

Ciudad Autónoma de Buenos Aires, 29 de setiembre del 2022.-

Jefatura de Gabinete de Ministros de la Nación

Directora de la Agencia de Acceso a la Información Pública

Mg. Beatriz Anchorena

S/D

Tenemos el agrado de dirigirnos a Ud. en el marco del proceso participativo establecido en el Reglamento General para la Elaboración Participativa de Normas, aprobado por el artículo 3° del Decreto N° 1172/03 (Anexo V) en relación a la propuesta del anteproyecto de la Ley de Protección de Datos Personales<sup>1</sup>.

La Defensoría del Pueblo, por Ley 1845, ha sido designada órgano de control de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa, de conformidad a lo establecido por el artículo 16 de la Constitución de la Ciudad de Buenos Aires. Dicha función es llevada dentro de la Institución por el Centro de Protección de Datos Personales, en base a dicho conocimiento acercamos algunos comentarios.

### **I. Comentarios generales**

En primer lugar, celebramos y apoyamos el impulso en pos de reformar la Ley Nacional de Protección de Datos Personales. Asimismo el proceso de consulta iniciado por la Agencia de Acceso a la Información Pública para la actualización de la Ley 25.326 de Protección de Datos Personales es una herramienta de importancia dado que permitirá que la norma se nutra de aportes multidisciplinarios así como también validar e impulsar la iniciativa.

---

<sup>1</sup> [BOLETIN OFICIAL REPUBLICA ARGENTINA - AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA - Resolución 119/2022](#)

Concordamos con la imperiosa necesidad de reformar la legislación en especial porque el avance tecnológico ha impactado particularmente en el derecho a la privacidad y la protección de los datos personales. De igual modo entendemos muy acertado seguir los lineamientos del Reglamento Europeo de Protección de Datos Personales (RGPD) porque es una norma guía que se ajusta a nuestro sistema jurídico y condensa los aspectos previstos en las legislaciones más modernas. Sin lugar a dudas el anteproyecto constituye una mejora respecto del estado normativo actual al incorporar la figura del delegado de protección de datos, temas relativos con la seguridad de la información, la notificación de incidentes, la posibilidad de ejercer la portabilidad, la regulación sobre transferencia internacional de datos personales, aspectos sobre decisiones automatizadas, cuestiones sobre responsabilidad proactiva, el concepto de la protección de la privacidad desde el diseño y multas entre otros.

También las previsiones relativas al ámbito de aplicación *material* y *territorial* contenido en los Arts. 3 y 4 dan robustez al derecho a la privacidad y permitirán que el derecho a la protección de datos personales no quede supeditado ante al derecho a la información y/o la libertad de expresión. Respecto del ámbito de aplicación territorial, las opciones contempladas en el articulado relativas a “quien realiza tratamiento de datos en el territorio, efectúa actividades o se aplica la norma argentina” constituyen una solución a los dilemas que impone la globalidad.

Asimismo es medular que la legislación garantice el cumplimiento de la protección de datos personales ante el desarrollo de la inteligencia artificial y las neurotecnologías y tecnologías emergentes, aspectos que analizamos en los puntos II. g) y h). Por ello las previsiones sobre el “principio de neutralidad tecnológica” incorporado al anteproyecto en el Art. 5 constituyen una posición necesaria. En efecto, ante la creciente digitalización creemos de importancia recalcar que hoy en día ya no es posible una división entre el mundo on-line y el mundo off-line, atento a ello el cuerpo normativo a sancionar tendrá plena vigencia sin importar el soporte o medio en el que se estén tratando los datos personales.

En otro orden, advertimos que el anteproyecto prevé ciertas definiciones que han adquirido relevancia, tales como “datos biométricos” o “datos genéticos”. Asimismo, sería importante incluir otras definiciones como “datos neuronales” que deberían incluirse en la tipología de datos sensibles.

Como último comentario general, creemos, que por una cuestión de técnica legislativa, sería deseable reestructurar el cuerpo legal en lo que hace “Principios” a fin de que queden concentrados debajo de un único Título. Por iguales razones entendemos que sería más

adecuado no legislar en este cuerpo sobre la “Acción de Habeas Data” (Capítulo 9) sobre todo porque existen remisiones a la normativa general en materia de acción de amparo.

## II. Comentarios específicos

Consideramos central el enfoque de la protección de datos personales como derecho humano fundamental. Su intrínseca relación con la protección a la privacidad constituye un rasgo concordante con la tradición y el sistema jurídico que rige en nuestro país. En efecto, otros modelos normativos poseen legislaciones sectoriales y teniendo en cuenta que nuestra legislación no lo prevé resulta clave considerarlo como un derecho inalienable de las personas centrado en la dignidad humana.

En tal sentido, adquieren especial relevancia el cumplimiento de idénticas previsiones de los distintos tratados internacionales sobre derechos humanos como así lo destacan los “Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales” del Comité Jurídico Interamericano. Hay disposiciones relativas a la privacidad, la protección del honor personal y la dignidad, la libertad de expresión y de asociación, y el libre flujo de información en los principales sistemas de derechos humanos del mundo.

El concepto de privacidad está claramente establecido en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre y en el artículo 11 de la Convención Americana sobre Derechos Humanos<sup>2</sup>. Por otra parte, el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre dispone lo siguiente: toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar. Además, el artículo IX (“Toda persona tiene el derecho a la inviolabilidad de su domicilio”) y el artículo X (“Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia”). Asimismo, el artículo 11 de la Convención Americana sobre Derechos Humanos dispone lo siguiente: 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques<sup>3</sup>. Sin

<sup>2</sup> Véanse también la Declaración Universal de Derechos Humanos (art. 12, 18-20), el Pacto Internacional de Derechos Civiles y Políticos (art. 17-19), el Convenio para la protección de los derechos humanos y de las libertades fundamentales (art. 8-10), Convención sobre los Derechos del Niño (art. 16), la Carta de los Derechos Fundamentales de la Unión Europea (art. 1, 7, 8, 10-12) y la Carta Africana sobre los Derechos Humanos y de los Pueblos (art. 5, 8-11 y 28).

<sup>3</sup> Además, el artículo 14 de la Convención Americana (“Derecho de Rectificación o Respuesta”) dispone lo siguiente: 1. Toda persona afectada por informaciones inexactas o agravantes emitidas en su perjuicio a través de medios de difusión

lugar a dudas ese es el punto de partida de bien jurídico que tutela este anteproyecto. Por ello resultan adecuadas las previsiones de los artículos 1 y 5 del anteproyecto.

## ***II. a) Principios***

Los principios contenidos en el anteproyecto constituyen una pieza central en el cuerpo normativo, dado que concentran el fundamento de la reforma y por ende serán una guía ante eventuales casos conflictivos o dudosos.

Sin perjuicio de ello creemos apropiado por ser más preciso y concreto **incluir una directriz sobre “proporcionalidad y razonabilidad”**. Se trata de una herramienta clásica del Derecho muy útil para analizar el tratamiento de datos personales además de ser más precisa que otras menciones que contiene el documento como por ejemplo el principio de minimización. Ese criterio es adoptado por los Estándares de Protección de Datos de los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos Personales (REDIP)<sup>4</sup>. Es decir, en caso de un eventual daño en la protección de los derechos a la protección de datos personales, deberían ponderarse con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a los principios fundamentales de derechos humanos.

## ***II. b) Bases para el tratamiento de datos personales - Consentimiento***

Sin dudas el modelo adoptado por el anteproyecto que admite distintos supuestos para el tratamiento de los datos personales, se encuentra en línea con el Reglamento Europeo de Protección de Datos Personales (RGPD). Como es sabido, este paradigma también fue receptado en destacados documentos como los Estándares de Protección de Datos de los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos Personales (REDIP) y el documento emitido por el Comité Jurídico Interamericano de la OEA (CJI) del año 2021, sobre requisitos mínimos en materia de protección de datos personales<sup>5</sup>.

Sin perjuicio de ello **tenemos dudas respecto del apartado final del Art. 13 del anteproyecto en lo que refiere a “...ya sea mediante una declaración o una clara acción afirmativa” toda vez que ello podría generar dudas interpretativas**. De tal modo podría

---

legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

<sup>4</sup> “7. Ponderación del derecho a la protección de datos personales 7.1. Los Estados Iberoamericanos podrán exentar, en su derecho interno, el cumplimiento de los principios y derechos previstos en los presentes Estándares, exclusivamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales. 7.2. Esta exención deberá requerir de un ejercicio de ponderación con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a las reglas y criterios que establezcan los Estados Iberoamericanos en su derecho interno”. [Estándares RIPD](#)

<sup>5</sup> [Principios Actualizados sobre la Privacidad y la Protección de Datos Personales](#)

habilitarse una suerte de consentimiento tácito. Vale recordar que el consentimiento además tiene efectos concretos respecto del ejercicio de los derechos de rectificación, supresión, información y oposición (Art. 14 del anteproyecto), garantías que podrían verse afectadas si no se reconoce certeza en consentimiento.

### ***II. c) Grupos vulnerables - NNyA***

Resulta central una previsión especial sobre ciertos grupos humanos. En tal dirección, la previsión respecto de los NNyA es muy auspiciosa, así como la línea de trabajo en información y capacitación. Entendemos que las prácticas preventivas son fundamentales para un uso adecuado, cuidado de la privacidad y los datos personales en entornos digitales. También **es vital reconocer la llamada “capacidad progresiva”** prevista por nuestro Código Civil y Comercial. En igual sentido vale mencionar la “Observación General Nro. 25” del Comité de los Derechos del Niño de Naciones Unidas<sup>6</sup> que dispone que los Estados parte deben aplicar plenamente los derechos y garantías reconocidos en la Convención al entorno digital no diferenciando por ende entre mundo real y virtual.

También en línea con lo comentado **podría incluirse otras personas en situación de vulnerabilidad**. Así por ejemplo, se trataría de sujetos con capacidad restringida y/o con incapacidad de acuerdo a la previsión del Código Civil y Comercial de la Nación y la Convención Internacional sobre los Derechos de las Personas con Discapacidad Ley 26.378. También siguiendo el criterio señalado podría trabajarse en una categoría sobre grupos desaventajados como por ejemplo lo hizo la Secretaría de Comercio Interior de la Nación en la Resolución 139/2020 que determinó que son “consumidores hiper vulnerables”.<sup>7</sup>

### ***II. d) Derechos***

El Capítulo 4 referido a los derechos de los titulares de los datos personales constituye un avance respecto de la ley actual. Resulta destacable la prohibición de supresión de información personal cuando sea necesario para la consolidación del proceso de memoria, verdad y justicia y de los Derechos Humanos en general.

Creemos que el apartado relativo a la supresión de información personal (art. 29) sin duda permite su ejercicio en el mundo virtual. En efecto, es necesaria la voz estatal respecto de los incesantes reclamos contra los intermediarios con el fin de que desindexen y/o supriman contenidos que contienen información personal. Como señala el Centro de Estudios para la Libertad de Expresión de la Universidad de Palermo se trata de un problema que además afecta particularmente a las mujeres “Se trata de casos que siguen, en general, un patrón

<sup>6</sup> [Observación General Nro. 25](#)

<sup>7</sup> [Secretaría de Comercio Interior de la Nación en la Resolución 139/2020](#)

similar: personas famosas, usualmente mujeres, demandan a Yahoo y Google por los resultados que encuentran asociados a sus nombres. Alegan que son injustamente vinculadas a sitios que promueven la pornografía o la prostitución y que sus imágenes son usadas por los buscadores sin su consentimiento”<sup>8</sup>. Atento a ello **creemos que hubiera sido mejor una previsión más explícita. Como es sabido, esta cuestión es una garantía para los ciudadanos europeos. Se encuentra contenido en el RGPD que lo denomina “derecho al olvido”** en razón de haberse resuelto de ese modo en el caso “Costeja” del año 2014 por parte del Tribunal de Justicia de la Unión Europea.

## ***II. e) Obligaciones***

Dado el cambio de paradigma respecto del principio de responsabilidad proactiva previsto en los art. 11 y 37 del anteproyecto, **sería deseable por norma reglamentaria que se prevea que quienes sean responsables de tratamiento de datos puedan generar controles en sí mismos, como resultado de hacer un proceso de debida diligencia en la organización que integran. En este caso, creemos que sería necesario que se prevea un entrenamiento y educación obligatorio dentro de las entidades que tratan datos personales, donde todos deberían capacitarse**, saber cómo actuar ante cada caso y entender cuáles son las consecuencias de no hacerlo. No solo quienes ocupen sectores especializados. Por este motivo, es necesaria la utilización de herramientas de evaluación y gestión de riesgos, previo a cada desarrollo. Siempre tratando de minimizar los datos y no exceder la finalidad.

## ***II. f) Inteligencia Artificial (IA) y protección de datos personales***

Ante la ausencia de legislación específica sobre IA creemos que constituye una oportunidad en pos de la protección de los derechos de las personas que la nueva legislación en materia de protección de datos personales pueda precisar o incluir breves aclaraciones sobre la necesidad de que esa tecnología garantice el respeto de la protección de datos personales. Ya algunos organismos internacionales<sup>9</sup> advirtieron que se deben prever medidas de rendición de cuentas de los responsables y, también, la evaluación del potencial impacto en los derechos previo al desarrollo y/o uso de la IA, entre otras formas de análisis continuo del desempeño y los impactos de la IA en los seres humanos. El anteproyecto deja vacío

<sup>8</sup> [Jurisprudencia - Intermediarios](#)

<sup>9</sup> Evaluación de la criticidad de las soluciones de inteligencia artificial. Las medidas que se adopten han de estar centradas en el ser humano y ser proporcionales a los riesgos de vulneración de los derechos humanos, en especial la discriminación, y la protección de datos, así como a la complejidad o criticidad de una solución de procesamiento de datos. A continuación se enumeran algunos enfoques adecuados: Fase de planificación. Fase de pruebas y correcciones – supervisión. La criticidad de los datos y la finalidad prevista. Realización de la evaluación periódica de los sistemas de inteligencia artificial, registro de esta y mantenimiento de datos a disposición de auditorías externas y organismos reguladores. Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci, <https://undocs.org/es/A/HRC/46/37> párr. 50

legales y lagunas interpretativas respecto del tratamiento de datos personales mediante la utilización de tecnologías de IA. En este sentido se recomienda que en los estudios de impacto a la privacidad que prevé el anteproyecto se incorpore la participación de múltiples actores pertenecientes a la sociedad civil, a los círculos académicos y a las organizaciones gubernamentales y no gubernamentales.

## ***II. g) Neurotecnologías, tecnologías emergentes y protección de datos personales***

En línea con lo señalado en el apartado precedente sobre IA, **estimamos necesario que esta nueva ley incorpore conceptos que se están discutiendo en el mundo de las tecnologías emergentes y las neurotecnologías.** En los últimos años la implementación de las neurotecnologías está aumentando rápidamente. Es sabido que determinadas aplicaciones permiten una conexión bidireccional entre el sistema nervioso central de un individuo (cerebro y médula espinal) y un sistema electrónico. En este marco, el cerebro humano aparece como una especie de “disco duro” que contiene documentos y memorias que se pueden consultar y guardar en un dispositivo externo. Es decir, se puede utilizar un disco o un ordenador para acceder a datos y explorarlos, eliminarlos o incluso modificarlos<sup>10</sup>.

Tal es así que la neurotecnología ofrece un enorme potencial en el campo médico para el tratamiento de trastornos neurológicos y mentales, como el Alzheimer, el Parkinson o la esquizofrenia. Incluso podría permitir que una persona amputada controle un miembro artificial a través del pensamiento. Al mismo tiempo, se aplica cada vez más en contextos fuera del área de la salud, en campos como la enseñanza, los juegos y el entretenimiento, donde el objetivo es influir en el cerebro de varias maneras, por ejemplo, a través de la "mejora de la memoria" o la "ingeniería cognitiva". Este proceso requiere la recopilación de datos neuronales y la decodificación de pensamientos. Si bien, estas aplicaciones pueden parecer limitadas o material para una novela de ciencia ficción. Sin embargo, a medida que gradualmente se vuelvan de uso generalizado, plantearán una serie de cuestiones éticas y legales que deben abordarse y anticiparse con una legislación moderna. Preguntas, tales como; ¿Quién debería tener acceso a los datos neurológicos acumulados obtenidos al medir la actividad neuronal? ¿Qué pasa si la interfaz cerebro-computadora llega a afectar la privacidad mental, la libertad cognitiva o el sentido de identidad personal del individuo? ¿Cómo podemos anticipar y monitorear el uso indebido de estos datos y el abuso potencial por parte de actores estatales y no estatales?

<sup>10</sup> Ver 28ª sesión del Comité Asesor (8-12 de agosto de 2022), Propuesta de investigación de Milena Costas Trascasas, “Evaluando el impacto de la neurotecnología en los derechos humanos: hacia el reconocimiento de los ‘neuroderechos’”.

En este sentido, y siempre teniendo presente la agenda de privacidad y datos personales, observamos que en su “Recomendación sobre innovación responsable en neurotecnología”, de 2019, la OCDE define la neurotecnología como “dispositivos y procedimientos utilizados para acceder, monitorear, investigar, evaluar, manipular y/o emular la estructura y función de los sistemas neuronales de personas físicas”<sup>11</sup>.

Asimismo, son varias organizaciones internacionales que han comenzado a reflexionar sobre el tema del impacto de la neurotecnología en la privacidad y han producido documentos iniciales, incluida la “Recomendación de la OCDE sobre innovación responsable en neurotecnología” antes mencionada.

En agosto de 2021 se emitió la Declaración del Comité Jurídico Interamericano sobre Neurociencias, Neurotecnologías y Derechos Humanos<sup>12</sup> que advirtió que “La ausencia de regulaciones específicas de las neurotecnologías, así como sus alcances e impactos, genera un riesgo de manipulación ilegítima de emociones, sentimientos y decisiones desde quienes produzcan estas tecnologías y/o controlen los grandes sistemas de inteligencia artificial (IA) que decodifican la información neuronal. Asimismo, el uso de estas neurotecnologías puede llegar a romper la última frontera natural de la persona, su intimidad mental, y con ello afectar la dignidad e identidad de cada ser humano”.

Por su parte, el Comité Jurídico Interamericano ha aprobado los “Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales” (CJI/doc. 638/21), estableciendo que los datos personales sólo pueden ser recopilados y usados para finalidades legítimas, debiéndose “adoptar medidas de privacidad y de seguridad reforzadas” para los datos más sensibles, como pueden ser en este caso los datos neuronales, que, “si se manejan o se divulgan de manera indebida, darían lugar a una intrusión profunda en la dignidad personal (...) o causar un riesgo de graves perjuicios para la persona”. Por ello, se ha reconocido la necesidad de adecuar a los tiempos actuales, las fórmulas tradicionales de protección del derecho a la vida privada.

El desarrollo de las neurotecnologías puede conducir al condicionamiento de la personalidad y a la pérdida de autonomía de las personas, y en ese marco, una de las preocupaciones más urgentes tiene que ver con las conductas maliciosas de quienes acceden a los datos de la actividad cerebral de las personas con fines de penetrar en su mente, condicionarla o aprovecharse de tal conocimiento. En tal sentido, es necesario buscar respuestas frente a la falta de desarrollo e implementación de un marco normativo

---

<sup>11</sup> Disponible en <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457>

<sup>12</sup> CJI/DEC. 01 (XCIX-O/21) [http://www.oas.org/es/sla/cji/docs/CJI-DEC\\_01\\_XCIX-O-21.pdf](http://www.oas.org/es/sla/cji/docs/CJI-DEC_01_XCIX-O-21.pdf)



específico de la protección de la privacidad de los datos neuronales, tanto conscientes como inconscientes. Asimismo, se encuentra establecido firmemente como principio el respeto de la finalidad de la recolección para la utilización de datos personales; sin embargo, ante las posibilidades de las neurotecnologías, genera inquietud que no se hayan desarrollado garantías adecuadas para que la información neuronal obtenida para fines médicos y de investigación científica, sea utilizada sólo para este fin, limitando la aplicación de las técnicas de descodificación que permitan identificar a una persona o hacerla identificable y, como consecuencia de desbordar esos límites, violar el santuario más profundo de su intimidad mental”.

Asimismo, el Comité Interamericano viene trabajando en el desarrollo de principios mínimos para recomendar a los Estados el tratamiento de estos datos, donde principalmente se enfoca en la necesidad de un consentimiento expreso y que sean considerados datos altamente sensibles<sup>13</sup>.

Por otra parte, el informe del Comité Internacional de Bioética de la UNESCO sobre cuestiones éticas y neurotecnología expresó <sup>14</sup> “Ahora bien, aunque existen marcos legales para proteger la vida privada de los consumidores, en lo que respecta a los riesgos éticos que pueden entrañar las neurotecnologías el vacío jurídico es prácticamente total. El sistema existente de protección de los derechos humanos no llega a abarcar todos los aspectos propios de las neurociencias, como la confidencialidad mental o el libre albedrío...”<sup>15</sup>.

Dentro de la ONU, el informe del Secretario General de la ONU de 2021 'Nuestra agenda común', la neurotecnología se menciona como un tema de derechos humanos fronterizo que hace necesaria la actualización o la clarificación del marco y los estándares de derechos humanos aplicables con miras a prevenir daños en los espacios digitales o tecnológicos.<sup>16</sup> Asimismo, durante su 28ª sesión (8-12.8.2022), el Comité Asesor del Consejo de Derechos Humanos discutió una propuesta de investigación titulada "Evaluación del impacto de la neurotecnología en los derechos humanos: hacia el reconocimiento de los 'neuroderechos'"<sup>17</sup>. También el reciente informe publicado por la Oficina del Alto

<sup>13</sup> [PROYECTO DE PRINCIPIOS INTERAMERICANOS EN MATERIA DE NEUROCIENCIAS, NEUROTECNOLOGÍAS Y DERECHOS HUMANOS](#)

<sup>14</sup> Disponible en <https://unesdoc.unesco.org/ark:/48223/pf0000378724>.

<sup>15</sup> Recomendaciones del Comité Internacional de Bioética de la UNESCO: <https://www.unesco.org/es/articulos/recomendaciones-del-comite-internacional-de-bioetica-de-la-unesco>

<sup>16</sup> Informe del Secretario General, septiembre de 2021, párr. 35.

<sup>17</sup> Op. cit.

Comisionado de las Naciones Unidas para Derechos Humanos: “El derecho a la privacidad en la era digital”<sup>18</sup> se menciona la cuestión.

A su turno en Europa, la Comisión Europea advirtió que se están desarrollando muchos metaversos que ello lo es con distintos fines: entretenimiento, sino también para trabajar juntos, desarrollar la creatividad artística, hacer simulaciones de la vida real destinadas a intervenciones médicas, preservación cultural, protección ambiental o prevención de desastres y mucho más. Es por ese motivo que consideraron que para regular y fomentar el metaverso deben contemplarse en los mundos virtuales tres aspectos: personas, tecnologías e infraestructura<sup>19</sup>.

En síntesis, observamos que los nuevos mundos virtuales están poniendo bajo mayor presión que los datos personales estén permanentemente protegidos.

### III. Conclusiones

En base a las consideraciones expuestas entendemos que la reforma de la ley constituye una gran oportunidad que sin duda eleva el estándar en materia de protección de datos personales, lo que será una mejora en los derechos de las personas.

En este punto, resaltamos la importancia de la protección de datos personales como un derecho humano fundamental anclado en el derecho a la privacidad reconocido así en instrumentos internacionales.

Asimismo, el diseño institucional referido a la transformación de una autoridad robusta por la posibilidad de imponer sanciones de envergadura constituye un avance sustancial para garantizar la protección de datos en el país.

En otro orden y como hemos señalado *ut-supra* creemos de importancia, dado el desarrollo legal que posee el tema, que en el enunciado de las definiciones se incluya a los “datos neuronales” y en la misma línea sería importante reparar que son datos altamente sensibles. Asimismo, es de importancia que se asegure el control de cada persona sobre su propia identidad, el respeto a la dignidad, la intimidad y la integridad de los datos personales, ante el uso de tecnologías inmersivas y procesos basados en neurotecnologías.

<sup>18</sup> Informe de la Oficina del Alto Comisionado de las Naciones Unidas para Derechos humanos “El derecho a la privacidad en la era digital” (2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement> (traducción propia)

<sup>19</sup> “Personas, tecnologías e infraestructuras: el plan de Europa para prosperar en el metaverso” DECLARACIÓN/22/5525: [https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT\\_22\\_5525](https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5525) (traducción propia)

Lo mismo respecto del consentimiento expreso e informado de dichos datos. Garantice la autodeterminación individual, soberanía y libertad en la toma de decisiones en el uso de tecnologías inmersivas y procesos basados en neurotecnologías, así como se asegure la confidencialidad de los datos obtenidos o relativos a sus procesos cerebrales y el pleno dominio y disposición sobre los mismos.

Para finalizar, confiamos que un próximo tratamiento parlamentario del anteproyecto permita una mejora normativa.

Atentamente.



**María Julia Giorgelli**

**Subordinadora**



**Eduardo Peduto**

**Coordinador**

**Centro de Protección de Datos Personales**

**Defensoría del Pueblo de la Ciudad de Buenos Aires**