se quedó en casa, y no me refiero al hecho de que se contagie del virus; me refiero a una vulneración mayor de todos sus derechos, desde su libertad de tránsito hasta su derecho a la vida. En efecto, de inmediato, una vez iniciada la emergencia, surgió la necesidad de restringir nuestra vida privada, confinándonos a nuestra casa, en la que creímos estaba más resguardada nuestra vida privada, sin que ello sea así. Es dentro de nuestra casa, con el uso de la tecnología, que más expuestos estamos, pues si somos de la población afortunada que pudo quedarse en casa, estamos en todo momento ubicados y vigilados de que ahí permanecemos; el abasto para permanecer dentro, también nos ubica y comparte por todas partes nuestras necesidades más básicas, a través de todo tipo de aplicaciones y aparatos con que cuente nuestro hogar, aunado a los servicios que utilizamos, particularmente el internet, el cual ya se volvió más indispensable que el gas, pues si no hay gas, pedimos comida, e igual no nos bañamos, al final de cuentas ya nos conocieron en zoom; pero sin internet verdaderamente morimos en el mundo virtual.

La gran cantidad de información que las personas estamos generando desde nuestras casas se recopila por un sin número de agentes externos que la está perfilando, en la mayoría de los casos sin cuidar el deber de confidencialidad, tratando nuestra información de salud particularmente y nuestros hábitos de consumo, violentando los principios más elementales de la protección de datos, como ejemplo, el consentimiento, cual en situaciones de pandemia no es necesario requerir tratándose de autoridades. Tal vez esto, como ya lo referí en los demás casos, no sea la situación fundamental en este tema; pues aún resguardados en casa, lo prioritario es también sobrevivir; si bien el riesgo de contagio disminuye, no estamos exentos.

Por lo que, confinados o no, sobrevivir es el tema, y la privacidad desafortunadamente no la estamos considerando prioritaria, pues también dentro de casa surge la necesidad de conexión para mantener nuestros lazos afectivos, nuestros nexos sociales y laborales, así como satisfacer nuestras necesidades básicas, como comer e inclusive sexuales. Nunca como ahora, la práctica del sexting se ha intensificado ante la separación de las personas, o la pornografía con la finalidad de satisfacer necesidades sexuales o mitigar la soledad. La vida privada y nuestras costumbres, que solían permanecer en el rigor del hogar; con el confinamiento, se han exacerbado; ahora se ven expuestas en internet a través del uso de múltiples aplicaciones y plataformas. Las personas se muestran como son pues están en casa (no se peinan, no se bañan, usan otro tipo de ropa, etc.), evidencian sus espacios para exhibir o resguardar las condiciones en las que viven; exponen sus costumbres, lo que comen, sus mascotas, sus hobbies, se conectan para trabajar o asistir a clases, sin preocuparse de qué tan seguras son esas plataformas o aplicaciones o si sus video llamadas son o no seguras; es decir, confiadas de que están en casa, se siguen manejando a través de estas comunicaciones en un esquema de privacidad que está muy lejos de serlo. Siempre creímos que la casa es el lugar más seguro que nos resguarda, pero ello no es así. Con la tecnología, ahora nuestra casa es el sitio más expuesto.

La desventaja de todo esto es que, durante la pandemia nuestra información personal está siendo procesada de una manera que tampoco tiene precedente; y lo mayormente riesgoso es que, pasada la emergencia y el confinamiento, toda la información y este tipo de control por parte del gobierno y las empresas, no se podrá borrar, no obstante que utilicemos mecanismos de acceso, rectificación, cancelación u oposición; pues se quedará como una forma habitual e irá avanzando en el grado de incursión para conocer otro tipo de información, que hasta ahora creíamos protegido por la privacidad.

Es así que ante la amenaza de la pandemia y so pretexto de salvar vidas, hemos, sin darnos cuenta, permitido la intromisión desmedida de terceros, como renunciado a nuestra vida privada, de la misma manera que por salvaguardar nuestra vida, iremos renunciando al ejercicio de otros derechos, como el de tránsito, por la necesidad del confinamiento y las restricciones para ir saliendo; el de expresión, pues aceptamos las restricciones que nos imponen las aplicaciones con tal de usarlas; el acceso a la información y la protección de nuestros datos personales, el primero por aceptar como válido todo lo que nos llegue vía electrónica sin cuestionarlo; mientras que el segundo, por sacrificar nuestra información personal en aras de continuar teniendo una vida, en un contexto que necesariamente se torna digital, con virus y sin virus.

Nos corresponde a todos generar en el entorno global digital una vida segura, lo que sólo podemos hacer sin restricciones de gobierno ni de las empresas, con ejercicio libre, consciente e informado, aprendiendo a cuidarnos, a cuidar el planeta y a cuidar nuestros datos personales, porque detrás de cada dato hay una persona. Sin personas la tecnología no existiría. Sin tecnología ya no podemos subsistir. Pero lo más importante, sin planeta no existiría ninguno, aunque sin nosotros y sin tecnología si subsiste. Ahora que nos hemos confinado nos damos cuenta de que nos lo agradece floreciendo nuevamente. Florezcamos otra vez en un nuevo mundo y que esto sea el proceso de aprendizaje que nos retorne a la vida como mejores personas, conscientes de proteger nuestra información privada.

Deseo que lo aquí escrito, sirva para reflexionar un poco sobre lo sucedido, particularmente en el tema de datos personales frente a un entorno de emergencia sanitaria nunca visto, pues espero que cuando tengas en tus manos este texto, todo esto haya pasado y veamos esto como un episodio más de ciencia ficción que, como dije al principio, ni al más ingenioso escritor se le hubiera ocurrido.

Reflexiones sobre el reglamento general de protección de datos de la Unión europea y los "estándares" de la Red Iberoamericana de protección de datos y su impacto sobre las reformas, proyectos de reformas y nuevas leyes de protección de datos en Latinoamérica.

Oscar R. Puccinelli

Doctor en Derecho Constitucional, Facultad de Derecho de la Universidad Nacional de Buenos Aires. Doctor Honoris Causa, Universidad Privada Antonio Guillermo Urrelo, Cajamarca, Perú. Profesor adjunto de Derecho Constitucional I ("Derecho Constitucional del Poder") y Derecho Constitucional II ("Derecho Constitucional de la Libertad" -incluye Derechos Humanos y Derecho Procesal Constitucional-), en la Facultad de Derecho de la Universidad Nacional de Rosario. Profesor adjunto a cargo de la cátedra Derecho Procesal Constitucional y Trasnacional en la Facultad de Derecho de la Universidad Nacional de Rosario. Profesor en el Profesorado de Filosofía, Escuela Normal nº 2 de Rosario. Profesor Honorario de la Universidad Antenor Orrego, de Trujillo (Perú). Profesor Honorario de la Universidad Nacional de San Agustín de Arequipa (Perú). Profesor Honorario de la Universidad Nacional de Piura (Perú). Profesor Honorario de la Universidad Nacional de Huánuco (Perú). Profesor Visitante de las Universidades Libre de Cali (Colombia) y Nacional de Trujillo (Perú). Docente investigador categorizado ("C") en el año 1995, por la Universidad Nacional de Rosario, a los fines del Programa de Incentivos a los Docentes Investigadores, establecidos en el ámbito universitario nacional (Decreto 2427/93). Re categorizado (Categoría "III") por la Comisión Regional de Categorización de la Región Centro Este, el 11/6/99.

Juez de la Sala Segunda de la Cámara de Apelación en lo Civil y Comercial de Rosario, Santa Fe, Argentina, desde 2009. Vocal del Directorio de la Empresa Provincial de la Energía de Santa Fe, durante 2007. Conjuez de la Cámara Federal de Apelaciones de Rosario, desde 2007 hasta 2009. Miembro Titular de la Asociación Argentina de Derecho Constitucional. Vicepresidente del Instituto de Derecho Procesal Constitucional del Colegio de Abogados de Rosario hasta 2009. Miembro Pleno Fundador del Centro de Estudios de Administración Local "Profesor Dr. Alberto Arrue Gowland", desde noviembre de 2004. Miembro de la Comisión Directiva de la Organización No Gubernamental de extracción empresaria

"Trascender", desde su fundación, y titular de la Comisión de Políticas Públicas, período 2006 en adelante. Secretario del Centro Argentino de Derecho Procesal Constitucional, desde su fundación, en 1994. Vicepresidente del Comité para el Estudio y Difusión del Derecho en América Latina (CEDDAL) para el período 2003/5. Coordinador en la Argentina del Comité para el Estudio y Difusión del Derecho en América Latina (CEDDAL) para el período 2003/5. Miembro del Instituto de Derecho Público y Ciencia Política del Colegio de Abogados de Rosario.

Sumario: 1. Introducción. **2.** Los nuevos paradigmas de la protección de datos en el Reglamento (UE) 2016/679 ("Reglamento General de Protección de Datos"). **3.** La incorporación de los principios del RGPD en las regulaciones y propuestas regulatorias en Latinoamérica. **3.1**. Los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos". **3.2.** Los proyectos de reformas y las leyes nacionales aprobadas en Latinoamérica desde el comienzo de la discusión del RGPD. **3.3.** El proyecto de reforma a la ley argentina de protección de datos personales, elaborado en el marco del programa "Justicia 2020". **4.** Conclusiones.

1. Introducción

Mucha agua bajo el puente ha corrido desde que ya más de un siglo atrás, la Constitución de Weimar garantizara a todo funcionario en el art. 129 los derechos "a examinar su expediente personal" y a que no se asiente en éste los hechos que le sean desfavorables "sino después de haberle dado ocasión de justificarse respecto de ellos".

Aquella norma constitucional, tal como lo expresara Sota , constituyó el primer antecedente constitucional del derecho a conocer y controlar los datos personales asentados en sistemas de información (archivos, ficheros, registros, bases y bancos de datos, etc.), cuyo ejercicio permitía, según la misma regla, tutelar los derechos eventualmente afectados por tratamiento ilegal o ilegítimo de tales datos, ya que además previó que tales funcionarios debían contar con "un recurso contra la decisión disciplinaria que le afecte y la posibilidad de un procedimiento de revisión".

Esa primitiva y parcial regulación de lo que hoy conocemos como "derechos ARCO" (por Acceso, Rectificación, Cancelación y Oposición al tratamiento) evolucionará también en el país germano ya entrando al tramo final de ese mismo siglo, -luego de que Arpa net emergiera en Estados Unidos como la primitiva Internet y de que se dictaran la primera ley de protección de datos en el Landa de Hesse (Daten Schütz, de 1970) y la Ley Federal de Protección de Datos (Bundesdatenschutzgesetz, de 1977), cuando, a la par de la aparición de la World Wide Web, el Tribunal Constitucional Federal aludiera a la existencia de un "derecho a la autodeterminación informativa" (primero, en 1982, en la no tan conocida sentencia del "Microcenso" e inmediatamente después, en 1983. por la referida a la "ley del censo de la población").

Ya en este siglo, ese novel derecho también evolucionará y se consolidará como el nuevo y autónomo "derecho a la protección de los datos personales", al ser expresamente incorporado en la Carta de Derechos Fundamentales de la Unión Europea (aprobada en 2000 y entrada en vigor en 2009), ya emancipado del derecho al respeto de la vida privada y familiar (contenido en el art. 7), en el art. 8 de la Carta, que además de reconocer el derecho estipuló que los 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", concediendo a "toda persona" el derecho "a acceder a los datos recogidos que la conciernan y a su rectificación", ordenando finalmente que la tutela de estas normas quedará sujeta al control "de una autoridad independiente".

Más allá de este reconocimiento general, en el ámbito europeo fueron dictadas múltiples normas comunitarias, destacándose entre ellas como paradigmáticas el Convenio nº 108, del Consejo de Europa, "para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" de 1981; la 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" y la más reciente y potente, el 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)" en vigencia desde mayo de 2018, al que aludiremos de inmediato.

2. Los nuevos paradigmas de la protección de datos en el Reglamento (UE) 2016/679 ("Reglamento General de Protección de Datos")

El Reglamento (UE) 2016/679 ("Reglamento General de Protección de Datos") fue adoptado luego de un intenso proceso de elaboración participativa en el ámbito regional europeo, y responde a la necesidad de dar nuevas respuestas normativas a los avances tecnológicos habidos desde la aprobación de la Directiva 95/46, en especial por la aparición de la "web 2.0" (la web "participativa", donde se incorporan las redes sociales, la computación en la nube, la internet de las cosas y los datos masivos, entre otros nuevos fenómenos), cuyos acelerados desarrollos empezaron a reconfigurar la red hacia nuevos formatos, en concreto una web semántica ("web 3.0") que nos prepara para la etapa tal vez final de la "web 4.0" (la web "simbiótica", que se redimensionará permanentemente a partir de los desarrollos de la robótica, las nanotecnologías, la Inteligencia Artificial, etc.).

Puesto de modo sintético, este nuevo Reglamento, de cara a dichos avances, realiza una serie de modificaciones al marco normativo anterior vigente, cuyas más relevantes son las siguientes:

a. Se extiende subjetivamente de modo expreso el alcance de sus disposiciones a rlas personas responsables o encargadas del tratamiento de datos no establecidos en la Unión Europea que realicen tratamientos derivados de una oferta de bienes o servicios destinados a la ciudadanía de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento, quienes quedan sujetos a la norma y por ello deben designar representantes en la Unión Europea que actuarán como punto de contacto de las autoridades de supervisión y de la ciudadanía.

b. Sobre el principio del consentimiento para el tratamiento de los datos personales, se exige que sea libre, informado, específico e inequívoco (mediante una declaración de las personas interesadas o una acción positiva que indique el acuerdo, pero no puede deducirse del silencio o de la inacción) y además, para ciertos tratamientos (v.gr., los datos sensibles, cuyo listado se amplía a los datos genéticos y biométricos y a las infracciones y condenas penales, aunque no las administrativas), se exige que sea explícito y verificable. Se introducen reglas específicas sobre el consentimiento de los menores en los servicios de la sociedad de la información, quienes pueden prestarlos autónomamente a partir de los 16 años (aunque cada Estado puede rebajarlo a no menos de los 13 años de edad, y en esta dirección, v.gr., España lo fijó en 14 años). Dicho consentimiento además debe ser verificable y el aviso de privacidad debe estar redactado en un lenguaje que puedan entender.

c. Se agregan los principios de transparencia e información, por virtud de los cuales las políticas de privacidad y los avisos legales deben ser

más simples, inteligibles y completos, incluso a través de íconos normalizados. Por consecuencia, las empresas deben revisar sus avisos de privacidad, rediseñándolos en un lenguaje claro y conciso, la base legal para el tratamiento de los datos, los períodos de retención y el derecho de las personas interesadas de dirigir sus reclamaciones a las autoridades de protección de datos.

d. Se reconoce explícitamente derecho a la limitación del tratamiento, donde el titular del dato puede solicitar el bloqueo temporal del tratamiento de sus datos cuando existan controversias sobre su licitud, tal como en el caso argentino está previsto en la ley de protección de datos personales, al prever las medidas cautelares que pueden solicitarse dentro de un proceso de hábeas data.

e. Se incorporan dos nuevos derechos: el derecho al olvido (anteriormente reconocido por el Superior Tribunal de Justicia de la Unión Europea en el célebre caso "Costeja") y el derecho a la portabilidad de los datos, que implica la posibilidad de transferirlos en formatos interoperables, en concreto, que permitan su reutilización por parte la persona titular de los datos o de otra responsable.

f. Se adiciona además el principio de "responsabilidad demostrada" (accountability), que se traduce en los de prevención y actuación proactiva por parte de las personas responsables y encargadas del tratamiento, trasladándose a las organizaciones el deber de demostrar que cumple con tales exigencias. En la misma dirección, se promueve la utilización de sellos y certificaciones para acreditar la accountability y se limita la posibilidad de selección del encargado del tratamiento por parte del responsable del tratamiento, dado que deberá elegir alguno que aporte suficientes garantías de cumplimiento normativo.

g. Se agregan los principios de protección de datos desde el diseño y por defecto (hardware y software deben ser diseñados para proteger la privacidad ya desde el diseño mismo de los sistemas y aplicaciones, y, además, en las opciones que otorgan estas últimas al momento de la instalación, se debe ofrecer como primera opción la que más protege a la privacidad la persona. Se intenta garantizar así el cumplimiento de la norma desde el mismo momento en que se diseñe una empresa, producto, servicio o actividad que implique tratamiento de dato, como regla y desde el origen).

h. Se exige a las personas responsables y encargadas del tratamiento el mantenimiento de un registro de tratamientos como medio de control interno que sustituye a la obligación de inscribir los ficheros y se prevén garantías más estrictas y mecanismos de seguimiento respecto de las transferencias de datos fuera de la UE. También se los obliga a la realización de evaluaciones de impacto sobre la privacidad frente a nuevos tratamientos (donde se establezcan los riesgos específicos de tratar ciertos datos y se prevean medidas para mitigar o eliminar dichas amenazas) y al nombramiento de una persona delegada de protección de datos (DPO), interna o externa (un técnico similar al oficial de privacidad que voluntariamente tienen muchas empresas), quien deberá asistir a las organizaciones en el proceso de cumplimiento, actuando como un verdadero delegado de la autoridad de control). Se establece la obligación de notificación inmediata a la autoridad de control y en algunos casos a los titulares de datos acerca del acaecimiento de incidentes de seguridad, y se refuerzan las medidas de seguridad, que deben aplicarse considerando especialmente el tipo de tratamiento de que se trate, los costos de implantación o el riesgo que el tratamiento presenta para los derechos y libertades, y todas las organizaciones que tratan datos deben realizar un análisis de riesgo de sus tratamientos. Finalmente, en este aspecto, se destaca la promoción de códigos de conducta sectoriales y esquemas de certificación ante la autoridad de control.

i. Se fortalece el sistema de control institucional, creándose el sistema de "ventanilla única", de modo que las empresas multinacionales tendrán como interlocutora a una sola autoridad de control nacional, en concreto la del establecimiento principal de la entidad), y se concibe un procedimiento de cooperación entre autoridades de los países involucrados, de forma tal que un afectado puede dirigirse a su autoridad de control para que atienda a los reclamos contra responsables establecidos en varios Estados miembros o que, estando en uno, hagan tratamientos que afecten significativamente a la ciudadanía en varios. También se dispone que las denuncias podrán ser presentadas a través de asociaciones de personas y que pueden exigirse indemnizaciones de los daños y perjuicios derivados del tratamiento indebido de los datos personales.Se agrava, asimismo, el marco sancionatorio, previéndose multas severas a quienes violen las reglas emergentes del Reglamento (incluso si fueran Administraciones públicas, aunque cada Estado puede optar por excluirlas), para cuya graduación se puede considerar el volumen de negocios de la empresa que incurra en infracción a dichas normas (en concreto, las sanciones pueden llegar a 20 millones de Euros o el 4% de la facturación global anual). Por último, en cuanto a las controversias que puedan surgir entre las autoridades, se deriva su resolución al Comité Europeo de Protección de Datos (organismo integrado por los directores de todas las autoridades de protección de datos de la UE). La incorporación de los principios del RGPD en las regulaciones y propuestas regulatorias en Latinoamérica.

Desde que la primera propuesta del RGPD fuera puesta en discusión, diversos proyectos legislativos iniciados de este lado del Atlántico tomaron algunas de las novedades que por entonces se pretendían incorporar y por ello es factible encontrar normas que se adoptaron antes de que fuera aprobada la versión final del reglamento; entre su aprobación y su entrada en vigencia, y luego de su entrada en vigencia.

Entre tales normas, el documento más relevante por su impacto en la región fue aprobado en 2017 por la Red Iberoamericana de Protección de

Datos (RIPD), a modo de actualización de sus "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana", de 2006. La importancia de estos "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", dimana de la autoridad científica y política de su emisor, y de ser esencialmente el resultado de una elaboración participativa entre las autoridades de protección de datos de la región, las que, como es obvio, aplicarán en la práctica los criterios fijados en la norma, estén o no expresamente legislados, ya que de los contenidos básicos de todas las leyes iberoamericanas de protección de datos se pueden extraer las reglas consagradas en las directrices referidas.

La marcada simbiosis entre el RGPD y los Estándares de la RIPD han contribuido a cimentar diversos proyectos de reforma a leyes preexistentes de protección de datos (entre ellas, las iniciadas respecto de las leyes chilena de protección a la vida privada y argentina de protección de datos personales) e incluso inspirado a regulaciones nuevas (la Ley General de Protección de Datos en Posesión de Sujetos Obligados de México, de 2017 y la leyes brasileña y panameña de protección de datos, de 2018) y modificaciones de las existentes (la ley uruguaya de protección de datos), además de proyectos elaborados por otros países que todavía no cuentan con una ley de protección de datos, como es el caso de El Salvador.

3.1. Los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"

Esta regla de soft law fue aprobada por la RIPD el 20 de junio de 2017, en el marco del XV Encuentro Iberoamericano de Protección de Datos por (RIPD) y está precedida (al igual que el RGPD) de extensos considerandos, donde se destaca que existe una falta de armonización en los Estados Iberoamericanos respecto al reconocimiento, adopción, definición y desarrollo de las figuras, principios, derechos y procedimientos que dan contenido al derecho a la protección de datos personales en sus legislaciones nacionales, lo cual, sin duda, dificulta actualmente hacer frente a los nuevos retos y desafíos para la protección de este derecho derivados de la constante y vertiginosa evolución tecnológica y la globalización en diversos ámbitos (considerando 9). Esto justifica la adopción de estos estándares, máxime al ser apremiante, en el marco de una constante innovación tecnológica, la adopción de instrumentos regulatorios que garanticen, por una parte, la protección de las personas físicas con relación al tratamiento de sus datos personales y, por la otra, el libre flujo de los datos personales que actualmente constituyen la base para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital, sobre los cuales se erigen las economías de los Estados Iberoamericanos (considerando 10). Y en tal inteligencia, se acuerda garantizar un nivel alto de protección de los derechos y libertades de las personas físicas, que entre otras cuestiones, se requiere un nivel uniforme y elevado de protección de las personas físicas con respecto a su información personal que responda a las necesidades y exigencias actuales en un contexto global, con la finalidad de no establecer barreras a la libre circulación de los datos personales en los Estados Iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas (considerando 11).

Ya en la parcela dedicada a las reglas que constituyen esos estándares, los 45 estándares que trae la norma se encuentran divididos en diez capítulos, donde se tratan una serie de disposiciones generales (Capítulo I, compuesto por nueve estándares); los principios de la protección de los datos personales (Capítulo II, compuesto por catorce estándares); los derechos del titular de los datos (Capítulo III, compuesto por nueve estándares); los derechos y obligaciones del encargado de los tratamientos (Capítulo IV, compuesto por tres estándares); las reglas que rigen las transferencias internacionales de datos personales (Capítulo V, compuesto por un estándar); las medidas proactivas que deben adoptarse en el tratamiento de datos personales (Capítulo VI, compuesto de cinco estándares); lo referente a las autoridades de control (Capítulo VII, compuesto por un estándar); el régimen de reclamaciones y sanciones (Capítulo VIII, compuesto por un estándar); el derecho a la indemnización por el indebido tratamiento de los datos personales (Capítulo IX, compuesto por un estándar) y, finalmente, los mecanismos de cooperación internacional (Capítulo X, compuesto por un estándar).

En cuanto a las reglas del **Capítulo I**, cabe ponderar que en ellas se define el objeto de la adopción de los estándares, que tienden, por un lado, a la homogeneización y elevación del nivel de la protección de datos en la región a partir de la regulación de un conjunto de principios y derechos a desarrollar en las legislaciones nacionales de datos personales, y por el otro, a facilitar el flujo internacional de los datos personales, con fines de desarrollo social y económico.

Allí se actualizan las definiciones propias de las normas de protección de datos; se define los ámbitos de aplicación subjetivo (personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones), objetivo (el tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, con sus reglas y excepciones) y territorial (donde incluye no sólo a responsables y encargados establecidos en la región sino a otros cuando no estándolo, sus actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos,

o bien, estén relacionadas con el control de su comportamiento, entre otros supuestos); las excepciones generales al derecho a la protección de datos personales, donde alude a las limitaciones permisibles (por motivos de seguridad nacional, seguridad pública, salud pública, otras cuestiones de interés público y la protección de los derechos y las libertades de terceros), la necesidad de que éstas se adopten de manera expresa por una ley que debe cumplir una serie de requisitos específicos y deben ser necesarias, adecuadas y proporcionales en una sociedad democrática; las reglas sobre el tratamiento de datos personales de niñas, niños y adolescentes (donde se afirma su interés superior, así como la necesidad de promover en su formación académica, el uso responsable, adecuado y seguro de las tics y sus riesgos), y las reglas de tratamiento de datos personales de carácter sensible.

En el **Capítulo II** se regulan los principios aplicables al tratamiento de datos personales (legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad), donde se tratan los nueve supuestos de legitimación para el tratamiento (con las respectivas excepciones relativos a los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones); lo relativo a las condiciones para obtener el consentimiento y su revocabilidad, estipulando reglas especiales para la obtención del consentimiento de niñas, niños y adolescentes; la cuestión de las finalidades compatibles con tratamientos anteriores (donde se extiende la licitud a nuevos tratamientos en interés público con fines archivísticos, de investigación científica e histórica o con fines estadísticos); la habilitación a las legislaciones nacionales para establecer excepciones con respecto al plazo de conservación de los datos personales; la responsabilidad proactiva (a cuyo respecto sugiere una serie de medidas y procedimientos); las medidas de seguridad (para cuya adopción sugiere considerar ciertos factores e impone ciertas acciones, entre las cuales incluye a la notificación de vulneraciones a la seguridad a la autoridad de control y a los afectados, aspecto regulado con gran detalle).

En el **Capítulo III** al referir a los derechos ARCO (acceso, rectificación, cancelación y oposición, al que agrega el de portabilidad), autoriza el ejercicio del derecho de oposición cuando el titular de los datos tenga una razón legítima derivada de su situación particular o se trate de un tratamiento para mercadotecnia directa; establece el derecho a no ser objeto de decisiones automatizadas que afecten de manera significativa al titular (y para el caso en que estas decisiones sean legales, garantiza los derechos a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión), regula el derecho a la portabilidad de los datos personales (para que una copia de ellos se le entregue o se le transfiera a otro responsable cuando los datos se traten por vía electrónica o medios automatizados); regula el derecho a la limitación del tratamiento de los datos personales a su mero almacenamiento (tanto durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable, como en el caso en que los datos sean innecesarios para el responsable, pero sean necesarios para formular una reclamación); regula la forma de ejercicio de estos derechos, su limitación por motivos relacionados con intereses públicos y privados y el derecho a cuestionar ante la autoridad de control y, en su caso, ante instancias judiciales.

En el **Capítulo IV** regula lo referido a la figura del encargado de tratamiento (quien realiza los tratamientos sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo), la obligación de instrumentar la vinculación jurídica con el responsable con determinados recaudos y contenidos mínimos que detalla, y lo relativo a la subcontratación de servicios, también de manera instrumentada.

El **Capítulo V** aborda las reglas para las transferencias internacionales de datos personales, autorizando a realizarlas tanto al responsable como al encargado bajo determinadas condiciones que pueden ser exceptuadas cuando concurran razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

En el **Capítulo VI** se incluyen las medidas proactivas en el tratamiento de datos personales (las que promuevan el mejor cumplimiento de la legislación y coadyuven a fortalecer y elevar los controles de protección de datos personales implementados por el responsable), incluyendo entre ellas a la privacidad por diseño y privacidad por defecto (en los medios de tratamiento y en programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales), a la inclusión del oficial de protección de datos personales (cuando el responsable sea una autoridad pública; realice tratamientos que tengan por objeto una observación habitual y sistemática de la conducta del titular; cuando los tratamientos probablemente entrañen un alto riesgo para sus titulares (por su naturaleza, número, transferencias previstas, alcances, tecnologías utilizadas o finalidades); a la adhesión a mecanismos de autorregulación (para cuyo fin se sugiere desarrollar, entre otros, códigos deontológicos, sistemas de certificación y sellos de confianza), y a la realización de estudios de impacto previos al tratamiento de datos personales (cuando por su alcance, contexto o finalidades, sea probable que el tratamiento entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares).

El **Capítulo VII** se refiere a las autoridades de control y supervisión, y estipula que en cada Estado Iberoamericano deberá existir una o más con plena autonomía, que podrá ser unipersonal o pluripersonal, pero deberá contar con poderes suficientes y actuar con carácter imparcial e

independiente, sin recibir instrucciones ni aceptar influencias externas, directas o indirectas, debiendo sus miembros contar con la experiencia y aptitudes específicas, ser nombrados mediante un procedimiento transparente y removibles únicamente por causales graves. Sus decisiones deben quedar únicamente sujetas al control jurisdiccional.

En el **Capítulo VIII** se regula todo lo relacionado con el régimen de reclamaciones y de imposición de sanciones ante la autoridad de control; se reitera el derecho de los titulares de recurrir a la tutela judicial para hacer efectivos sus derechos, y se establece que la legislación debe indicar, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones, a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia.

El **Capítulo IX** reconoce el derecho de todo titular a ser indemnizado cuando hubiere sufrido daños y perjuicios como consecuencia de una violación de su derecho a la protección de datos personales, para lo cual el derecho interno debe señalar la autoridad competente, los plazos, requerimientos y términos a través de los cuales se indemnizará al afectado.

Finalmente, el **Capítulo X** refiere al establecimiento de mecanismos de cooperación internacional entre los Estados Iberoamericanos que faciliten la aplicación de las legislaciones nacionales aplicables en la materia, entre ellos, mecanismos de refuerzo de la asistencia y cooperación internacional; de asistencia en la notificación y remisión de reclamaciones, investigaciones, intercambio de información y la adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

3.2. Los proyectos de reformas y las leyes nacionales aprobadas en Latinoamérica desde el comienzo de la discusión del RGPD.

Como se dijo, a partir de 2016 comienzan a verificarse alineamientos nacionales a las reglas del RGPD. En ese año, en Perú, mediante Decreto Legislativo 1353 se creó la autoridad de control de la Ley de Transparencia y Acceso a la Información Pública y se reformó la ley de protección de datos personales, además de aprobarse la Directiva sobre Tratamiento y Protección de Datos Personales en el Poder Judicial, mediante Resolución administrativa 065-2016-CE-PJ, pero ninguna de estas normas incorporó novedades provenientes de las versiones previas al texto finalmente aprobado del RGPD. También en ese año, en Costa Rica se reformó el Reglamento de la Ley de Protección de Datos Personales mediante decreto ejecutivo n° 40008-JP, de 2016, donde puede observarse una reglamentación del derecho al olvido de una manera más precisa que la que se había adoptado en el decreto ejecutivo 37554-JP, de 2012. La regla tampoco puede imputarse a una aplicación directa del RGPD, precisamente porque la versión finalmente aprobada de éste limitó la regulación originalmente elaborada del derecho al olvido a una mera mención en el epígrafe del artículo que regula el derecho de supresión.

En enero de 2017, en México se aprobó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, una extensa norma de 168 artículos y ocho transitorios -que complementa la anterior Ley Federal de Protección de Datos Personales en Posesión de Particulares, aprobada en 2010-, donde se incorporaron diversas regulaciones alineadas con el RGPD, aunque debido a que su debate se inició antes de la aprobación del reglamento europeo, se basó en las primeras versiones del documento, que luego fue modificado. Así, por ejemplo, al regular el derecho a la portabilidad (art. 57) replicó la redacción anterior del reglamento, que luego fue acotado en este punto. Además, quedó incorporado para el ámbito público (el RGPD se refiere exclusivamente a los datos tratados por particulares y por ello mal podía extenderlo), aspecto que ha traído sus inconvenientes, pero que aparece como un avance legislativo auspicioso pues el derecho a la portabilidad de los datos debe regir tanto para los sistemas de información privados como para los públicos.

Ya en 2018, Chile reformó su Constitución mediante la ley 21.096, incorporando expresamente el derecho a la protección de los datos personales y disponiendo en concreto que el tratamiento y protección de esos datos debe realizarse conforme a la ley.

Esta reforma potenció la ya abundante actividad legislativa alrededor de esta temática -se presentaron medio centenar de proyectos- por lo cual se encuentra en discusión una reforma integral a la ley de protección de la vida privada (n° 19.628 de 1999). El proyecto actualmente en debate, alineado con el RGPD, endurece considerablemente el principio de finalidad, estandariza el principio de proporcionalidad, ensancha el principio de caducidad del dato, especifica con mayor precisión el principio de limitación de la recolección, mejora el principio de responsabilidad, detalla aún más el principio de seguridad, regula el de responsabilidad demostrada, incorpora el deber de reportar las vulneraciones de seguridad, agrega el principio de transparencia y de responsabilidad proactiva y actualiza los tipos de datos sensibles (biométricos, de perfil biológico, de geolocalización, de niños, niñas y adolescentes). También, en cuanto a los derechos de los titulares de

los datos, agrega a los derechos ARCO el de portabilidad (por lo que ahora los denomina "ARCOP"), cambia el régimen disciplinario y crea un sistema de tutela administrativa que recae en el Consejo para la Transparencia (que pasa a denominarse Consejo para la Transparencia y la Protección de Datos Personales).

También en 2018, Brasil -primer país en incorporar el hábeas data como una acción autónoma para la defensa de los datos personales en su Constitución de 1988- aprobó la ley 13709 (por la que se dispone sobre la protección de datos personales y se modifica la ley 12.965, de 2014 que estableció el "marco civil de Internet"), la cual, con vigencia desde 2020, constituye una verdadera Ley General de Protección de Datos.

Aunque la versión aprobada por el Congreso se alineaba con diversas características del RGPD, algunas de ellas, que se consideran centrales, fueron vetadas, como las que referían a la creación de una autoridad independiente de protección de datos; las sanciones aplicables y los requisitos de transparencia para los agentes del sector público. Posteriormente, mediante la ley nº 13.853, de 2019 se creó la Autoridade Nacional de Proteção de Dados ("ANPD"), órgano con competencia para regular sobre protección de datos y privacidad; interpretar administrativamente la LGPD, con carácter exclusivo y aun en los casos de silencio legal; solicitar información a responsables y encargados información sobre el tratamiento de los datos personales; supervisar el cumplimiento de la ley y aplicar las sanciones administrativas derivadas de violaciones a ésta; promover la protección de datos y la privacidad; realizar estudios sobre estas temáticas y asociarse con autoridades de otros países para optimizar la cooperación internacional.

También en 2018 en Uruguay, se aprobó la Ley de Rendición de Cuentas N°19.670, que entre sus arts. 37 y 40 incorporó importantes modificaciones a la normativa de protección de datos personales, alineando la legislación preexistente a algunas de las novedades emergentes del RGPD y de los Estándares de la RIPD.

Así, por ejemplo, amplió el ámbito de aplicación de la ley, que se extiende fuera de las fronteras del país cuando las actividades del tratamiento estén relacionadas con la oferta de bienes y servicios dirigidos a habitantes del Uruguay o involucren el análisis de su comportamiento, así como cuando así lo dispongan normas de derecho internacional o un contrato. También incorporó la obligación de notificar las vulneraciones de seguridad, así como las medidas adoptadas, tanto al titular de los datos como a la Unidad Reguladora y de Control de Datos Personales (URCDP), quien coordinará las acciones pertinentes con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy).

En cuanto al principio de responsabilidad, establece que tanto los responsables como los encargados de bases de datos deben adoptar las medidas técnicas y organizativas que correspondan (privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, etc.); se crea la figura del "delegado de protección de datos", con funciones de asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales; supervisar el cumplimiento y proponer las medidas pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia y actuar como nexo entre su entidad y la URCDP.

En el mismo año, en Argentina el Poder Ejecutivo nacional envió un proyecto de ley al Congreso de reforma integral a la ley 25.326 -en realidad se trata de una norma totalmente nueva-, en sintonía con el RGPD y los Estándares de la RIPD, aunque con algunas particularidades distintiva de tales normas. Nos referiremos a este proyecto por separado, en el apartado siguiente.

En 2019 Panamá aprobó la ley 81 sobre protección de datos personales, que previó entrar en vigencia en marzo de 2021. La regla, basada expresamente en los principios establecidos por el RGPD y los Estándares de la RIPD, se compone de 47 artículos, distribuidos en los siguientes siete capítulos: Disposiciones Generales (arts. 1 a 14); Derechos de los Titulares de Datos Personales (arts. 15 a 24); Utilización de datos personales (arts. 25 a 33); Consejo de Protección de Datos Personales (arts. 34 y 35); Responsabilidad por las infracciones (arts. 36 y 37); Infracciones y sanciones (arts. 38 a 43) y Disposiciones finales (arts. 44 a 47).

Entre las reglas que reflejan una influencia concreta del RGPD y los Estándares, se destacan los principios de proporcionalidad o minimización de los datos, seguridad y transparencia, la incorporación del derecho a la portabilidad y a no ser sometido a decisiones basadas únicamente en el tratamiento automatizado de los datos. La norma también reconoce el derecho a la tutela judicial y administrativa ante la autoridad de control, la ANTAI, ante quien se recurren las decisiones de la Dirección de Protección de Datos. Seguramente la reglamentación de la ley profundizará sus relaciones con el RGPD y los Estándares de la RIPD.

En 2019, en El Salvador, se iniciaron dos expedientes legislativos a los fines de adoptar una "ley de protección de datos personales y hábeas data", uno presentado por el Grupo Parlamentario ARENA, y otro por el FMLN, los cuales tienen como base el modelo europeo, el cual contiene los más altos estándares de protección de datos personales y se encontraba en discusión al momento de cierre de este trabajo.

3.3. El proyecto de reforma a la ley argentina de protección de datos personales, elaborado en el marco del programa "Justicia 2020"

En septiembre de 2018, el Poder Ejecutivo nacional envió al Congreso un proyecto de reforma a la ley de protección de datos vigente, el cual fue elaborado en el marco del programa "Justicia 2020", motorizado por el Ministerio de Justicia y Derechos Humanos de la Nación, en un esquema de elaboración participativa que incluyó una amplia convocatoria a nivel federal, y que de ser aprobado sin modificaciones sustanciales y entrar en vigencia, significaría un notorio avance aunque se adelantan desde aquí objeciones concretas respecto de la incorporación innecesaria de los capítulos referidos al "Registro No Llame" (ya que debería mantenerse en ley especial que lo regula) y del inadecuado diseño del control judicial y administrativo de la ley.

Ingresando brevemente a tales definiciones, en el listado se incorporan las de autoridad de control; base de datos (con sus históricos seudónimos: archivo, registro, fichero o banco de datos); datos personales (con una descripción acerca de su extensión y de qué debe entenderse por persona determinable; datos biométricos y datos genéticos); datos sensibles (asociados a los que afectan la esfera íntima de su titular con potencialidad de originar discriminación); disociación de datos; encargado del tratamiento; fuentes de acceso público (restricto e irrestricto); grupo económico; incidente de seguridad; responsable del tratamiento; tercero; titular de los datos; transferencia internacional y tratamiento de datos.

Así, en el art. 5, además de tratar los principios de licitud y lealtad en la recolección (ya contenidos en la ley 25.326), se agrega el principio de transparencia, expresamente regulado en el Reglamento General de Protección de datos europeo. Luego, en el art. 6 se refiere al principio de finalidad, ya previsto en la ley vigente, complementándolo, en el art. 7, con el principio de minimización de datos, recogiéndose, en definitiva, el principio de limitación en la recolección, pero con terminología actualizada a los parámetros del RGPD.

Los arts. 10 y 11 incorporan novedades interesantes. En concreto el primero de ellos se refiere al principio de responsabilidad proactiva, tomado del Reglamento General de Protección de Datos europeo, que hoy resulta central para la protección de los datos personales frente a los avances tecnológicos.

En el art. 16 se actualiza la regulación de los datos sensibles, con un detalle minucioso de los supuestos y condiciones en que quedan habilitadas las excepciones al principio general de prohibición de tratamiento sin consentimiento expreso del titular.

En el art. 18 se regula el tratamiento de datos de niños, niñas y adolescentes, en regla que recoge la preocupación especialmente existente en los ámbitos internacionales y que es recogida por las legislaciones más recientes. La norma parte de la necesidad de preservar, ante todo, el interés superior de estos sujetos de derechos, pero también tiene en cuenta sus intereses y por ello declara lícito el consentimiento que aquellos presten -en el marco de la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos- desde los 13 años de edad, requiriendo para el caso de los menores de esa edad, que aquél sea otorgado por el titular de la responsabilidad parental o tutela sobre el niño, el cual no puede ser entendido más allá de la medida en que se dio o autorizó. Se obliga además al responsable del tratamiento a "realizar esfuerzos razonables para verificar, en tales casos, que el consentimiento haya sido otorgado por el titular de la responsabilidad parental o tutela sobre el niño, niña o adolescente, teniendo en cuenta sus posibilidades para hacerlo", y en tal sentido existen diversas propuestas en el plano internacional de establecer mecanismos de verificación que incluyan la prestación de esos consentimientos por vía audiovisual.

Por su parte, el art. 20 resulta una incorporación muy valiosa por cuanto obliga a los responsables y encargados de tratamiento a notificar la ocurrencia de incidentes de seguridad que puedan afectar significativamente los derechos de los titulares de los datos, aunque el problema radica en qué puede entenderse por "afección significativa", aspecto sobre el cual adquiere suma relevancia el rol de legislador secundario del órgano de control. En concreto, la norma obliga a aquellos a notificar inmediatamente tanto al titular de los datos como a la autoridad de control la ocurrencia de tales incidentes (la norma alude a 72 horas para la notificación a la autoridad de control) y establece además, con claridad, el contenido que debe tener esa información (en concreto, la naturaleza del incidente; los datos personales que pueden estimarse comprometidos; las acciones correctivas realizadas de forma inmediata; las recomendaciones al titular de los datos acerca de las medidas que éste pueda adoptar para proteger sus intereses y los medios a disposición del titular de los datos para obtener mayor información al respecto).

Finalmente, el art. 26, luego de declarar lícita a la prestación del servicio de tratamiento de datos en el marco de medios tecnológicos tercerizados cuando dicho tratamiento garantice el cumplimiento de los principios y obligaciones establecidos en la ley, expresa que el responsable del tratamiento debe realizar esfuerzos razonables para elegir un proveedor de servicios que garantice dicho cumplimiento, para lo cual deberá considerar determinadas pautas que menciona , y dispone que el responsable del tratamiento responderá ante el titular de los

datos y ante la autoridad de control por incumplimientos del proveedor.

El art. 30 refiere a un derecho que no se previó expresamente como tal en la ley 25.326 y que sí está en las regulaciones más recientemente adoptadas en el derecho extranjero: el derecho de oposición al tratamiento de los datos,

El art. 31, al regular el derecho de supresión estipula que éste no procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información, pero se trata de una excepción que si bien es tomada literalmente del Reglamento Europeo resulta problemática, pues así redactada, bajo el amparo de esta excepción cualquiera podría argumentar que sigue tratando los datos ya que los necesita para informarse o expresarse. Una forma compatible de atender a esta libertad sería, v.gr., cerrar la frase mencionando que ello es así "en los casos y en la medida en que la actividad del responsable del tratamiento esté amparada por dichos derechos".

El art. 32 regula el derecho de impugnación de valoraciones personales automatizadas, extendiendo una regla ancestral que era exclusiva del ámbito público al ámbito privado -que actualmente es donde tienen mayor ámbito de aplicación-, ampliando sí, como se expresó, reglas típicas de las leyes de protección de la primera generación que se limitaban al ámbito público y reconocían sólo el derecho a no ser objeto de decisiones judiciales ni administrativas basadas exclusivamente en el tratamiento automatizado de datos.

Ahora se dice lisa y llanamente que el titular de los datos "tiene derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa", aunque tal derecho no es absoluto puesto que la regla trae sus excepciones, en concreto cuando tal tratamiento se base en su consentimiento expreso; esté autorizado por ley o sea necesario para la celebración o para la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento. De todos modos, aun en estos supuestos de excepción y salvo en el caso en que exista habilitación legal, estipula que "el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos del titular de los datos; como mínimo, el derecho a obtener intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión".

El art. 33, incorporando otro derecho contenido en el Reglamento Europeo, consagra al derecho a la portabilidad de los datos personales, que en el derecho argentino cuenta con un precedente en materia de telecomunicaciones. La norma dispone que en los casos en que se brinden servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización e incluso puede solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible. Asimismo establece que este derecho no procede cuando su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el responsable o encargado del tratamiento (excepción que debiera tener un límite ser temporal y no abarcar los tratamientos que se realicen luego de un tiempo de adaptación específico que debiera otorgarse para el cumplimiento de la ley); se vulnere la privacidad de otro titular de los datos; se afecten las obligaciones legales del responsable o encargado del tratamiento o se impida que el responsable del tratamiento proteja sus derechos, su seguridad o sus bienes, o los derechos, seguridad y bienes del encargado del tratamiento, o del titular de los datos o de un tercero.

El art. 35, al referirse al ejercicio abusivo de los derechos contenidos en este capítulo, más allá que pueda ser considerado como una reiteración innecesaria del art. 10 del Código Civil y Comercial, tiene aquí un formato y una finalidad específica evidentes porque refiere concretamente a los fines de la propia ley, a los límites impuestos por la buena fe y a la eventual imposición sobre el obligado de una carga técnica o financiera irrazonable. La norma resulta particularmente de utilidad para enfrentar acciones judiciales espurias que se han verificado en la deformada praxis tribunalicia, esto es, acciones articuladas sin base real para el reclamo por violación de los derechos sustanciales protegidos por la norma y con base en meros tecnicismos, incoadas con la sola finalidad de generar honorarios judiciales o extrajudiciales a favor de los abogados que realizaron tales reclamos sin base real alguna.

El art. 37 incorpora, en consonancia con las reglas más avanzadas del derecho extranjero, el principio de responsabilidad proactiva y alude a las medidas que deben adoptarse para el cumplimiento. Luego de indicar que tales medidas deben "ser proporcionales a las modalidades y finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear sobre los derechos de su titular", indica que éstas tienen que contemplar, como mínimo la adopción de procesos internos para lograr una mayor efectividad en la protección de datos; la implementación tanto de procedimientos para atender el ejercicio de los derechos de los titulares de los datos, como de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas. Finalmente, dispone que tales medidas "deben ser aplicadas de modo que permitan su demostración ante el requerimiento de la autoridad de control"

(ya que el criterio general de la ley es que los responsables y encargados son los que deben probar que sus tratamientos se ajustan a los parámetros de la ley) y que debe adoptarse "una política de privacidad o adherirse a mecanismos de autorregulación vinculantes, que serán valorados por la autoridad de control para verificar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

El art. 38 incluye otra novedad al incorporar, como también lo hace el RGPD, los Estándares de la RIPD y las legislaciones más recientes, los principios de protección de datos desde el diseño y por defecto (privacy by design y privacy by default), los cuales constituyen imprescindibles en un contexto tecnológico donde tanto el diseño de hardware como de software en sistemas que de un modo u otro tratan datos personales y la actividad de quienes prestan diversos servicios de la sociedad de la información tienen que estar diseñados para permitir un correcto tratamiento de la información personal y además prever, en las opciones que de manera predispuesta ofrecen al titular de los datos, las que mejor protegen la privacidad de éste pese a que no sea la que favorece al tratante al permitirle un mayor acceso a la información del titular.

La regla, en concreto, dispone que el responsable del tratamiento

"debe aplicar medidas tecnológicas y organizativas apropiadas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos" y que tales medidas **"deben ser adoptadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares".**

Agrega luego que dicho responsable del tratamiento debe aplicar tales medidas "con miras a garantizar que, por defecto, sólo sean objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento" y agrega que tal obligación "se aplica a la cantidad y calidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad", debiendo además tales medidas "garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención del titular de los datos, a un número indeterminado de personas humanas" (aquí la regla exagera en aclarar "personas humanas", siguiendo la idea de privar de toda protección a las personas jurídicas, pero literalmente interpretada la norma permitiría que la información fuera accesible por un número indeterminado de personas jurídicas, lo que resultaría contrario a los principios de la ley.

Entre los arts. 40 y 42 se incorpora y regula en detalle una nueva exigencia también derivada de las leyes más avanzadas, referida a la exigencia de contar, en determinados casos y con carácter previo al inicio de los tratamientos, con una evaluación de impacto relativa a la protección de datos personales.

El art. 40 dispone que en los casos en que un responsable del tratamiento prevea realizar algún tipo de tratamiento de datos "que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos", debe realizar tal evaluación de impacto "de manera previa a la implementación del tratamiento", siendo ésta obligatoria cuando así lo disponga la autoridad de control y además en los casos en que se esté frente a datos sensibles a gran escala; a datos de antecedentes penales o contravencionales y cuando se prevea la evaluación sistemática y exhaustiva de aspectos personales basadas en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o les afecten significativamente de modo similar.

El art. 41 detalla qué debe incluir, como mínimo, la evaluación de impacto, en concreto la descripción de las operaciones de tratamiento de datos previstas, los fines del tratamiento y -cuando proceda- el interés legítimo perseguido por el responsable del tratamiento; la evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad; la evaluación de los riesgos para los titulares de datos, y las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales, y los derechos e intereses legítimos de los titulares de los datos y de otras personas que pudieran verse potencialmente afectadas.

El art. 42 indica que el responsable del tratamiento debe informar a la autoridad de control antes de proceder al tratamiento de datos cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento de datos entrañaría un alto riesgo, y que éste debe incluir, como mínimo, además de la evaluación de impacto, información sobre las responsabilidades del responsable y de los encargados del tratamiento (en particular cuando el tratamiento de datos se da dentro de un mismo grupo económico); los fines y medios del tratamiento previsto y las medidas y garantías establecidas para proteger los datos personales de sus titulares, así como, en su caso, los datos de contacto del delegado de protección de datos. Finalmente, estipula que la autoridad de control deberá iniciar el procedimiento de verificación de oficio cuando considere que el tratamiento de datos previsto pueda infringir esta ley.

En este artículo también se incorporan reglas que se encuentran en las normas más recientes de protección de datos, exigiéndose la realización -previa a iniciar los tratamientos- de un estudio de impacto sobre los derechos de los titulares de los datos en diversos supuestos que se explicitan y en los cuales los tratamientos exponen a aquellos a situaciones de mayor riesgo (como cuando se elaboren perfiles, se traten datos sensibles a gran escala, se incluyan datos de niños, niñas o adolescentes o intervengan tecnologías potencialmente invasivas).

El art. 43 constituye otra innovación del proyecto a partir de la cual se incorpora la figura del delegado de protección de datos, que debe ser designado por los responsables y encargados del tratamiento en bases de datos del sector público o, en el ámbito privado, cuando se realice el "tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento" o se haga "tratamiento de datos a gran escala".

También su designación está prevista para los casos en que así lo disponga la autoridad de control o cuando "los responsables y encargados del tratamiento no se encuentren obligados a la designación de un delegado de protección de datos de acuerdo a lo previsto en este artículo, pero decidan designarlo de manera voluntaria".

La norma dispone asimismo la posibilidad de designar un delegado único cuando se trate "de una autoridad u organismo público con dependencias subordinadas", teniendo para ello "en consideración su tamaño y estructura organizativa". Y también prevé la figura del delegado único cuando se trate de un grupo económico, a condición que "esté en contacto permanente con cada establecimiento".

De similar modo expresa que "Las funciones del delegado de protección de datos pueden ser desempeñadas por un empleado del responsable o encargado del tratamiento o en el marco de un contrato de locación de servicios" -circunstancia que es asimilable a la vinculación entre responsables y encargados del tratamiento, ya que aquí también se exige la celebración de un contrato- y que el delegado "puede ejercer otras funciones siempre que no den lugar a conflictos de intereses".

Por último, la regla trae previsiones relativas a las calidades que necesariamente debe reunir todo delegado de protección de datos y a la independencia para ejercer el cargo, cuando expresa que "La designación del delegado de protección de datos debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones. En cualquier caso, el delegado debe ejercer sus funciones sin recibir instrucciones y sólo responde ante el más alto nivel jerárquico de la organización".

El art. 44 ya ingresa en el detalle de las funciones del delegado y le atribuye "sin perjuicio de otras que se le asignen especialmente", las de informar y asesorar a los responsables y encargados del tratamiento, así como a sus empleados, acerca de las obligaciones que les cabe en la normativa de protección de datos; promover y participar en el diseño y aplicación de una política de protección de datos que contemple los tratamientos de datos que realice el responsable o encargado del tratamiento; supervisar el cumplimiento de la ley y de la política de protección de datos de un organismo público, empresa o entidad privada; asignar responsabilidades, concientizar y formar al personal, y realizar auditorías; ofrecer asesoramiento para la evaluación de impacto cuando entrañe un alto riesgo de afectación para los derechos de los titulares de los datos, y supervisar luego su aplicación, y cooperar y actuar como referente ante la autoridad de control para cualquier consulta sobre el tratamiento de datos efectuado por el responsable o encargado del tratamiento.

Finalmente, el art. 45 se ocupa de los mecanismos de autorregulación vinculantes, actualizándose las reglas sobre autorregulación que en la ley 25.326 se limitaban a los códigos de conducta pero que ahora se extiende también a las normas corporativas.

Conclusiones

La nueva y compleja regulación adoptada por la Unión Europea, así como los Estándares de la RIPD han planteado exigencias muy altas para quienes tratan datos personales y para las autoridades de control, pues está concebida a fin de asegurar, a través de novedosas herramientas, la máxima vigencia posible del derecho a la protección de datos personales y de los derechos que éste está destinado a tutelar (en los hechos, todos los derechos fundamentales pueden ser afectados por el tratamiento indebido de los datos personales),

La exportación de estos criterios al ámbito Latinoamericano ya se ha iniciado, y tiempo más, tiempo menos, aparece casi inevitable, porque la problemática tecnológica y los derechos a proteger son análogos, y todos esos nuevos principios, derechos y obligaciones han sido objeto de largos y profundos debates tanto institucionales como académicos (y hasta judiciales) que lo han consolidado fuertemente. Desde luego, algunos aspectos, como el derecho al olvido, o el modelo de autoridad de control, no han tenido uniforme recepción en las distintas latitudes del continente americano y están sujetos a un intenso debate.

Será cuestión de tiempo, pero cierto es que las iniciativas legislativas presentadas a partir de 2016 han ido incorporando estas reglas, por lo que es de esperar que rápidamente se consolide, de este lado del Atlántico, una nueva generación de leyes de protección de datos que estén a la altura de los acontecimientos tecnológicos y permita a sus habitantes gozar plenamente de sus derechos, sin interferencias perjudiciales derivadas del uso indebido de sus datos personales.

Entrevista a Elizabeth Denham

Entrevista a Elizabeth Denham[1], presidenta de la Asamblea Global de Privacidad[2]

It has been a busy year for the Global Privacy Assembly, from the conference in Tirana, Albania to a name change from the International Conference of Data Protection and Privacy Commissioners. Tell us about the conference first of all. What were the key topics discussed?

Yes, it was a busy year! The conference in Tirana last year was one of the most defining in our organisation's 40 year history.

We adopted a policy strategy that set out a clear vision for our organisation for the next two years on what practical issues and actions the GPA will turn its collective attention to in order to make real progress. It is a strategy that tells a shared story.

We want to be a group that not only shares best practice, but shares policy work and even information on investigations of mutual concern, reflecting a regulatory environment that is increasingly international. And we want to have a stronger collective voice to answer data protection questions around how new technologies and approaches to data use impact citizens.

It is a bold approach, but the diversity of support in Tirana showed the global awareness of the need for action.

On top of that policy strategy work, we also had practical discussions on AI including outside experts in the field, and adopted resolutions that showed an appreciation of what complex legal and ethical issues mean for people in their everyday lives, including the interrelationship of privacy with other fundamental rights and the value of regulatory cooperation with consumer protection and competition authorities.

And of course we agreed our new name and logo.

What was the motivation for the name change to Global Privacy Assembly?

Data protection and privacy is now too great an issue for its regulatory community to only have a role once a year at a conference, which the previous name suggested. The priorities we agreed in Tirana strengthened the Assembly's position as an effective and influential international forum, and the new name reflects that. The Global Privacy Assembly brand marks our commitment to be a group that supports one another year round, sharing knowledge and building stronger cooperation.

How has that work continued since the conference?

A key way the Global Privacy Assembly continues its work throughout the year is through the working groups, which cover topic areas of key concern, such as the link between data protection and other fundamental rights, and allow groups of interested member authorities to concentrate on the most significant initiatives identified by the membership at our conference. The working groups then report back to the main annual conference, and their reports are key to moving forward the GPA's collective approach to those topics.

We now have a new Policy Strategy Working Group to support the work plan arising from the policy strategy adopted in Tirana, as well as other working groups focused on AI, international enforcement cooperation, digital education, data protection metrics and digital citizens and consumers. We are also looking to develop the GPA further as an influential and active body all year round by engaging in a coordinated manner with relevant regional forums and events where GPA members hold observer membership.

Of course, we also have to be adaptive to the world around us, and the GPA's leadership has been focused more recently on supporting authorities and commissioners through the COVID-19 pandemic.

1. Elizabeth Denham fue nombrada Comisionada de Información del Reino Unido en julio de 2016, habiendo ocupado anteriormente el cargo de Comisionada de Información y Privacidad para Columbia Británica, Canadá y Comisionada Asistente de Privacidad de Canadá. Más información en ico.org.uk
2. La entrevista fue realizada en el mes de junio de 2020.

What's been the focus of that coronavirus work?

The pandemic brings unprecedented challenges, and privacy is central to many of those, from how health data is shared to work around contact tracing apps. Authorities around the world are facing similar challenges.

The GPA is playing a role in supporting members, reiterating that data protection laws allow for safe data sharing and pragmatic approaches to protection of privacy in a situation of immediate public health concern.

As GPA members, we can pool our expertise on key issues, like we did when we organised a joint workshop with the OECD, which brought together more than 250 commissioners, government representatives, and privacy professionals to discuss the key current issues of COVID-19 and data protection.

And the GPA can act as a forum to share best practice: we are already sharing our policies and statements, and have set up a Taskforce that can extend this work.

Sadly, the pandemic also means we have had to postpone our annual gathering, in Mexico City, until 2021. Our ability to gather internationally is limited by this pandemic, but our determination to keep the momentum around our work is not. The GPA has never been more important, and we will continue to lead the debate and bring privacy authorities together for the essential elements of our annual conference at a virtual closed session later this year.

You talked about authorities facing similar challenges, but across different legal regimes. Do you think convergence on national and regional data protection laws is likely in the future, and how would that work?

I think we all know and accept that the digital economy has made the work of a data protection authority international. When people download apps or visit websites, they expect their information to be protected without having to check what country the service is based in. That places an expectation on authorities to find ways to act beyond their own national borders to keep their citizens' data safe.

And we are definitely seeing a growing level of baseline data protection standards internationally, with more and more countries developing laws that require organisations to be accountable for what they do with people's data. That has to be a positive step.

The next step is how those laws could work together. The argument here is not for uniformity in national laws - we must respect our legal and cultural differences - but instead to find practical ways to bridge those differences.

Bridging those differences could help businesses by providing transfer mechanisms to let data flow around the world, and it could reassure citizens that they can trust they have legal protections wherever their data may flow.

The GPA can continue to play a role as a facilitator for cooperation between its members.

Dictámenes de interés

Dictamen N° 1/019, de 15 de enero de 2019

Consulta efectuada por el Instituto Nacional de Inclusión Social (INISA), acerca del procedimiento de intercambio de información entre Entidades Públicas.

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

DICTAMEN N°	1	2019
Expediente N°	2018-2-10-000544	

Montevideo, 15 de enero de 2019

VISTO: La consulta realizada por el Instituto Nacional de Inclusión Social (INISA).

RESULTANDO:

I. Que zel INISA consulta sobre un procedimiento de intercambio de información entre Entidades Públicas. Expresa que, en el marco de la ejecución de convenios entre el Instituto Nacional de la Juventud, el INISA y el Ministerio de Desarrollo Social, se le ha solicitado información de las bases de datos referida a la comisión de infracciones a la ley penal de determinadas personas, a los efectos de que éstas sean atendidas por un programa del MIDES sobre reinserción social.

II. Que, a los efectos de complementar la consulta, se solicitó a INISA que agregara toda la documentación existente relacionada con el tema, lo cual fue cumplido en tiempo y forma.

III. Que dentro de la información aportada se encuentra detallada el tipo de datos solicitados: cédulas de identidad, ID del evento, fecha de evento, tipo de delito, rol en la infracción, detalle de la infracción y tipo de medida adoptada. Asimismo, cabe indicar la existencia de un Acuerdo de trabajo con el MIDES para la construcción de un observatorio sobre adolescentes en conflicto con la Ley para la construcción de información técnica en la materia. Y la existencia de un convenio entre MIDES, INJU; INAU e INISA con la finalidad de fortalecer la articulación interinstitucional entre los organismos para abordar la situación de egreso de adolescentes y jóvenes del sistema penal adolescente.

CONSIDERANDO:

I. Que la presente consulta refiere a un intercambio de información privada entre Entidades Públicas. Que el intercambio de información está regulado en los artículos 157 a 160 de la Ley N° 18.719, de 27 de diciembre de 2010, indicando que se deberá promover el intercambio de información o privada autorizada por su titular. Estas mismas normas establecen los principios, el procedimiento y las competencias de AGESIC en este ámbito. Que, por su parte, el artículo 3° del Decreto N° 178/013, de 25 de julio de 2013, reglamentario de la citada norma, establece que cuando se trata de información privada debe estarse a lo establecido en la Ley N° 18.331, de 11 de agosto de 2008.

II. Que, desde la perspectiva de la protección de datos personales, se está ante una comunicación de datos de acuerdo con el artículo 4° literal b) de la Ley N° 18.331. Que, en este marco, el artículo 17 de la misma norma establece que solo se puede comunicar datos personales para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, y con el previo consentimiento del titular.

III. Que el INISA, conforme con lo establecido en la Ley N° 19.367, de 31 de diciembre de 2005, tiene como objetivo la inserción social y comunitaria de los adolescentes en conflicto con la ley penal. Que, por su parte, la Dirección Nacional de Evaluación y Monitoreo del Ministerio de Desarrollo Social tiene como misión ejercer la rectoría en el monitoreo y evaluación de planes, programas, acciones, dispositivos y proyectos sociales en territorio nacional, así como su diseño y gestión. Por otro lado, el INJU es el responsable de las políticas sociales nacionales, así como de su coordinación, articulación, seguimiento, supervisión y evaluación de los planes, programas y proyectos relacionados con el desarrollo social. Por último, el INAU es el órgano rector en lo que hace relación con las políticas destinadas a promover y proteger a los adolescentes.

IV. Que, en virtud de lo expresado, existe tanto interés legítimo del emisor como del destinatario para intercambiar información, cuya clara finalidad es brindar políticas sociales tendientes a la reinserción social de los infractores menores de edad. Que en cuanto al consentimiento aplica el artículo 9° de la Ley N° 18.331, por el cual no sería necesario recabarlo por tratarse de funciones propias de los organismos y es información necesaria para el cumplimiento de las funciones legalmente establecidas a cada uno de ellos.

V. Que en cuanto a la consulta relativa a que los datos de la comisión de infracciones penales corresponde considerarlos como datos sensibles, cabe indicar que no se pueden considerar como tales en virtud de que el artículo 4° literal e) de la Ley N 18.331 establece un elenco taxativo que no los incluye. Que si deben ser considerados datos especialmente protegidos por ser una categoría de incluidos dentro del Capítulo IV de la Ley que los regula.

VI. Que el INISA cuestiona si está autorizada a comunicar datos personales relativos a la comisión de infracciones a INJU -MIDES tomando en consideración lo dispuesto en el artículo 18 inciso 3° de la Ley N° 18.331. Que, a esos efectos, el artículo 96 del Código de la Niñez y la Adolescencia establece la reserva respecto a los medios de comunicación. El artículo 97 del mismo cuerpo normativo regula la reserva del proceso y el artículo 221 refiere a que el INAU será el custodio de la información contenida en el Sistema Nacional de Información sobre Niñez y Adolescencia por lo que se debe garantizar el uso reservado y confidencial de los datos personales. En base a ello, los organismos están habilitados a comunicar la información, pero el tratamiento debe ser confidencial y exclusivamente para las finalidades legalmente impuestas no siendo posible su difusión a terceros.

ATENTO: a lo expuesto y establecido por el artículo 72 de la Constitución de la República, artículos 28, 29 y 31 de la Ley N° 18.331.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Indicar que resultan de aplicación los artículos 157 a 160 de la Ley N° 18.719, de 27 de diciembre de 2010 así como su decreto reglamentario N° 178/013, así como las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008.

2) Establecer que es posible el intercambio de información en virtud del marco normativo aplicable por el cual se le atribuyen competencias suficientes a las Entidades Públicas intervinientes, así como la existencia de convenios entre las partes que establecen los objetos de intercambio.

3) Que los datos relativos a las infracciones penales no son datos sensibles, pero si especialmente protegidos por estar dentro del régimen del artículo 18 de la Ley N° 18.331. Que a su respecto debe tenerse en cuenta que la información puede ser intercambiada en forma confidencial, sin revelarse a terceros por ser conveniente según decisión adoptadas por las Entidades participantes.

4) Notifíquese y publíquese

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 2/019, de 12 de marzo de 2019

Consulta remitida por la Dirección Nacional de Aduanas con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016, por el que se faculta a esta Dirección a publicar, entre otra, información de nombres de los importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen de destino de las mercaderías.

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

DICTAMEN N°	2	2019
Acta N°	3	2019

Montevideo, 12 de marzo de 2019

VISTO: La consulta recibida de la Dirección Nacional de Aduanas (en adelante DNA) con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016.

RESULTANDO:

Que por la Ley mencionada-artículo 43- se faculta a la Dirección Nacional de Aduanas a publicar, entre otra, información de nombres de importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen y de destino.

CONSIDERANDO:

I. Que, desde la perspectiva de la protección de datos personales, toda revelación de información personal a una persona distinta del titular se configura en una comunicación de datos, regulada expresamente por el artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008. Las hipótesis en las que la comunicación de datos puede realizarse en legal forma se encuentran reguladas en este artículo y en el artículo 9°, por remisión del primero.

II. Que esta Unidad ya se ha pronunciado en dictamen N° 27/013, de 8 de agosto de 2013, N° 1/015 y N° 3/015, ambos del 4 de marzo de 2015. En el punto vinculado a la comunicación de datos de despachantes de aduanas a entidades públicas en el último de esos dictámenes, se expresó que la DNA se encuentra facultada para recolectar y comunicar datos a otros organismos públicos en el cumplimiento de sus funciones, sin requerir para ello del consentimiento de los involucrados, atento a lo establecido en los artículos 9 literal B y 17 literales A y B de la Ley N° 18.331. Con respecto a restantes comunicaciones de datos, ella corresponde según el apartado 1 del dictamen N° 27/013, sólo con el previo consentimiento o luego de la aplicación de mecanismos de disociación, o en su defecto, habilitando la publicación de los datos expresamente mencionados en el literal C del artículo 9° en formato de listado. Esto es reiterado en el dictamen N° 3/015.

III. Que el análisis de pertinencia previo a la comunicación debe realizarse de acuerdo con los principios establecidos en los artículos 6° a 12 de la Ley Nº 18.331, en especial el de finalidad, los cuales deben orientar todo tratamiento de datos, teniendo presente que el derecho a la protección de datos personales es un derecho inherente a la personalidad humana (artículos 1° de esa Ley y 72 de la Constitución).

IV. Que en este caso existe una autorización legal para la publicación de la información -siendo de aplicación de lo dispuesto en el artículo 9° literal B por remisión del artículo 17 literal B de la ley citada-, sin perjuicio de lo cual, toda publicación de datos personales -sobre todo si es realizada en internet-, debe basarse en determinados principios y emplear técnicas que mitiguen los impactos eventuales en los derechos de los titulares de esos datos (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).

ATENTO: A lo expuesto,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Señalar que la comunicación de datos personales referida por la consultante se encuentra habilitada por ley (artículo 17 literal B y artículo 9° literal B de la Ley N° 18.331, de 11 de agosto de 2008), sin perjuicio de que en forma previa a la publicación, la DIRECCIÓN NACIONAL DE ADUANAS deberá realizar un ejercicio de ponderación de derechos, empleando para ello los criterios recomendados por los dictámenes Nº 12/012 de 7 de junio de 2012, 2/014 de 13 de febrero de 2014 y las Resoluciones Nº 1040/012 de 20 de diciembre de 2012 y 6/016 de 9 de marzo de 2012, entre otras.

2) Comuníquese, publíquese y archívese.

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 3/019, de 26 de marzo de 2019

Consulta efectuada por el Área Programática de Adolescencia y Juventud del Ministerio de Salud Pública, acerca de la posibilidad de acceder por la Mesa de Coordinación de Estrategia Territorial y Nacional de Prevención de Embarazo no Intencional en Adolescentes, a los datos necesarios para cumplir con sus objetivos.

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

DICTAMEN N°	**3**	**2019**
Expediente N°	**2018-2-10-000777**	

Montevideo, 26 marzo de 2019

VISTO: La consulta realizada por el Área Programática de Adolescencia y Juventud del Ministerio de Salud Pública.

RESULTANDO:

I. Que se requiere la opinión de esta Unidad sobre la posibilidad de acceder por parte de la Mesa de coordinación de la estrategia intersectorial y nacional de prevención del embarazo no intencional en adolescentes, a los datos necesarios para cumplir con sus objetivos.

II. Que la Estrategia es una iniciativa impulsada por los Ministerios de Salud Pública, Desarrollo Social, Educación y Cultura, la Oficina de Planeamiento y Presupuesto, la Administración Nacional de Educación Pública, el Instituto del Niño y Adolescente del Uruguay y la Administración de los Servicios de Salud del Estado, con el apoyo del Núcleo Interdisciplinario Adolescencia, Salud y Derechos Sexuales y Reproductivos de la Universidad de la República y del Fondo de Población de las Naciones Unidas.

III. Que la Mesa necesita para cumplir con sus objetivos, acceder a información nominada de los adolescentes de acuerdo con los indicadores de riesgo identificados y plasmados en el documento de la estrategia, a la información identificadora de las adolescentes que están cursando un embarazo, y a las adolescentes madres, entre otros. Los datos y registros se encuentran dispersos en diferentes sistemas de información de cada una de las sectoriales que integran la estrategia y en otros organismos públicos.

CONSIDERANDO:

I. Que la consulta versa sobre la posibilidad de realizar comunicación de datos personales entre distintas Entidades Públicas por lo que resulta de plena aplicación las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, sus concordantes y modificativas

II. Que según el artículo 4° literal b) de la citada Ley N° 18.331, se entiende la comunicación de datos como toda revelación de datos realizada a una persona distinta del titular de los datos. Por su parte, el artículo 17 de la misma norma establece que los datos personales sólo podrán ser comunicados "para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario (...)".

III. Que es necesario indicar la vigencia de numerosos tratados internacionales en nuestro país relacionados con los Derechos Humanos, así como una serie importante de normas relacionadas con la salud sexual y reproductiva en los adolescentes desde distintos enfoques, los cuales fueron oportunamente mencionados en el informe que luce en el presente expediente.

IV. Que además cada una de las Entidades involucradas tiene diversas competencias legales que le permiten tener registros de adolescentes en las distintas condiciones mencionadas. En el caso del Ministerio de Salud Pública cuando hace referencia al Área Programática de adolescencia y juventud, el Ministerio de Desarrollo Social cunado hace referencia a formular, ejecutar, supervisar, coordinar, programar, dar seguimiento y evaluar las políticas, estrategias y planes en las áreas de juventud, mujer y familia, adultos mayores, discapacitados y desarrollo social en general; y a diseñar, organizar y operar un sistema de información social con indicadores relevantes sobre los grupos poblacionales en situaciones de vulnerabilidad, que permita la adecuada localización del conjunto de políticas y programas sociales nacionales. Que ASSE posee competencias en cuanto a los datos de salud de las adolescentes embarazadas y que también cuenta con cometidos relacionados con adolescentes en materia educativa el Ministerio de Educación y Cultura, así como la Administración Nacional de Educación Pública.

V. Que surge probada la existencia de interés legítimo del emisor y del destinatario para realizar la comunicación de datos. Sin perjuicio de ello, se debe tener en cuenta que el artículo 12 de la Ley N° 18.331, de 11 de agosto de 2008, con la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, indica que el responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de las disposiciones de la Ley. Que, por tanto, se requiere que una de las Entidades involucradas sea la encargada de adoptar todas las medidas necesarias para cumplir con la normativa de protección de datos personales. Que en forma complementara, las distintas Entidades están cumpliendo competencias legalmente establecidas

VI. Que resulta necesario indicar que son aplicables los artículos 157 a 160 de la Ley N° 18.719, por las cuales se regula el intercambio de información entre Entidades Públicas. Como en el caso se va a intercambiar información privada se deben tomar en cuenta las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, modificativas y concordantes y que se consideran interés que se establezcan los mecanismos o condiciones de éste.

ATENTO: a lo expuesto y establecido por el artículo 72 de la Constitución de la República, artículos 28, 29 y 31 de la Ley N° 18.331.

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Indicar que la comunicación de datos a realizar se considera legítima y cumple con los requisitos establecidos en el artículo 17 de la Ley N° 18.331.

2) Que es necesario que una de las Entidades Públicas sea designada responsable a los efectos de cumplir la normativa de protección de datos personales.

3) Que es necesario tener en cuenta los artículos 157 a 160 de la Ley N° 18.719 en cuanto a la conveniencia de firmar acuerdos de intercambio de información

4) NOTIFÍQUESE Y PUBLÍQUESE

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 4/019, de 2 de abril de 2018

Consulta realizada por la Dra. Virginia Cervieri, por sí y en representación de Estudio Jurídico Cervieri Monsuárez Asociados, acerca de la publicación de informaciones que entiende falsas a través de páginas web paraguayas, a las que es posible acceder desde Uruguay, y que han sido replicadas por medios noticiosos nacionales.

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

DICTAMEN **N°**	4	2019
Expediente N°	2018-2-10-000129	

Montevideo, 3 de abril de 2019

VISTO: La consulta realizada por la Dra. Virginia CERVIERI, por sí y en representación de ESTUDIO JURÍDICO CERVIERI MONSUAREZ ASOCIADOS.

RESULTANDO:

I. Que se requiere opinión de esta Unidad sobre la publicación de informaciones que entiende falsas a través de páginas web paraguayas, a las que es posible acceder desde nuestro país, y que han sido replicadas por medios noticiosos en Uruguay. Adjunta medios probatorios de sus dichos.

II. Que se plantean además cuestiones vinculadas al alcance territorial de la normativa nacional y la aplicación del denominado "derecho al olvido".

CONSIDERANDO:

I. Que el artículo 3° de la Ley N° 18.331, de 11 de agosto de 2008 prevé que "(...) será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado". El artículo 12° establece que el responsable de la base de datos es responsable por el cumplimiento de la Ley, sin perjuicio de la responsabilidad que le cabe a los encargados de tratamiento (resolución N° 104/2015, de 23 de diciembre de 2015, Considerando V, entre otros).

II. Que el llamado "derecho al olvido" no posee consagración a nivel nacional, siendo una extensión del derecho de supresión y actualización, en el marco de los principios de finalidad y veracidad consagrados en las normas que regulan la protección de datos personales (artículos 7, 8, 14 y 15 de la Ley Nº 18.331, de 11 de agosto de 2008).

III. Que la Resolución Nº 1040/012 de 20 de diciembre de 2012 propuso soluciones técnicas para evitar la indexación de contenidos e inclusión en el caché de los buscadores y recomendó la aplicación de criterios técnicos para la publicación de contenidos en sitios web. A su vez, el Dictamen Nº 2/014 de 13 de febrero de 2014 señala que es el responsable del contenido del sitio web, quien decida la información a ser publicada, y por cuánto tiempo, al igual que los controles o filtros para evitar la indexación por los motores de búsqueda. Ello fue reiterado en la Resolución Nº 6/016 de 9 de marzo de 2016.

IV. Que en el dictamen N° 17/2016 se señala 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".

ATENTO: a lo expuesto e informado,

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) En la situación planteada la consultante podrá dirigir el ejercicio de sus derechos ante

2) los responsables o los encargados de

3) tratamiento -incluyendo los motores de búsqueda-, fundado en los artículos 14 y 15 de la Ley N° 18.331, de 11 de agosto de 2008, y en caso de denegación o limitación de sus derechos, plantear la denuncia ante esta Unidad o ante el Poder Judicial en el marco de lo dispuesto en los artículos 34 y 37 y siguientes de la referida Ley.

4) NOTIFÍQUESE Y PUBLÍQUESE

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 5/019, de 23 de abril de 2019

Consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones (URSEC) acerca de la legalidad que un operador de televisión para abonados del interior del país, coloque cámaras en la vía pública y transmita en vivo durante las 24 horas a través de su canal local.

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

DICTAMEN N°	**5**	**2019**
EXPEDIENTE N°	**2019-2-10-0000002**	

Montevideo, 23 de abril de 2019.

VISTO: La consulta remitida por la Unidad Reguladora de Servicios de Comunicaciones (URSEC).

RESULTANDO: Que específicamente se solicita dictamen en referencia a la consulta que le fuera realizada respecto a la legalidad o no de que un operador de televisión para abonados del interior del país -que identifica-, coloque cámaras en la vía pública y trasmita en vivo durante las 24 horas a través de su canal local.

CONSIDERANDO:

I. Que conforme al art. 4° "D" de la Ley Nº 18.331, de 11 de agosto de 2008 (LPDP), dato personal es toda información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, lo que incluye la imagen.

II. Que el Dictamen N° 10/010, de 16 de abril de 2010 indica que la video vigilancia "es toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo y esas imágenes constituyen información personal y por tanto será de aplicación la LPDP y sus normas complementarias."

III. Que la sola reproducción en tiempo real de imágenes captadas por las cámaras supone un tratamiento de datos personales, entendida este como "operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias" (art. 4° "M" de LPDP).

IV. Que la actuación de las personas se encuentra regida por el principio de libertad consagrado en los arts. 7° y 10 de la Constitución, por lo que la limitación al ejercicio de los derechos está dada por leyes establecidas por razones de interés general. La limitación a la colocación de las cámaras, lo está por los requisitos establecidos por la LPDP, en especial los principios que ella explicita.

V. Que la colocación de cámaras de video vigilancia con fines de seguridad pública está atribuida al Ministerio del Interior, y en el caso de contralor del tránsito y policía de espacios públicos, a los Gobiernos Departamentales específicamente como cometidos de la Intendencia, según art. 35 numeral 25 la Ley N° 9.515, en cuanto a la organización y cuidado de la vialidad pública, la que puede ser ejercida mediante la colocación de cámaras (Dictamen N° 15/018, de 04 de setiembre de 2018)

VI. Que la colocación de cámaras por particulares en la vía pública tiene los límites establecidos por la LPDP, específicamente la actuación de los responsables de las bases de datos debe ajustarse a los principios de su art. 5° (Legalidad, Veracidad, Finalidad, Previo consentimiento informado, Seguridad de los datos, Reserva y Responsabilidad), y en particular a lo dispuesto en los arts. 6º y 7º.

VII. Que de acuerdo con las precitadas disposiciones no resulta viable colocarse cámaras en espacios públicos si captan lugares, personas, matrículas, números de puerta u otro dato similar que identifique o haga identificable a una persona si no se da cumplimiento a la obtención del consentimiento previo, expreso e informado (art 9° y 13 LPDP). Por otra parte, la retrasmisión de las imágenes configura una hipótesis de comunicación de datos en los términos establecidos en el artículo 4 literal B y 17 de la Ley citada.

ATENTO: A lo expuesto,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Indicar que la colocación de cámaras en la vía pública solo resulta legítima si se da cumplimiento a los principios rectores en materia de protección de datos personales.

2) Señalar que no existe vulneración a la referida protección si las cámaras no permiten la identificación de las personas y se colocan en lugares que capten en forma general la ciudad o son de baja resolución (con aplicación de filtros de privacidad).

3) Señalar que, si las cámaras están orientadas a lugares privados y permiten la identificación de las personas, deberá obtenerse su consentimiento previo, expreso e informado e inscribirse la base de datos, además de cumplir el resto de las obligaciones referidas en la Ley Nº 18.331, de 11 de agosto de 2008.

4) Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 6/019, de 7 de mayo de 2019

Consulta presentada por el Banco de Previsión Social respecto a la firma de un Acuerdo de Programa con la organización SMILE TRAIN con sede en los Estados Unidos.

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

DICTAMEN N°	6	2019
EXPEDIENTE N°	2019-2-10-0000079	

Montevideo, 7 de mayo de 2019

VISTO: La consulta presentada por el BANCO DE PREVISIÓN SOCIAL respecto a la firma de un acuerdo de Programa con la organización con sede en los Estados Unidos denominada SMILE TRAIN.

RESULTANDO:

I. Que la consultante solicita a esta Unidad se pronuncie sobre la adecuación a la normativa en materia de protección de datos de las cláusulas del acuerdo que adjunta con SMILE TRAIN -organización sin fines de lucro dedicada a la provisión de fondos, herramientas y educación en materia de labio/paladar hendido-.

II. Que surge de la documentación presentada que el objetivo del acuerdo es concretar esfuerzos de cooperación, permitiendo al BANCO DE PREVISIÓN SOCIAL ofrecer cirugías reconstructivas gratis, entre otros servicios.

III. Que SMILE TRAIN se encuentra ubicada en Nueva York, Estados Unidos de América, y no cuenta con certificación de Privacy Shield.

CONSIDERANDO:

I. Que el presente caso se trata de la aplicación de normativa en materia de transferencias internacionales de datos de salud y de menores de edad a territorio no adecuado, por lo que resulta aplicable la Ley N° 18.331, de 11 de agosto de 2008, en particular sus artículos 17, 18 y 23. Además corresponde la aplicación de los artículos 8° a 12°, este último en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018.

II. Que el BANCO DE PREVISIÓN SOCIAL tiene cometidos específicos vinculados al tratamiento de las patologías objeto del acuerdo presentado, conforme lo establecido por el Decreto-Ley N° 15.084, de 28 de noviembre de 1980, el decreto N° 227/981, de 27 de mayo de 1981 y demás normas reglamentarias.

III. Que en tanto los padres brinden el consentimiento para la comunicación de la información a SMILE TRAIN, se cumple con lo establecido en el artículo 23 literal A de la Ley N° 18.331, que prevé la transferencia de información con el consentimiento del interesado -en este caso de su representante-. No obstante, deberá revisarse la redacción del modelo de consentimiento -o complementarse en debida forma-, en lo que respecta a la posibilidad de establecerse finalidades adicionales, e informarse que aún en caso de negativa a proporcionar dicho consentimiento, el menor tendrá la posibilidad de obtener la asistencia debida.

IV. Que en lo que respecta a la comunicación de información a SMILE TRAIN, deberá limitarse a la estrictamente necesaria para el cumplimiento de las obligaciones asumidas, y asegurarse la supresión de ésta a requerimiento del interesado por una vía sencilla y gratuita. El BANCO DE PREVISIÓN SOCIAL deberá asumir la obligación de recabar esas manifestaciones de voluntad, y que cumpla con lo solicitado por los titulares de los datos o sus representantes.

V. Que en lo que respecta a las restantes obligaciones en el marco del artículo 12° de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, corresponde la realización de una Evaluación de Impacto en la Protección de Datos y el registro de la base de datos de los menores que formen parte del programa.

VI. Que atento a lo dispuesto por el artículo 37 literal A de la Ley N° 19.670, SMILE TRAIN se encontrará alcanzada por las disposiciones de la Ley N° 18.331.

ATEN TO: A lo expuesto e informado, y a lo previsto en las normas aplicables,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1) El acuerdo presentado por el BANCO DE PREVISIÓN SOCIAL cumple con las disposiciones en materia de protección de datos para las transferencias internacionales previstas, por encontrarse abarcado en lo dispuesto en el artículo 23 literal A de la Ley N° 18.331, debiendo previamente adaptarse el modelo de consentimiento en la forma indicada en los Considerandos, dando cuenta a esta Unidad.

2) El BANCO DE PREVISIÓN SOCIAL deberá dar cumplimiento a lo dispuesto en el artículo 12° de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, incluyendo las recomendaciones que surgen de los Considerandos del presente Dictamen y lo informado en obrados, dando cuenta a esta Unidad.

3) Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 7/019, de 14 de mayo de 2019

Consulta acerca del Oficio N° 108/2018-rdjd remitido por la Oficina de Instrucciones Sumariales de la Dirección Nacional Guardia Republicana del Ministerio del Interior.

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

DICTAMEN N°	7	2019
EXPEDIENTE N°	2018-2-10-0000659	

Montevideo, 14 de mayo de 2019.

VISTO: El Oficio N° 108/2018-rdjd remitido por la Oficina de Instrucciones Sumariales de la Dirección Nacional Guardia Republicana del Ministerio del Interior.

RESULTANDO:

I. Que, en el marco de un Sumario Administrativo dispuesto a un integrante de la Guardia Republicana por una publicación en un grupo de WhatsApp, (creado con la finalidad de coordinar y ver las publicaciones de las órdenes de Servicio) denominado "ART 222", un video en el cual refiere al Señor Presidente de la República y a su familia.

II. Puntualmente, el Instructor sumariante solicita respuesta a las siguientes preguntas "la siguiente información sobre WhatsApp: a) ¿Es una red social? b) ¿Existe regulación para el uso de una información compartida en los grupos de WhatsApp? En caso positivo ¿cuál es? c) ¿Debe existir consentimiento por parte de quien comparte una información en un grupo de WhatsApp para ser utilizada posteriormente? d) ¿Existe reglamentación que proteja a quien comparte una información, imagen, etc. por WhatsApp? e) ¿Existe reglamentación para proteger la privacidad de lo compartido en un grupo de WhatsApp?". Solicita además el consultante que "sin perjuicio de las anteriores preguntas, toda aquella información que puedan aportar al respecto, será de utilidad" para el Sumario Administrativo.

CONSIDERANDO:

I. Que en lo que refiere a la pregunta a), a nivel normativo no se ha definido qué se entiende por "red social", por lo que se trata de un concepto que debe construirse desde la doctrina. A ese respecto, el Diccionario de la Real Academia Española de la Lengua define en la 23a. acepción del vocablo "red" al "conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información", y, más precisamente, "red social" como "plataforma digital de comunicación global que pone en contacto a gran número de usuarios".

II. Que en el mismo sentido el Instituto Nacional de Ciberseguridad (INCIBE), ex INTECO, expresa que "Las redes sociales son espacios virtuales en los que cada usuario cuenta con un perfil público, que refleja datos personales, estado e información de uno mismo. A su vez dispone de herramientas que permiten interactuar y conocer al resto de usuarios, por ejemplo, mediante la creación de grupos de interés". Ahora bien, WhatsApp Messenger es definido como una aplicación de mensajería multiplataforma que permite enviar y recibir mensajes instantáneos a través de un teléfono móvil y posibilita el intercambio de textos, audios, videos y fotografías; cuenta en la actualidad con cifrado de extremo a extremo de la comunicación que evita que terceros accedan al contenido de esta. Se requiere la creación de un perfil y permite interactuar con otros usuarios o grupos. Por tanto, cumple con las características de una red social.

III. Que respecto de la pregunta b), es de aplicación a la información (mensajes, fotografías, videos) compartida a través de WhatsApp, el marco jurídico dado por la Constitución de la República, en lo que refiere a libertad de expresión, de asociación, inviolabilidad de la correspondencia, protección de datos personales, así como la normativa específica relativa a la difamación e injurias cuando correspondiere. Alcanza también a la información compartida por WhatsApp la normativa de derechos de propiedad intelectual, derechos de autor y marcas registradas, en lo que sea aplicable. El funcionamiento a nivel interno de un grupo de WhatsApp -más allá de la normativa antes reseñada-, es de resorte exclusivo de sus creadores y participantes por lo que la forma de ingreso, el tipo de información, lenguaje, será determinado de forma autorregulada por su administrador/creador y por los términos y condiciones de uso propios de WhatsApp.

IV. **IV.**Que en cuanto a la pregunta c), cabe indicar que quien comparte información en WhatsApp queda comprendido en lo establecido en los artículos 4° literal B) y artículo 17 de la Ley N° 18.331 de 11 de agosto de 2008, y, por tanto, si una persona envía información propia a un grupo de WhatsApp, está prestando su consentimiento para su utilización en el marco de dicho grupo (artículo 9° de la citada Ley), y con una finalidad determinada. En virtud de ello, utilizarla más allá de ese ámbito implica comunicar datos sin previo consentimiento e infringiendo el principio de finalidad.

V. Que en cuanto a la pregunta d), resulta de aplicación a la información compartida por WhatsApp, además de la normativa antes reseñada, la Ley N° 9.739 de 12 de diciembre de 1937 por la cual se protegen los Derechos de Autor y la Ley N° 17.616, de 10 de enero de 2003, de Protección de la Propiedad Intelectual, en lo que corresponda.

VI. Que respecto a la pregunta e), se indica que es de aplicación la Ley N° 18.331, de 11 de agosto de 2008, en lo relativo al consentimiento y comunicación de datos, para proteger la privacidad de lo compartido en un grupo de WhatsApp.

ATENTO: A lo expuesto y lo dispuesto por los artículos citados,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido indicado en los Considerandos I a VI del presente dictamen.

2) Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 8/019, de 14 de mayo de 2019

Consulta remitida por el Instituto Nacional de Inclusión Social Adolescente acerca de la compatibilidad entre lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015 y el proyectado artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria.

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

DICTAMEN N°	**8**	**2019**
Expediente N°	**2018-2-10-000347**	

Montevideo, 14 de mayo de 2019

VISTO: La consulta remitida por el Instituto Nacional del de Inclusión Social Adolescente.

RESULTANDO:

I. Que en el marco de lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015, surge una diferencia de visión respecto de la redacción del artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria; especialmente respecto al inciso final, cuyo texto reza: "Exceptuase la participación y acceso a las declaraciones de los adolescentes y jóvenes atendidos en el Instituto, así como cualquier otro dato relativo a ellos para el sumariado, de conformidad con la Ley 18.381 y Ley 19.178".

II. Que se realizó consulta a la Asesoría de la Oficina Nacional de Servicio Civil, la que estimó que era necesario que el funcionario y su abogado patrocinante tuvieran acceso a todas las declaraciones para una mejor defensa, en pos de la sustanciación del debido proceso. En forma similar opinó el Sindicato, que además propuso una redacción alternativa.

CONSIDERANDO:

I. Que el presente caso involucra el tratamiento de datos personales de diversas personas en un sumario administrativo, incluidas menores de edad y jóvenes, por lo que resulta de plena aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.

II. Que a los efectos de poder determinar si procede el acceso a la información por parte del sumariante y su patrocinante, es necesario tomar en cuenta dos elementos sustanciales que se encuentran en juego: el debido proceso y el interés superior del menor.

III. Que, con respecto al primero, es una garantía esencial en un Estado de Derecho, consagrada en los arts. 12 de la Constitución y 8° del Pacto de San José de Costa Rica. Si no se accede a la información de que se trata, se estaría ante la posibilidad de vulnerar el debido proceso, siendo aplicable el artículo 7° de la Carta que establece que solamente los límites a los derechos deben provenir de una ley y por razones de interés general. Por otro lado, se aprecia el interés superior del menor, reconocido en la mayoría de los instrumentos internacionales de los cuáles Uruguay forma parte y normas de menos valor y fuerza.

IV. Que, por tanto, resulta pertinente la ponderación de los referidos elementos y como resultado, corresponde pronunciarse por la prevalencia de debido proceso por su especial vínculo con la libertad de la persona. Sin perjuicio de ello, como alternativa, cabe establecer un procedimiento para acceder a la información, basado en ley que protege los bienes jurídicos presentes; así se pueden determinar algunas características, como las de que la información sea tratada en forma individual y reservada, sin presencia de representantes de la persona denunciada ni de los denunciantes y sin identificar en el expediente los datos de los declarantes. La información recaba puede ser resguardada fuera del expediente y permanecer a cargo de la entidad durante un plazo a establecer, para el caso que así lo solicite la sede judicial, con lo cual cumpliría con el principio de reserva regulado en el artículo 11 de la Ley N° 18.331, de 11 de agosto de 2008.

V. Que otro principio a considerar es el de finalidad por el cual los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su atención.

VI. Que otro elemento de importancia es que en el tratamiento de datos personales se utilicen criterios de disociación. A esos efectos, la Unidad mediante la Resolución 68/017, de 26 de abril de 2017, aprobó el documento "Criterios de disociación de datos personales" por el cual se establecen diversos mecanismos de disociación de datos personales.

VII. Que se considera adecuado que en todo lo que hace relación con la clasificación de la información, se remita consulta a la Unidad de Acceso a la Información Pública, como órgano rector en la materia.

ATENTO: a lo expuesto e informado.

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) En la consulta planteada se está ante un caso de ponderación de derechos y que se estime pertinente garantizar el debido proceso y si interés superior del menor salvo que se establezca por vía legislativa un procedimiento para la entrega de la información, indicando además la forma de tratar los datos personales.

2) La información deberá ser tratada de conformidad con los principios de la protección de datos personales, en especial énfasis en la reserva y la finalidad, debiendo tenerse presente los Criterios de Disociación de Personales como herramienta para disociar la información.

3) Notifíquese y publíquese.

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 8/019, de 14 de mayo de 2019

Consulta remitida por el Instituto Nacional de Inclusión Social Adolescente acerca de la compatibilidad entre lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015 y el proyectado artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria.

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

DICTAMEN N°	8	2019
Expediente N°	2018-2-10-000347	

Montevideo, 14 de mayo de 2019

VISTO: La consulta remitida por el Instituto Nacional del de Inclusión Social Adolescente.

RESULTANDO:

I. Que en el marco de lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015, surge una diferencia de visión respecto de la redacción del artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria; especialmente respecto al inciso final, cuyo texto reza: "Exceptuase la participación y acceso a las declaraciones de los adolescentes y jóvenes atendidos en el Instituto, así como cualquier otro dato relativo a ellos para el sumariado, de conformidad con la Ley 18.381 y Ley 19.178".

II. Que se realizó consulta a la Asesoría de la Oficina Nacional de Servicio Civil, la que estimó que era necesario que el funcionario y su abogado patrocinante tuvieran acceso a todas las declaraciones para una mejor defensa, en pos de la sustanciación del debido proceso. En forma similar opinó el Sindicato, que además propuso una redacción alternativa.

CONSIDERANDO:

I. Que el presente caso involucra el tratamiento de datos personales de diversas personas en un sumario administrativo, incluidas menores de edad y jóvenes, por lo que resulta de plena aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.

II. Que a los efectos de poder determinar si procede el acceso a la información por parte del sumariante y su patrocinante, es necesario tomar en cuenta dos elementos sustanciales que se encuentran en juego: el debido proceso y el interés superior del menor.

III. Que, con respecto al primero, es una garantía esencial en un Estado de Derecho, consagrada en los arts. 12 de la Constitución y 8° del Pacto de San José de Costa Rica. Si no se accede a la información de que se trata, se estaría ante la posibilidad de vulnerar el debido proceso, siendo aplicable el artículo 7° de la Carta que establece que solamente los límites a los derechos deben provenir de una ley y por razones de interés general. Por otro lado, se aprecia el interés superior del menor, reconocido en la mayoría de los instrumentos internacionales de los cuáles Uruguay forma parte y normas de menos valor y fuerza.

IV. Que, por tanto, resulta pertinente la ponderación de los referidos elementos y como resultado, corresponde pronunciarse por la prevalencia de debido proceso por su especial vínculo con la libertad de la persona. Sin perjuicio de ello, como alternativa, cabe establecer un procedimiento para acceder a la información, basado en ley que protege los bienes jurídicos presentes; así se pueden determinar algunas características, como las de que la información sea tratada en forma individual y reservada, sin presencia de representantes de la persona denunciada ni de los denunciantes y sin identificar en el expediente los datos de los declarantes. La información recaba puede ser resguardada fuera del expediente y permanecer a cargo de la entidad durante un plazo a establecer, para el caso que así lo solicite la sede judicial, con lo cual cumpliría con el principio de reserva regulado en el artículo 11 de la Ley N° 18.331, de 11 de agosto de 2008.

V. Que otro principio a considerar es el de finalidad por el cual los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su atención.

VI. Que otro elemento de importancia es que en el tratamiento de datos personales se utilicen criterios de disociación. A esos efectos, la Unidad mediante la Resolución 68/017, de 26 de abril de 2017, aprobó el documento "Criterios de disociación de datos personales" por el cual se establecen diversos mecanismos de disociación de datos personales.

VII. Que se considera adecuado que en todo lo que hace relación con la clasificación de la información, se remita consulta a la Unidad de Acceso a la Información Pública, como órgano rector en la materia.

ATENTO: a lo expuesto e informado.

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) En la consulta planteada se está ante un caso de ponderación de derechos y que se estime pertinente garantizar el debido proceso y si interés superior del menor salvo que se establezca por vía legislativa un procedimiento para la entrega de la información, indicando además la forma de tratar los datos personales.

2) La información deberá ser tratada de conformidad con los principios de la protección de datos personales, en especial énfasis en la reserva y la finalidad, debiendo tenerse presente los Criterios de Disociación de Personales como herramienta para disociar la información.

3) Notifíquese y publíquese.

DR. FELIPE ROTONDO
URCDP

Dictamen Nº 9/019, de 27 de agosto de 2019

Consulta realizada por la Facultad de Veterinaria sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral.

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

DICTAMEN N°	9	2019
EXPEDIENTE N°	2019-2-10-0000070	

Montevideo, 13 de agosto de 2019.

VISTO: La consulta formulada por la FACULTAD DE VETERINARIA sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral

RESULTANDO:

I. Que el planteo de la consultante se fundamenta en la solicitud realizada por estudiantes y docentes de la Facultad citada, y que fuera elevado a la Comisión de Enseñanza.

II. Que la consultante adjunta informe de la Dirección General Jurídica de la Universidad de la República, en el que se esgrime la posibilidad de aplicar las definiciones existentes en el Dictamen N° 10/010 de 16 de abril de 2010 del Consejo Ejecutivo de la Unidad, respecto al tema de video vigilancia.

CONSIDERANDO:

I. Que corresponde considerar la aplicación del artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008, que prevé el consentimiento previo, expreso e informado de los titulares de los datos y otras bases legítimas del tratamiento -calificadas como excepciones al principio del previo consentimiento informado-. No es necesario en consecuencia el consentimiento, cuando el tratamiento se encuentra alcanzado por las excepciones expresamente previstas en la norma.

II. Que son aplicables, además, la Ley N° 12.549 de 29 de octubre de 1958 (Ley Orgánica de la Universidad de la República), el Reglamento de 27 de diciembre de 1967 aprobado por el Consejo Directivo Central para la Facultad de Veterinaria y la Ordenanza de Estudios de Grado y Otros Programas de Formación Terciaria (Res. Nº 3 de C.D.C. de 2/VIII/2011 - Dista. Nº 451/11, Res. Nº 4 del C.D.C. de 30/VIII/2011- Dist. Nº 575/11 y 576/11, publicada en el Diario Oficial el 19 de setiembre de 2011).

III. Que del análisis de las normas resulta que resulta necesaria su armonización a efectos de homogeneizar el tratamiento de los datos personales, aunque no resulta necesario el consentimiento previo, expreso e informado de los estudiantes y docentes para la grabación de los exámenes orales si así lo disponen los reglamentos que se dicten a nivel universitario y se establecen medios para garantizar un adecuado tratamiento de los datos personales.

ATENTO: A lo expuesto y lo dispuesto por los artículos mencionados,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) La grabación de los exámenes orales y su almacenamiento no vulnera las normas en materia de protección de datos personales si así lo establecen los reglamentos a nivel universitario.

2) El tratamiento de los datos referido en el numeral anterior deberá realizarse al amparo de lo establecido en la Ley N° 18.331, de 11 de agosto de 2008, dando cumplimiento a los principios en ella establecidos.

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 10/019, de 27 de agosto de 2019

Consulta formulada por el Banco de Previsión Social sobre contestación de oficios judiciales con especial atención a la información referida a montos de prestaciones de actividad y pasividades de afiliados, así como otra información de naturaleza sensible.

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

DICTAMEN N°	10	2019
EXPEDIENTE N°	2018-2-10-0000653	

Montevideo, 27 de agosto de 2019.

VISTO: La consulta formulada por el BANCO DE PREVISIÓN SOCIAL sobre contestación de oficios judiciales.

RESULTANDO:

Que el consultante solicita pronunciamiento de esta Unidad con respecto a la aplicación de las normas en materia de protección de datos personales a las contestaciones de oficios recibidos del poder judicial, con especial atención a la información de montos de prestaciones de actividad y pasividad de afiliados y otra información de naturaleza sensible.

CONSIDERANDO:

I. Que en la situación de prestaciones de actividad y pasividad es de aplicación lo dispuesto por el artículo 47 del Código Tributario del Uruguay, no siendo por ende los datos abarcados por dicho artículo confidenciales sino secretos.

II. Que, con respecto a los datos sensibles, resultan de aplicación en la especie los artículos 17 y 18 de la ley N° 18.331, de 11 de agosto de 2008, en los que se prevé distintas hipótesis para la comunicación de los datos, que no se limitan al consentimiento previo, expreso y en su caso escrito del titular del dato. En consecuencia, si existe un interés por parte del Juzgado correspondiente, reflejado en un oficio, con determinación de la información solicitada, su fin y aplicación a un proceso determinado, corresponderá su entrega.

ATENTO: A lo expuesto y lo dispuesto por los artículos mencionados,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) La información asociada al pago de los tributos recaudados por la consultante se encuentra abarcada por las disposiciones en materia de secreto tributario y por ende sólo podrá ser entregada -aún al Poder Judicial- en los casos expresamente previstos en la norma.

2) Toda otra información fuera de la mencionada en el literal anterior, aún de naturaleza sensible, podrá ser entregada a requerimiento del Poder Judicial, aún sin contar con consentimiento expreso y por escrito del interesado, siempre que se acrediten las condiciones establecidas en el artículo 17 literal B y en el artículo 9 literal B de la Ley N° 18.331, de 11 de agosto de 2008.

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 11/019, de 24 de setiembre de 2019

Consulta remitida por la Secretaría Nacional para la lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAF) acerca de la posibilidad legal de esa Secretaría de publicar las resoluciones que imponen sanciones a los sujetos obligados.

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

DICTAMEN N°	11	2019
Expediente N°	2019-2-10-0000345	

Montevideo, 24 de setiembre de 2019

VISTO: La consulta remitida por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (en adelante SENACLAFT).

RESULTANDO:

I. Que en el marco de lo dispuesto en el artículo 4° y 13 de la Ley N° 19.574, de 20 de diciembre de 2017, se establece dentro de los cometidos de la SENACLAFT el control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo, así como ejecutar las sanciones pecuniarias impuestas.

II. El procedimiento administrativo tendiente a la aplicación de las referidas sanciones se tramita por el Decreto N° 500/991, culminando -de corresponder- con la aplicación de una sanción de apercibimiento, observación, multa o suspensión o en su caso el archivo, previo conocimiento del interesado.

CONSIDERANDO:

I. Que la consulta involucra el tratamiento de datos personales de diversas personas físicas o jurídicas, por lo que resulta de aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.

II. Que a los efectos de determinar si procede la publicación de las resoluciones es preciso tomar en cuenta lo establecido en los artículos 4° literal B, 17 y 18 de la Ley N° 18.331 (comunicación de datos, previo consentimiento informado, datos especialmente protegidos). En particular, corresponde analizar la ponderación de los derechos en conflicto (transparencia de las sanciones y facultad conferida a las entidades públicas en general en el artículo 18 in fine de la Ley N° 18.331 por un lado, y derecho de la persona a que dicha información no quede a perpetuidad por otro).

III. Que, además, todo tratamiento de datos, incluyendo su comunicación, deberá ajustarse a los principios establecidos en la Ley N° 18.331, sin perjuicio de la clasificación o calificación que se realice por parte de SENACLAFT de la información contenida en el expediente en el marco de lo dispuesto por la Ley N° 18.381, de 17 de octubre de 2008.

IV. Que en lo que refiere a la publicación de sanciones en internet, corresponde considerar los criterios indicados en la Resolución N° 1040/2012 de esta Unidad, de fecha 20 de diciembre de 2012.

ATENTO: a lo expuesto.

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Resulta aplicable a la situación detallada en la consulta, la excepción al principio del previo consentimiento informado indicada en el art. 18 in fine de la Ley N° 18.331, de 11 de agosto de 2008 (infracciones penales, civiles o administrativas). La responsabilidad por la valoración en la publicación en caso de no existir norma específica corresponde a la entidad que la pública (en el caso SENACLAFT).

2) Los datos personales deberán ser tratados de conformidad con los restantes principios de la protección de datos personales, debiendo tener presente en particular lo indicado en la Resolución N° 1040/2012 de esta Unidad, de fecha 20 de diciembre de 2012.

3) Notifíquese y publíquese.

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 12/019, de 24 de setiembre de 2019

Consulta realizada por el Instituto de Regulación de Cannabis (IRCCA) sobre el tratamiento correcto a conferir a los datos históricos, teniendo en cuenta que la justicia penal podría solicitar datos sobre personas, así como la pertinencia de solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

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

DICTAMEN N°	12	2019
Expediente N°	2019-2-10-0000240	

Montevideo, 24 de setiembre de 2019

VISTO: La consulta realizada por el INSTITUTO DE REGULACIÓN Y CONTROL DE CANNABIS (en adelante IRCCA).

RESULTANDO:

I. Que el IRCCA indica que es responsable de una base de datos que se encuentra registrada ante la Unidad Reguladora y de Control de Datos Personales, y que los datos concretos que se asientan en dicha base (adquirientes de cannabis locales de expendio, cultivadores domésticos y miembros de los Clubes Cannábicos de Membresía) son considerados datos sensibles de acuerdo con lo dispuesto en el artículo 3° del Decreto Ley N° 14.294, en la redacción dada por el artículo 5° de la Ley N° 19.172, de 20 de diciembre de 2013.

II. **I**Que, en ese marco, requiere la opinión de la Unidad sobre dos aspectos: a) el tratamiento correcto a conferir a los datos históricos, teniendo presente que la Justicia Penal puede llegar a solicitar datos sobre personas; b) si el IRCCA debe solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

CONSIDERANDO:

I. Que conforme a la Ley N° 19.172, de 20 de diciembre de 2013, se pretende promover y mejorar la salud pública de la población mediante una política orientada a minimizar los riesgos y a reducir los daños del uso del cannabis. La norma crea el IRCCA como persona pública no estatal, encargada de todos los temas vinculados al uso de cannabis.

II. Que, conforme con el artículo 8 de la ley citada, se crea un registro que "...llevará sendos registros para las excepciones previstas en los literales A), B), C), D), E), F) y G) del artículo 3° del Decreto-Ley N° 14.294, de 31 de octubre de 1974, en la redacción dada por el artículo 5° de la presente ley (...)". Esta norma fue posteriormente reglamentada por los decretos Nº 128/016 de 02 de mayo de 2016, Nº 46/015 de 04 de febrero de 2015, Nº 372/014 de 16 de diciembre de 2014 y Nº 120/014 de 06 de mayo de 2014 (este último regula en sus artículos 52 a 77 el "Registro del Cannabis").

III. Que resulta de aplicación al caso concreto la Ley N° 18.331, ya que se trata de la posibilidad de conservar datos personales declarados sensibles de acuerdo con el artículo 8° de la Ley N° 19.172, con la potencialidad de ser comunicados a la Justicia Penal.

IV. Que, en cuanto a la conservación, se debe considerar el artículo 8° de la Lay N° 18.331 que establece con carácter general en su inciso primero que "Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.". No obstante, corresponde señalar que el Decreto N° 120/014, establece en las distintas secciones del Registro criterios para la conservación de los datos personales (artículos 52 en adelante).

V. Que en los casos en que existan razones legales suficientes, se podrán conservar los datos previo bloqueo (definido por el artículo 4° del decreto N° 414/009 como "procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento").

VI. Que, transcurrido el plazo referido en el considerando anterior, corresponde la eliminación de toda la información, salvo que se acrediten razones históricas, estadísticas o científicas basadas en la legislación específica que permitan su conservación para lo cual deberá seguirse el procedimiento previsto en el artículo 37 del Decreto N° 414/009.

VII. Que en lo que refiere a la entrega de información solicitada por la Justicia Penal, es de aplicación el Dictamen N° 16/2018, de 11 de setiembre de 2018 de esta Unidad, conforme el cual se deberá proceder a la entrega de la información cuando ésta efectivamente exista, indicándose en caso contrario que no existe la información solicitada por la causal que corresponda al caso concreto (vencimiento del plazo, sanción, etc.).

ATENTO: a lo expuesto e informado,

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) En relación con la primera consulta, corresponde la aplicación del artículo 8° de la Ley N° 18.331, por lo que los datos se pueden conservar en tanto existan las razones por las cuales se recolectaron. La normativa específica que regula los distintos sectores que conforman el Registro de Cannabis prevé plazos especiales de conservación que deberán ser respetados.

2) Para la conservación de los datos más allá de la finalidad para la que fueron recolectados debe existir un fundamento legal y realizarse un bloqueo previo. Vencidos todos los plazos, se debe proceder a su eliminación, pudiendo conservarlos solamente por razones históricas, científicas o estadísticas, siguiendo el procedimiento establecido a esos efectos por el artículo 37 del Decreto N° 414/009.

3) NOTIFÍQUESE Y PUBLÍQUESE.

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 13/019, de 24 de setiembre de 2019

Consulta formulada por la Dirección Nacional de Empleo del Ministerio de Trabajo y Seguridad Social (DINAE) con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

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

Dictamen N°	13	2019
Expediente N°	2019-2-10-0000252	

Montevideo, 24 de setiembre de 2019

VISTO: La consulta realizada por la Dirección Nacional de Empleo (en adelante DINAE) del Ministerio de Trabajo y Seguridad Social con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

RESULTANDO:

Que la consulta versa sobre la aplicabilidad de la Ley N° 18.331, de 11 de agosto de 2008, a la información publicada por menores de edad en el perfil del sistema de intermediación laboral web desarrollado por la DINAE y el Instituto Nacional de Empleo y Formación Profesional (INEFOP), disponible a través de la Plataforma Vía Trabajo.

CONSIDERANDO:

I. Que en el presente caso resultan aplicables las disposiciones de la Ley N° 18.331, y los artículos 213 y siguientes del Código Civil (en especial el artículo 267 referente al peculio industrial, entre otros), el Código de la Niñez y la Adolescencia (en particular el Capítulo XII, artículos 161 a 180) y la Ley N° 19.133, de 20 de setiembre de 2013, sobre fomento del empleo juvenil.

II. Que el derecho a la protección de datos personales es un derecho fundamental reconocido en el artículo 1° de la Ley N° 18.331, y se sustenta en varios principios, entre los que se encuentra el del previo consentimiento informado (artículo 9°). Este principio sienta varias bases legítimas de tratamiento de los datos estableciendo al previo consentimiento como la principal, pero regulando otras en la forma de excepciones.

III. Que no existen normas específicas que regulen el consentimiento de menores de edad e incapaces en lo que respecta a la protección de sus datos personales, por lo que deberá acudirse a las normas en materia de representación previstas en el derecho civil.

IV. Que, en el caso específico del desarrollo de tareas laborales, el consentimiento de los adolescentes habilitados por las normas para trabajar no es suficiente, debiendo complementarse con el de sus progenitores -conforme lo indicado en los artículos 167 del Código de la Niñez y de la Adolescencia y 7° de la Ley N° 19.133-.

V. Que, sin perjuicio de tratarse de derechos diferentes, en el caso concreto de obrados el consentimiento referido en el considerando anterior resulta comprensivo del requerido para la publicación de la información en la plataforma referida.

ATENTO: a lo expuesto e informado,

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) El consentimiento de los representantes de los menores de edad habilitados por las normas para trabajar, para la publicación de información vinculada a su experiencia y preparación laboral exclusivamente en el Portal Vía Trabajo, se encuentra incluido en el consentimiento otorgado para el cumplimiento de las tareas laborales, reflejado en el carné de habilitación laboral.

2) El Ministerio de Trabajo y Seguridad Social deberá arbitrar todas las medidas necesarias para el cumplimiento de los principios de la Ley N° 18.331 en la publicación de datos de los menores de edad en el Portal Vía Trabajo, con la asistencia y colaboración de las instituciones vinculadas a la defensa de dichos menores.

3) NOTIFÍQUESE Y PUBLÍQUESE.

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 14/019, de 1 de octubre de 2019

Consulta presentada por el Colegio Nueva Cultura sobre la publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

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

DICTAMEN N°	14	2019
Expediente N°	2019-2-10-000338	

Montevideo, 1 de octubre de 2019

VISTO: La consulta realizada por el COLEGIO NUEVA CULTURA.

RESULTANDO:

Que se requiere opinión de esta Unidad sobre la publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

CONSIDERANDO:

I. **I**Que el artículo 3° de la Ley N° 18.331, de 11 de agosto de 2008 prevé que "(...) será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado". El artículo 12° establece que el responsable de la base de datos es responsable por el cumplimiento de la Ley, sin perjuicio de la responsabilidad que le cabe a los encargados de tratamiento (resolución N° 104/2015, de 23 de diciembre de 2015, Considerando V, entre otros).

II. Que el llamado "derecho al olvido" no posee consagración a nivel nacional, siendo una extensión del derecho de supresión y actualización, en el marco de los principios de finalidad y veracidad consagrados en las normas que regulan la protección de datos personales (artículos 7, 8, 14 y 15 de la Ley Nº 18.331, de 11 de agosto de 2008).

III. Que la Resolución Nº 1040/012 de 20 de diciembre de 2012 propuso soluciones técnicas para evitar la indexación de contenidos e inclusión en el caché de los buscadores y recomendó la aplicación de criterios técnicos para la publicación de contenidos en sitios web. A su vez, el Dictamen Nº 2/014 de 13 de febrero de 2014 señala que es el responsable del contenido del sitio web, quien decida la información a ser publicada, y por cuánto tiempo, al igual que los controles o filtros para evitar la indexación por los motores de búsqueda. Ello fue reiterado en la Resolución Nº 6/016 de 9 de marzo de 2016.

IV. Que en el dictamen N° 17/2016 se señala 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".

V. Que, en el caso de información publicada por medios de prensa, es necesario realizar una ponderación de derechos, por no ser los derechos reconocidos por la Constitución absoluto conforme jurisprudencia de la Suprema Corte de Justicia. Ese ejercicio de ponderación corresponde en primer lugar a los responsables y encargados en su caso, sin perjuicio de la actuación del Poder Judicial cuando la naturaleza de los derechos en conflicto lo amerite.

ATENTO: a lo expuesto e informado,

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) En la situación planteada el consultante podrá dirigir el ejercicio de sus derechos ante los responsables o los encargados de tratamiento -incluyendo los motores de búsqueda-, fundado en los artículos 14 y 15 de la Ley N° 18.331, de 11 de agosto de 2008, que podrán aplicar los mecanismos mencionados en el Considerando III.

2) En caso de denegación o limitación de sus derechos, el consultante podrá plantear la denuncia ante esta Unidad o ante el Poder Judicial en el marco de lo dispuesto en los artículos 34 y 37 y siguientes de la referida Ley.

3) NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 15/019, de 5 de noviembre de 2019

Consulta formulada por el Consejo de Educación Técnico Profesional sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de las personas (nombre completo, C.I., título obtenido, nivel que se obtiene con él, plan en que cursó y centro educativo), la situación del trámite del título incluyendo la repartición en que se encuentra y fecha.

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

DICTAMEN N°	**15**	**2019**
Expediente N°	**2019-2-10-0000340**	

Montevideo, 5 de noviembre de 2019

VISTO: La consulta realizada por el Consejo de Educación Técnico Profesional.

RESULTANDO:

I. Que la Unidad de Prosecretaria del Consejo de Educación Técnico Profesional consulta sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de la persona con nombre completo, cédula de identidad, título obtenido, nivel que se obtiene el mismo, plan en que cursó y centro educativo. Asimismo, el trámite del título con la repartición en que se encuentra y fecha.

II. **I**Que además agrega que sería un apartado en el sitio web al que se accedería ingresando el nombre de la persona o su cédula de identidad, y se desplegaría una ventana con los datos antes referidos. En ese marco, solicita conocer si para instrumentar una base de datos de este tenor, se requiere el previo consentimiento a efectos de proceder a publicar esos datos personales.

CONSIDERANDO:

I. Que el presente caso refiere a la legalidad de realizar una comunicación de datos, definida en el artículo 4° literal b) de la Ley N° 18.331, de 11 de agosto de 2008.

II. Que para realizar dicha comunicación el artículo 17 de la misma norma indica que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, salvo excepciones que en este caso no resultan aplicables.

III. Que otro aspecto de análisis es el impacto de la publicación en Internet de este tipo de datos. Que se debe tener en cuenta el principio de veracidad (artículo 7° de la Ley N° 18.331), indicando que los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la que se obtuvieron. Que, desde esta perspectiva, al no ser aplicable ninguna de las excepciones establecidas, ni normas que mandaten su publicación, no corresponde la publicación sin el consentimiento de los titulares.

IV. Que conforme con las modificaciones introducidas por la Ley N° 19.670, específicamente el nuevo artículo 39, los responsables y encargados de bases de datos deben adoptar las medidas técnicas y organizativas que correspondan para asegurar su protección (privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, etc.).

ATENTO: a lo expuesto y establecido por el artículo 72 de la Constitución de la República, artículos 28, 29 y 31 de la Ley N° 18.331.

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Que, a los efectos de la publicación de la información referida en estos procedimientos en Internet, es necesario recabar el previo consentimiento informado de los titulares de los datos por no resultar aplicable ninguna de las excepciones previstas en la Ley N° 18.331, de 11 de agosto de 2008.

2) Que el tratamiento de los datos deberá ajustarse a los principios de la normativa de protección de datos personales en la forma indicada en el presente Dictamen,

3) NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE
URCDP

Dictamen Nº 16/019, de 5 de noviembre de 2019

Consulta formulada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT) respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.

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

DICTAMEN N°	16	2019
Expediente N°	2019-2-10-0000448	

Montevideo, 5 de noviembre de 2019

VISTO: La consulta realizada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (en adelante SENACLAFT);

RESULTANDO:

I. Que la SENACLAFT consulta respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.

II. Que las referidas resoluciones contienen datos personales (nombres y documentos) tanto de los sujetos obligados como de sus clientes, por lo que la Secretaría considera oportuno recabar la opinión de esta Unidad a efectos de conocer la aplicabilidad de las normas en materia de protección de datos.

CONSIDERANDO:

I. Que la situación planteada refiere a una comunicación de datos (artículo 4° literal b) de la Ley N° 18.331, de 11 de agosto de 2008). El artículo 17 de la citada norma establece que sólo podrán ser comunicados los datos personales para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, y con el previo consentimiento del titular de los datos -salvo excepciones expresamente previstas en dicho artículo y en el artículo 9° de la Ley-.

II. Que corresponde considerar además el artículo 18 de la Ley citada en cuanto establece: "Los datos relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren inconveniente".

III. Que el artículo 4 de la Ley N° 19.574, de 20 de diciembre de 2017, establece que la SENACLAFT es un órgano desconcentrado dependiente directamente de la Presidencia de la República, con autonomía técnica, y que posee entre sus cometidos: "E) El control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo por parte de los sujetos obligados por el artículo 13 de la presente ley. (...) H) Ejecutar las sanciones pecuniarias que imponga mediante resolución...". Por tanto, en este caso la solicitud de información es realizada a la Entidad Pública competente para brindarla.

IV. Que el Tribunal de lo Contencioso Administrativo es un órgano jurisdiccional que tiene como cometido resolver las demandas de nulidad de los actos generales que dicte la Administración (artículo 25 de la Ley N° 15.524) y ha sido opinión firme de esta Unidad, que cuando la información sea solicitada en el marco de una función jurisdiccional, ésta debe ser entregada. Corresponde considerar especialmente la opinión reflejada en Dictamen N° 10/019 de 27 de agosto de 2019 del Consejo de la Unidad.

V. Que en cuanto a la necesidad o no del previo consentimiento informado de los titulares de datos, corresponde indicar que al caso concreto se aplica el artículo 9° literal B) de la Ley N° 18.331, y por ende no resulta necesario recabarlo por tratarse de una Entidad Pública en ejercicio de sus funciones y de una obligación legal.

VI. Que, por tanto, se encuentran debidamente acreditados todos los requisitos del artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008, para proceder a entregar la información solicitada.

ATENTO: a lo expuesto e informado,

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Indicar que la entrega de la información en la forma solicitada por el Tribunal de lo Contencioso Administrativo se ajusta a las normas de protección de datos personales.

2) NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE
URCDP

Notas de interés

La reglamentación de los artículos 37 a 40 de la Ley N° 19.670, del 15 de octubre de 2018

Equipo jurídico de la URCDP

a. Breve reseña:

La Ley Nº 19.670, de 15 de octubre de 2018, en sus artículos 37 a 40, realiza actualizaciones a la normativa de protección de datos personales e incorpora nuevas tendencias internacionales en la materia. Su finalidad fue contemplar el avance de la tecnología y el nuevo contexto que esto apareja, y adoptar las mejores soluciones internacionales para dar respuesta adecuada a los titulares de los datos personales.

Es así entonces que se incorporan como elementos nuevos el concepto de extraterritorialidad, el de vulneraciones de seguridad, el de responsabilidad proactiva (que incluye la realización de evaluaciones de impacto, adopción de medidas de privacidad por diseño y por defecto), así como la creación de la figura del delegado de protección de datos para determinadas situaciones.

A dichos efectos, y para poder ampliar los conceptos que se incorporaron a la normativa de protección de datos, se reglamentaron los artículos indicados por Decreto Nº 64/020, de 17 de febrero de 2020

b. La adopción de nuevas medidas en el marco de la responsabilidad proactiva.

En términos generales, la nueva normativa modifica el principio de responsabilidad haciéndolo evolucionar hacia el concepto de responsabilidad proactiva, incluyendo en este concepto a la privacidad por diseño y por defecto y las evaluaciones de impacto.

c. Privacidad por diseño y Privacidad por defecto

La privacidad por diseño implica que desde el comienzo del tratamiento se adopten medidas que aseguren el cumplimiento de las normas de protección de datos personales.

El objetivo es que la protección de datos personales no sea una medida que se adopta con posterioridad, sino que se considera desde el inicio del tratamiento de datos personales.

En ese marco, los responsables y los encargados de tratamiento, en su caso, deberán incorporar en el diseño de las bases de datos, las operaciones de tratamiento, las aplicaciones y los sistemas informáticos, aquellas medidas dirigidas a dar cumplimiento a la normativa de protección de datos personales. A esos efectos, previo al tratamiento y durante todo su desarrollo, aplicarán medidas técnicas y organizativas apropiadas, tales como, por ejemplo:

- Técnicas de disociación, seudonimización y minimización de datos.
- Mecanismos para asegurar el ejercicio de los derechos de los titulares de los datos personales.
- Documentación de los consentimientos o de otros fundamentos que legitimen el tratamiento.
- Tiempo de conservación de los datos, considerando sus tipos y su tratamiento.
- Adopción de planes de contingencia que incluyan medidas de seguridad de la información.
- Análisis funcionales y modelos de arquitectura de los datos.
- Otras medidas establecidas por la Unidad Reguladora y de Control de Datos Personales.

Asimismo, es importante tener en cuenta la privacidad por defecto. En este caso, el responsable y el encargado del tratamiento (cuando corresponda) aplicarán las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Se debe remarcar que esta obligación tiene relación directa con la cantidad de datos personales recogidos por el responsable, a la extensión de

su tratamiento, a su plazo de conservación y a su comunicación cuando así corresponda.

d. Las evaluaciones de impacto en la protección de datos

La evaluación de impacto en la protección de datos es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. Ello considerando que el tratamiento de datos personales puede provocar impactos en los derechos de las personas que deben ser de algún modo identificados, gestionados, minimizados o eliminados para cumplir con la normativa vigente[1]

El Decreto N° 64/020 indica una serie de situaciones donde los responsables de tratamiento y eventualmente los encargados, deben realizar la Evaluación de impacto en forma obligatoria:

En general, a la hora de realizar una evaluación de impacto se recomienda determinar quiénes van a ser los participantes del proceso y la forma en que se va a documentar la evaluación. En segundo lugar, es necesario realizar un análisis del marco normativo aplicable. Ambas se consideran tareas previas e imprescindibles antes de la evaluación en sí misma [2].

En cuanto a las etapas subsiguientes, es necesario realizar en forma sucesiva un análisis preliminar, un contexto de tratamiento, un análisis de gestión de riesgos y culminar con un plan de tratamiento de riesgos, etapas que detallan en la Guía indicada, a cuya lectura y aplicación nos remitimos.

e. Las vulneraciones de seguridad.

Las nuevas disposiciones establecen que tanto el responsable y el encargado de tratamiento deben adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar su seguridad.

A estos efectos, se considera importante valorar la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por la Agencia para el Des[3]arrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento .

Constatada la existencia de incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables y encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados.

El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarlo a la Unidad Reguladora y de Control de Datos Personales en un plazo máximo de 72 horas de conocida la vulneración.

La comunicación a la Unidad Reguladora y de Control de Datos Personales deberá contener información relevante, tal como la fecha cierta o estimada de la ocurrencia de la vulneración, su naturaleza, los datos personales afectados, y los posibles impactos generados.

Se regula además que en caso que la vulneración hubiere sido conocida por el encargado del tratamiento, éste la comunicará de inmediato al responsable del tratamiento.

El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarla en un lenguaje claro y sencillo a los titulares de los datos que hayan sufrido una afectación significativa en sus derechos.

Solucionada la vulneración, el responsable del tratamiento deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la Unidad Reguladora y de Control de Datos Personales.

Se deberá tener presente que todo lo anterior podrá ser evaluado por el Consejo de la Unidad y solicitar información en caso de que entienda que no se cumplió con los pasos mencionados.

1. Definición contenida en la Guía de Evaluación de Impacto de esta Unidad y la AAIP. Descargar guía.
2. A los efectos de conocer más detalladamente cómo se debe realizar una evaluación de impacto se sugiere consultar lGuía de Evaluación de Impacto en la Protección de Datos. Descargar guía.
3. Consultar documento.

f. Los Delegados de Protección de Datos Personales

El Delegado de Protección de Datos Personales constituye un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrolla la Autoridad de Control.

Dentro de la actualización del marco normativo nacional en materia de protección de datos personales, se crea la figura del Delegado de Protección de Datos Personales. La Ley establece determinados casos en los cuales resulta necesaria su designación, a saber:

- Entidades públicas o privadas, estatales o no, las privadas y las parcialmente de propiedad estatal
- Entidades privadas que traten datos sensibles como negocio principal.
- Entidades privadas que traten grandes volúmenes de datos personales. De acuerdo con la reglamentación posterior se entiende que gran volumen de datos es aquel que implique un tratamiento de datos de más de 35.000 personas.
- La referencia a Entidades puede alcanzar a personas físicas o jurídicas que realicen el tratamiento de datos personales o terceros, en calidad de responsable o encargado de tratamiento.
- El decreto reglamentario expresamente indica que además la Unidad, de oficio o ante una gestión expresa, puede expedirse en el sentido de indicar la pertinencia o no de su designación.

Sus funciones principales son [4]:

- Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales
- Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad
- Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia.
- Actuar como nexo entre la entidad y la URCDP

La norma además establece que el delegado debe poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuar con autonomía técnica.

Además, existen otros aspectos de los delegados que merecen ser analizados como por ejemplo la calidad y condiciones del delegado, su posición y su plazo de designación, cese o renuncia.

En ese marco, es importante indicar que el delegado puede desempeñar sus funciones a través de cualquier modalidad contractual sea en forma dependiente o no.

Conforme el decreto N° 64/020, los delegados deben contar con conocimiento en Derecho, especializados en protección de datos personales debiendo acreditarse dicha calidad al momento de su comunicación a la URCDP. La URCDP ha clarificado el alcance de esta disposición a través de la Resolución N° 32/020 del 19 de mayo de 2020, por la que se establece que se deberá tener en cuenta especialmente su calidad de profesional del área jurídica o poseer conocimientos en Derecho, con énfasis en derechos humanos, y conocimientos sobre regulación en materia de protección de datos personales lo que podrá acreditarse mediante cursos o actividades brindadas por la URCDP u otras entidades nacionales e internacionales, valorándose especialmente la realización de cursos vinculados a responsabilidad proactiva y tratamiento de categorías especiales de datos. Se tendrá en cuenta, asimismo, la experiencia previa en el ámbito de la protección de datos [5].

La evaluación de sus conocimientos corresponde a responsables y encargados en función de los citados criterios, aclarándose por Resolución de la URCDP N° 44/020 de 21 de julio de 2020 que el énfasis en derechos humanos es el necesario para contextualizar el derecho a la protección de datos en sus relaciones con otros derechos [6].

El delegado de protección de datos puede ser una persona jurídica. En estos casos, se debe informar a la URCDP quienes son sus integrantes y cuál es su órgano de administración, sin perjuicio de lo cual, es necesario identificar a sus representantes y a una persona física que se

4. Ver artículo 40 de la Ley N° 19.670.
5. Consultar la Resolución.
6. Consultar la Resolución.

constituya en el nexo con la Unidad, de conformidad con la precitada resolución Idéntica obligación existe para equipos de delegados, de conformidad con lo indicado por Resolución de la URCDP N° 44/020.

A los efectos de desarrollar en tiempo y forma sus tareas, el delegado tiene que poder participar en forma adecuada en todas las cuestiones relativas a la protección de datos. Para ello debe poder tener acceso a las bases de datos y a las operaciones de tratamiento.

El delegado debe guardar absoluta confidencialidad de las informaciones que tiene acceso por su calidad y no debe tener conflicto de intereses.

Cabe indicar que cuando corresponde la designación de un delegado se cuenta con un plazo de 90 días a contar desde el inicio del tratamiento para comunicarlo a la Unidad. También se preveía un plazo para su designación para aquellas entidades que debían contar con esta figura desde la entrada en vigor del Decreto. La comunicación del delegado se realiza a través del Sistema de Registro de Base de Datos y Comunicaciones de Delegados disponible a través de la web de la URCDP.

Por otra parte, el decreto establece que un conjunto de entidades con cometidos o actividades afines pueden nombrar un único delegado de protección de datos, al igual que varias entidades públicas, siempre que pueda cumplir las funciones legalmente establecidas en relación a todas y cada una de ellas.

g. El ámbito territorial

La Ley se aplica a todo tratamiento de datos personales que se realice en territorio uruguayo.

Para aquellos responsables y encargados de tratamiento radicados en el exterior del país, se prevé su aplicación si las actividades de tratamiento están relacionadas con la oferta de bienes y servicios dirigidos a los habitantes de la República, si las normas de derecho internacional público o un contrato así lo disponen, o si en el tratamiento se utilizan medios situados en el país. Esta ampliación del ámbito territorial fue establecida por el artículo 37 de la Ley N° 19.670, de 15 de octubre de 2018, y reglamentada por los artículos 1° y 2° del Decreto Nº 64/020, de 17 de febrero de 2020, que precisan el alcance de los supuestos incluidos de las obligaciones de responsables y encargados.

En este sentido, existen ejemplos ilustrativos, aunque teniendo en cuenta que el análisis debe realizarse caso a caso: se puede mencionar el caso de un hotel o una empresa de reparto internacional que ofrece servicios a habitantes de Uruguay mediante promociones específicamente diseñadas para nuestro país, con la posibilidad de abonar en moneda local y en idioma español, y en ese sentido, encontrarse alcanzada por el ámbito territorial de la Ley en función de las presunciones establecidas en el propio decreto.

h. Notas finales

La reglamentación ha venido a precisar algunos aspectos relevantes de los artículos 37 a 40 de la ley precitada, lo que debe complementarse además con las distintas resoluciones y dictámenes emitidos por el Consejo Ejecutivo de la URCDP en el marco de sus competencias legales y reglamentarias.

A través de estas modificaciones a la estructura del sistema de protección de datos en Uruguay podemos afirmar que se ha elevado el nivel de garantías que éste brinda a la población, siguiendo los lineamientos de los estándares definidos por la Red Iberoamericana de Protección de Datos y en línea con los más modernos desarrollos normativos en la materia.

Normativa

Artículos 37 a 40 de la Ley Nº 19.670, de 15 de octubre de 2018

Artículo 37.- El tratamiento de datos personales estará sometido a la Ley Nº 18.331, de 11 de agosto de 2008 y sus modificativas y concordantes, cuando se efectúe por un responsable o encargado de tratamiento establecido en territorio uruguayo, lugar donde ejerce su actividad. En caso de que no e sté establecido en ese territorio, dicha ley regirá:

A) Si las actividades del tratamiento están relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República o con el análisis de su comportamiento.

B) Si lo disponen normas de derecho internacional público o un contrato.

C) Si en el tratamiento se utilizan medios situados en el país. Exceptúanse los casos en que los medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable del tratamiento designe un representante, con domicilio en territorio nacional, ante la Unidad Reguladora y de Control de Datos Personales, a fin de cumplir con las obligaciones previstas por la Ley Nº 18.331, de 11 de agosto de 2008.

Artículo 38.- Cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, deberá informar inmediata y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la Unidad Reguladora y de Control de Datos Personales, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy). La reglamentación determinará el contenido de la información correspondiente a la vulneración de seguridad.

Artículo 39.- Sustitúyese el artículo 12 de la Ley Nº 18.331, de 11 de agosto de 2008, por el siguiente: "ARTÍCULO 12. (Principio de responsabilidad).- El responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de la violación de las disposiciones de la presente ley. En ejercicio de una responsabilidad proactiva, deberán adoptar las medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación. La reglamentación determinará las medidas que correspondan según los tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización".

Artículo 40.- Las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos deberán designar un delegado de protección de datos. Sus funciones principales serán:

A) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

B) Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.

C) Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales.

D) Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales. El delegado deberá poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuará con autonomía técnica.

E) Decreto N° 64/020, de 17 de febrero de 2020

VISTO: los artículos 37 a 40 de la Ley N° 19.670 de 15 de octubre de 2018;

RESULTANDO: que contienen nuevas disposiciones en materia de protección de datos personales que impactan en el sistema nacional y procuran brindar a las personas un nivel de protección acorde a los nuevos desarrollos tecnológicos y a la evolución en las formas de tratamiento de los datos personales;

CONSIDERANDO:

I) que el derecho a la protección de datos personales es un derecho inherente a la persona humana comprendido en el artículo 72 de la Constitución de la República, como lo reconoce el artículo 1° de la Ley N° 18.331 de 11 de agosto de 2008;

II) que a efectos del dictado de esta reglamentación se han tenido en cuenta las disposiciones y doctrinas más recientes, tales como el Reglamento Europeo N° 2016/679 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, los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001 -ambos aprobados por Ley N° 19.030 de 27 de diciembre de 2012-, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, suscrito por la República Oriental del Uruguay el 10 de octubre de 2018;

III) que la ubicuidad de las personas en el mundo digital y la protección de sus derechos requiere atender debidamente el alcance de la protección de su información

personal, lo que corresponde complementar con los mecanismos de control de cumplimiento en el ámbito internacional y las necesarias obligaciones de responsables y encargados, que no obstante situarse en el exterior del país, realizan tratamientos de datos de personas que se ubican en éste;

IV) que por otra parte, por la trascendencia y el volumen de la información tratada por múltiples organizaciones respecto de las personas y las eventuales vulneraciones de seguridad, resulta imprescindible establecer un régimen claro en lo que atañe al procedimiento que se debe realizar en esas situaciones;

V) que el estado actual de la protección de datos personales ha llevado a fortalecer el principio de responsabilidad, en su evolución hacia un principio de responsabilidad demostrada, que impone al responsable y encargado en su caso, la obligación de demostrar que las actividades de tratamiento cumplen con la legislación aplicable. En ese sentido se ha incorporado un mínimo de medidas -entre las que se encuentran la protección de datos desde el diseño y por defecto y las evaluaciones de impacto previas-, máxime en los casos en que existe un mayor riesgo para las personas;

VI) que, asimismo, la Ley que se reglamenta ha incorporado la figura del delegado de protección de datos, el que debe contar con las competencias necesarias e independencia técnica para cumplir sus funciones en forma apropiada. Su designación resulta pertinente en los casos de entidades públicas, entidades que traten datos sensibles o que realicen tratamiento de grandes volúmenes de datos personales;

VII) que acorde con lo previsto en el artículo 32 de la Ley N° 18.331 de 11 de agosto de 2008, se consultó al Consejo Consultivo de la Unidad Reguladora y de Control de Datos Personales y se contemplaron, en lo pertinente, sus planteos, elevándose proyecto de reglamentación por parte del Consejo Ejecutivo de dicha Unidad.

ATENTO: a lo expuesto y a lo previsto por el artículo 168 ordinal 4° de la Constitución de la República;

EL PRESIDENTE DE LA REPÚBLICA
- actuando en Consejo de Ministros -
DECRETA:

CAPÍTULO I - ÁMBITO TERRITORIAL

Artículo 1

Ámbito territorial. A los efectos de lo dispuesto por el artículo 37 de la Ley N° 19.670 de 15 de octubre de 2018, se entenderá que el responsable o encargado de tratamiento se encuentra establecido en territorio uruguayo cuando realice en éste una actividad estable, sin importar la forma jurídica adoptada para ello.

A) En caso que el responsable o encargado no se encuentre establecido en territorio uruguayo, la Ley Nª 18.331 de 11 de agosto de 2008 y esta reglamentación igualmente regirán si:

B) Las actividades de tratamiento de datos están relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República lo cual se apreciará a través de elementos tales como el uso del idioma, la referencia al pago en moneda nacional o la provisión de servicios conexos -no necesariamente prestados por el responsable o encargado- en territorio uruguayo.

C) Las actividades de tratamiento de datos están relacionadas con el análisis del comportamiento de los habitantes de la República, incluyendo las destinadas a la elaboración de perfiles, siendo aplicable al efecto en especial lo dispuesto en el artículo 16 de la ley N° 18 331 de 11 de agosto de 2008.

D) Lo dis-ponen normas de derecho internacional público o un contrato. En ningún caso los contratantes podrán excluir la aplicación de la ley nacional, cuando ésta corresponda.

E) En el tratamiento se utilizan medios situados en el país, tales como redes de información y de comunicación, centros de datos e infraestructura informática en general.

Artículo 2

Alcance de las obligaciones. En las situaciones previstas en el inciso segundo del artículo anterior, los responsables y encargados de tratamiento, en su caso, deberán dar cumplimiento a las obligaciones previstas en la Ley N° 18.331 de 11 de agosto de 2008, y modificativas, incluyendo el registro de sus bases de datos y brindar la información de contacto correspondiente ante la Unidad Reguladora y de Control de Datos Personales.

Se exceptúa de la obligación de registro de las bases de datos, las situaciones referidas en el literal d) del inciso segundo del artículo 1° siempre que los medios se utilicen exclusivamente con fines de tránsito y el responsable del tratamiento designe un representante domiciliado en territorio nacional ante la Unidad Reguladora y de Control de Datos Personales.

CAPÍTULO II - VULNERACIONES DE SEGURIDAD

Artículo 3

Medidas de Seguridad. El responsable y el encargado de tratamiento, en su caso deberán adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales. A estos efectos valorarán la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Constatada la existencia de incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables y encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados.

Artículo 4

Comunicación de vulneraciones de seguridad. El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarlo a la Unidad Reguladora y de Control de Datos Personales en un plazo máximo de 72 horas de conocida la vulneración.

La comunicación a la Unidad Reguladora y de Control de Datos Personales deberá contener información relevante, tal como la fecha cierta o estimada de la ocurrencia de la vulneración, su naturaleza, los datos personales afectados, y los posibles impactos generados.

En caso que la vulneración hubiere sido conocida por el encargado del tratamiento, éste la comunicará de inmediato al responsable del tratamiento.

Este último, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarla en un lenguaje claro y sencillo a los titulares de los datos que hayan sufrido una afectación significativa en sus derechos.

Solucionada la vulneración, el responsable del tratamiento deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la Unidad Reguladora y de Control de Datos Personales.

CAPÍTULO III - MEDIDAS DE RESPONSABILIDAD PROACTIVA

Artículo 5

Responsabilidad proactiva. Los responsables y encargados de tratamiento de datos personales en su caso, deberán adoptar, en atención a la naturaleza de los datos, los tratamientos que efectúen y los riesgos que impliquen, las medidas indicadas en el presente Capítulo y toda aquella que corresponda según lo dispuesto en el artículo 12 de la Ley N° 18.331 de 11 de agosto de 2008, en la redacción dada por el artículo 39 de la Ley N° 19.670 de 15 de octubre de 2018.

Para adoptar estas medidas se deberá tener en cuenta el estado de la técnica, el costo de su aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que aquél entrañe para los derechos de las personas.

Las medidas adoptadas deberán ser documentadas, revisadas periódicamente y evaluadas en su efectividad.

La documentación de las medidas deberá contener, como mínimo, la forma, medios y finalidad del tratamiento, los procedimientos orientados a dar cumplimiento a las normas de protección de datos, la planificación de mecanismos para responder a vulneraciones de seguridad, y el rol del delegado de protección de datos cuando corresponda.

Esta documentación deberá estar disponible ante la solicitud efectuada por la Unidad Reguladora y de Control de Datos Personales.

Artículo 6

Evaluación de impacto en la protección de datos personales. En forma previa al inicio del tratamiento, el responsable y el encargado del tratamiento en su caso, deberán realizar una evaluación de impacto en la protección de datos personales, cuando en las operaciones de tratamiento pueda:

A) Utilizarse datos sensibles como negocio principal.

B) Proyectarse un tratamiento permanente o estable de los datos especialmente protegidos a que refiere el Capítulo IV de la Ley N° 18.331 de 11 de agosto de 2008, o de los datos vinculados a la comisión de infracciones penales, civiles o administrativas.

C) Implicar una evaluación de aspectos personales de los titulares con el fin de crear o utilizar perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad de comportamiento y solvencia financiera y localización.

D) Llevarse a cabo el tratamiento de datos de grupos de personas en situación de especial vulnerabilidad y, en particular, de menores de edad o personas con discapacidad.

E) Producirse un tratamiento de grandes volúmenes de datos personales.

F) Transferirse datos personales a otros Estados u organizaciones internacionales respecto de los que no exista nivel adecuado de protección.

G) Otros que determine la Unidad Reguladora y de Control de Datos Personales.

Artículo 7

Contenido de la evaluación de impacto en la protección de datos personales - La evaluación prevista en el artículo precedente deberá contener, como mínimo:

A) Una descripción sistemática del tratamiento a realizar y su finalidad.

B) Una evaluación del tratamiento con relación al cumplimiento de la normativa de protección de datos personales.

C) Una evaluación de los riesgos para los derechos de los titulares de los datos.

D) Un detalle de las medidas de seguridad y de los mecanismos para demostrar el cumplimento de la normativa de protección de datos personales.

En relación a los tratamientos ya iniciados y que se encuentren incluidos en los supuestos del artículo 6°, el responsable y el encargado de tratamiento en su caso, deberán realizar esta evaluación en un plazo de 1 año a contar de la publicación de este decreto en el Diario Oficial.

Si del resultado de la correspondiente evaluación surge un riesgo potencial y significativo para los derechos de los titulares de los datos, el responsable y el encargado del tratamiento en su caso, deberán ponerlo en conocimiento de la Unidad Reguladora y de Control de Datos Personales, con información pormenorizada de las medidas que adoptaron o adoptarán, y en este último caso el respectivo plazo.

A los efectos de la realización de la evaluación de impacto, según el tipo o volumen de datos y de su tratamiento, la Unidad antes citada fijará criterios que contribuyan al cumplimiento de la obligación prevista en el presente artículo.

Artículo 8

Privacidad por diseño. El responsable y el encargado de tratamiento, en su caso, deberán incorporar en el diseño de las bases de datos, las operaciones de tratamiento, las aplicaciones y los sistemas informáticos, medidas dirigidas a dar cumplimiento a la normativa de protección de datos personales. A esos efectos, previo al tratamiento y durante todo su desarrollo, aplicarán medidas técnicas y organizativas apropiadas, tales como:

A) Técnicas de disociación, seudonimización y minimización de datos.

B) Mecanismos para asegurar el ejercicio de los derechos de los titulares de los datos personales.

C) Documentación de los consentimientos o de otros fundamentos que legitimen el tratamiento.

D) Tiempo de conservación de los datos, considerando sus tipos y su tratamiento.

E) Adopción de planes de contingencia que incluyan medidas de seguridad de la información.

F) Análisis funcionales y modelos de arquitectura de los datos.

G) Otras medidas establecidas por la Unidad Reguladora y de Control de Datos Personales.

Artículo 9

Privacidad por defecto. El responsable y el encargado del tratamiento, en su caso, aplicarán las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Esta obligación refiere a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su comunicación.

CAPÍTULO IV - DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

Artículo 10

Alcance. De acuerdo con lo dispuesto en el artículo 40 de la Ley N° 19670 de 15 de octubre de 2018, deberán designar un delegado de protección de datos personales:

A) Entidades públicas, estatales o no estatales y las privadas total o parcialmente de propiedad estatal.

B) Entidades privadas que traten datos sensibles como negocio principal. De conformidad con lo establecido por el artículo 4° literal E) de la Ley N° 18.331 de 11 de agosto de 2008, son datos sensibles aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

C) Entidades privadas que realicen tratamiento de grandes volúmenes de datos.

Se considera tratamiento de grandes volúmenes de datos cualquier actividad en la que se realice un tratamiento de datos personales de más de 35.000 personas.

La Unidad Reguladora y de Control de Datos Personales, de oficio o ante gestión realizada ante la misma, podrá expedirse sobre la pertinencia de que una entidad privada cuente con un delegado de protección de datos.

Artículo 11

Funciones de los delegados de protección de datos. Las funciones principales de los delegados de protección de datos serán:

A) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

B) Supervisar el cumplimiento de la normativa sobre dicha protección en la entidad o entidades para las que preste servicios.

C) Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.

D) Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

Artículo 12

Calidad y condiciones del delegado. El delegado de protección de datos podrá desempeñar sus funciones a través de cualquier modalidad contractual, sea que implique dependencia o no. Deberá contar con conocimientos en Derecho, especializados en materia de protección de datos personales, los que deberán acreditarse.

En el caso de que el delegado sea persona jurídica, deberá comunicarse a la Unidad Reguladora y de Control de Datos Personales cómo está integrado su órgano de administración, así como los datos de sus integrantes y de la persona o personas físicas que se designen para realizar la tarea.

Artículo 13

Posición del delegado de protección de datos. El delegado de protección de datos deberá participar de forma adecuada en todas las cuestiones relativas a la protección de datos personales.

Para desarrollar sus tareas en el desempeño de sus funciones, se le brindará pleno acceso a las bases de datos personales y a las operaciones de tratamiento. Actuará con autonomía técnica y no recibirá instrucciones en el desempeño de sus funciones específicas como delegado de protección de datos.

El delegado de protección de datos deberá guardar absoluta confidencialidad de las informaciones a las que tenga acceso por su calidad, siendo de aplicación lo establecido en el artículo 11 de la Ley N° 18.331 de 11 de agosto de 2008.

Este delegado podrá desempeñar otras funciones en cuanto no generen conflicto de intereses.

Artículo 14

Plazo de designación, cese o renuncia del delegado. Cuando corresponda la designación de un delegado de protección de datos personales, ésta deberá ser comunicada a la Unidad Reguladora y de Control de Datos Personales en un plazo de 90 días a contar del inicio del tratamiento.

Toda entidad que al momento de la entrada en vigencia del presente decreto se encuentre en la situación prevista en el artículo 40 de la Ley N° 19.670 de 15 de octubre de

2018, deberá designar al delegado de protección de datos en el plazo previsto en el inciso anterior, a contar de la publicación del presente decreto en el Diario Oficial.

Todo cese o renuncia de un delegado de protección de datos deberá ser comunicada a la Unidad Reguladora y de Control de Datos Personales en el plazo previsto en el inciso anterior, debiendo designarse un nuevo delegado.

El delegado de protección de datos podrá comunicar directamente a la Unidad Reguladora y de Control Datos Personales su cese o renuncia.

Artículo 15

Posibilidad de designar un único delegado. Un conjunto de entidades con cometidos o actividades afines, podrán nombrar un único delegado de protección de datos siempre que éste pueda cumplir cabalmente con las funciones legalmente establecidas en relación a todas y cada una de ellas.

También podrán designar un único delegado de protección de datos en los términos señalados en el presente artículo, varias entidades públicas que formen parte de la misma estructura administrativa, lo que se efectuará por resolución fundada, en especial en cuanto a la viabilidad del cabal cumplimiento antes referido.

La Unidad Reguladora y de Control de Datos Personales podrá requerir la designación de delegados de protección de datos adicionales a fin de proteger los derechos de los titulares de los datos en los casos previstos en la presente disposición.

CAPÍTULO V - NORMAS FINALES

Artículo 16

Criterios y sanciones. La Unidad Reguladora y de Control de Datos Personales fijará criterios para el cumplimiento, auditoría y evaluación de las medidas establecidas en la Ley N° 18.331 de 11 de agosto de 2008 y en el presente decreto. El Consejo Ejecutivo de esa Unidad impondrá las sanciones correspondientes a los incumplimientos a las disposiciones del presente decreto de conformidad con lo dispuesto por el artículo 35 de la Ley N° 18.331 de 11 de agosto de 2008, en la redacción dada por el artículo 152 de la Ley N° 18.719 de 27 de diciembre de 2010 y el artículo 83 de la Ley N° 19.355 de 19 de diciembre de 2015.

Artículo 17

Deróganse los artículos 7° y 8° del Decreto N° 414/009 de 31 de agosto de 2009.

Artículo 18

Comuníquese, publíquese.

TABARÉ VÁZQUEZ - JORGE VÁZQUEZ - RODOLFO NIN NOVOA - DANILO ASTORI - JOSÉ BAYARDI EDITH MORAES - VÍCTOR ROSSI - GUILLERMO MONCECCHI - ERNESTO MURRO - JORGE BASSO - ENZO BENECH - BENJAMÍN LIBEROFF - ENEIDA de LEÓN - MARINA ARISMENDI