

ORD N°: 031.-

REF.: Solicitud de ingreso de iniciativa de norma convencional constituyente referente a Derecho a la Protección de los Datos de Carácter Personal

Santiago de Chile, 25 de enero de 2022

De: Francisco Caamaño Rojas - Carolina Videla Osorio
Convencionales Constituyentes

A: María Elisa Quintero Cáceres
Presidenta de la Convención Constitucional

Por medio de la presente, nos dirigimos a usted en su calidad de presidenta de la Convención, según lo dispuesto en los artículos 81, 82 y 83 del Reglamento general de la Convención Constitucional, para presentar la siguiente iniciativa de norma constitucional que reconoce el Derecho a la Protección de los Datos de Carácter Personal, dirigida a la Comisión N°7 de Sistemas de Conocimiento, Ciencia y Tecnología, Cultura, Arte y Patrimonio, según se indica a continuación:

DERECHO A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos de carácter personal. El intercambio de datos y la magnitud de la recolección de información personal de parte de empresas privadas y autoridades públicas se ha multiplicado significativamente, lo que supone altos riesgos para las personas y la consecuente vulneración a la protección de sus datos. Esto plantea además un reto al ejercicio de otros derechos, como el derecho a la intimidad, a la vida privada, a la salud, educación y otros.

Los diversos tipos de tratamiento de datos que están en auge en sectores como el sanitario, farmacéutico, bancario, laboral, comercial, retail, seguros, educación, las plataformas digitales y *marketplaces*. Además, las diversas tecnologías o soluciones como la biometría, el internet de las cosas, smart cities y nuevas técnicas de big data e inteligencia artificial, así como la capacidad de los algoritmos de predecir y moldear el comportamiento de personas con altos grados de precisión, **hacen necesario consagrar el derecho a la protección de los datos con carácter de autónomo**. Por lo que es importante impulsar un rol más activo de las autoridades públicas, asimismo establecer una autoridad independiente y especializada que lleve a cabo sus tareas de manera libre de influencias externas para garantizar debidamente la eficacia y fiabilidad de la supervisión, fiscalización y sanción a las infracciones a este derecho y los demás derechos que les puedan ser adscritos¹.

¹ [Minuta redactada por Jessica Matus, presentada ante la Comisión de Economía de la Cámara de Diputados en la discusión del proyecto de ley que establece medidas para incentivar la protección de los derechos de los consumidores. Boletín N° 12.409-3.](#)

En un mundo donde ya casi no existen acciones cotidianas, compras, movimientos, decisiones y hábitos personales que no queden registrados en alguna base de datos, nuestro desafío es garantizar que **la libre circulación de la información en ningún caso justifique una reducción al nivel de protección de los datos de las personas**².

Si bien, la protección de datos de carácter personal está consagrada en la actual Constitución Política, la vulneración de este derecho fundamental es sistemática, por lo que **se propone un modelo global de protección de datos para afrontar los desafíos relativos a su protección efectiva**.

La información relativa a las personas³ no está sujeta al derecho de propiedad⁴. El derecho a la protección de datos de carácter personal es un derecho fundamental relativamente nuevo, vinculado con anterioridad de manera estrecha al derecho a la vida privada⁵, pero que luego emerge como un derecho fundamental autónomo⁷ seguido del derecho de acceso a Internet⁸ más amplio⁹ y con características propias. Esto sucedió gracias al reconocimiento jurisprudencial internacional por parte del Tribunal Constitucional Federal Alemán (1983) y del Tribunal Constitucional Español (1978). La autoridad alemana declaró que, a partir del derecho general de la personalidad, *“existe para el individuo, derivada de la autodeterminación, [el derecho] de decidir básicamente por sí mismo, cuándo y dentro de qué límites, procede revelar situaciones referentes a la vida propia”*. Por su parte, la autoridad española consideró que *“la protección de datos personales es un derecho distinto de la intimidad, tanto en su función como en su objeto y contenido”*¹⁰.

En vista de la necesidad de alcanzar un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos y después de años de debate, en 1981 la Comunidad Europea aprobó el Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108)¹¹. Este instrumento legislativo, junto con la Carta de los Derechos Fundamentales de la Unión Europea¹², el Reglamento General de Protección de Datos¹³ y otros a nivel internacional, han establecido las bases para la protección de la información personal, pues han sido diseñados para reforzar los derechos de las personas en cuanto a la protección de su información.

² [Roldán, S \(7 de Enero, 2021\).El "Health Data Hub", la controvertida plataforma que centraliza los datos de salud franceses, ha sido paralizado.La Tribune.](#)

³ [Flacso. \(2021\).Carta Magna Digital.](#)

⁴ [Lucas, A., Devèze, J., Frayssinet, \(2001\).Derecho informático y de Internet. UFP.](#)

⁵ [Derieux, E. \(2015\). Privacidad y datos de carácter personal - Derecho a la protección y «derecho al olvido» frente a la libertad de expresión.](#)

⁶ [Clément-Fontaine, M. \(2017\).L'union du droit à la protection des données à caractère personnel et du droit à la vie privée.](#)

⁷ [Diario Oficial de las Comunidades Europeas \(2000\). Carta de Derechos Fundamentales de la unión Europea. Artículo 7 y 8.](#)

⁸ [Cassin, R\(s.f\).Derechos digitales y fundamentales.](#)

⁹ [Convención Europea de Derechos Humanos.\(2020\). Guía sobre el artículo 8 del convenio Europeo de Derechos Humanos: Derecho al respecto de la vida privada y familiar: Actualizado hasta el 31 de diciembre 2019.](#)

¹⁰ [Contreras, Pablo. \(2020\). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios constitucionales*, 18\(2\), 87-120. <https://dx.doi.org/10.4067/S0718-52002020000200087>](#)

¹¹ [Unión Europea \(1981\). Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.](#)

¹² [Diario Oficial de las Comunidades Europeas \(2000\). Carta de Derechos Fundamentales de la unión Europea.](#)

¹³ [Unión Europea \(2016\) Reglamento General de Protección de Datos](#)

Uno de los Protocolos adicionales al referido Convenio 108, abierto a la firma desde noviembre de 2021, obliga a las partes a crear autoridades de control que ejerzan sus funciones con total independencia y que constituyan un elemento de la protección efectiva de las personas en lo que respecta al tratamiento de datos de carácter personal. Estos instrumentos, y los basados en ellos, exigen que los datos sean obtenidos de manera lícita y justa, que éstos sean utilizados únicamente para los propósitos declarados, sean adecuados y no excesivos a dichos fines, veraces y actualizados, accesibles a la persona titular de la información, almacenados de manera segura y destruida una vez que haya cumplido dicha finalidad¹⁴.

Por otro lado, en base a la investigación académica sobre lo que se ha denominado el “trabajo digital”¹⁵, cuya tesis principal es que cada clic que hacemos en la red es una huella que vale dinero¹⁶, se ha propuesto considerar los datos de carácter personal como una característica indisoluble del patrimonio¹⁷ y la propiedad privada como vehículo jurídico apropiado para el ejercicio de los derechos asociados a su protección, mediante su monetización individual¹⁸ y colectiva¹⁹. No obstante, esta idea es incompatible con el pleno ejercicio de los derechos fundamentales ya que los datos de carácter personal, una vez considerados como informaciones relativas a la persona, no pueden ser libremente transferibles ni sujetos a las posibilidades de transferencia y expropiación intrínsecas al concepto de propiedad. **Una persona no sería libre de elegir cómo utilizar sus datos una vez que los haya vendido puesto que ya no podría revocar su consentimiento.** En resumen, introducir la propiedad como vehículo jurídico para la protección de los datos de carácter personal **mermaría gravemente la capacidad real de las personas de hacerlo**²⁰.

¹⁴ [Becerri, A. \(s.f\). Acuerdos internacionales para la privacidad de la información. Revista Seguridad.](#)

¹⁵ Scholtz, T. (2012). Trabajo digital: Internet como patio de recreo y fábrica.

¹⁶ [Casilli, A. \(2009\). ¿Qué es el trabajo digital?](#)

¹⁷ [Flacso. \(2021\). Carta Magna Digital](#)

¹⁸ [Koenig, G. \(2018\). Dejando atrás la Edad Media de los datos](#)

¹⁹ [Ruhaak, A. \(2021\). Fideicomisos de datos para proteger la privacidad.](#)

²⁰ [CNIL. \(2017\). Proteger los datos de carácter personal, apoyar la innovación, preservar las libertades individuales.](#)

ANTECEDENTES

En la actual Constitución Política chilena²¹, el derecho a la protección de datos de carácter personal se encuentra reconocido de manera autónoma desde 2018 por una reforma constitucional a través de la Ley N° 21.096, que establece:

Artículo 19.4º. “El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos de carácter personal. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.”

En materia de ley, este derecho se encuentra contenido en la Ley N°19.628 sobre Protección de la Vida Privada²², promulgada en 1999, después de seis años de discusión parlamentaria, bajo un contexto radicalmente diferente:

Artículo 1º. “El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

Toda persona puede efectuar el tratamiento de datos de carácter personal, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.”

En términos generales, este marco legal es insuficiente para la defensa de los derechos de las personas y desde el año 2007 se han realizado diversos esfuerzos legislativos para modificarlo y adaptarse a los nuevos estándares. El último de estos se encuentra contenido en los Boletines N°11.144-0 y N° 11.092-07, refundidos, en actual tramitación.

La Ley N°20.285 sobre el acceso a la información pública²³, de 2008, crea un órgano especializado en materia de transparencia y acceso, el Consejo para la Transparencia, a quien le entrega la facultad de:

“Velar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado”.

Conforme a su redacción, esta norma no permite a esta entidad la investigación, fiscalización o sanción en materia de protección de datos, como tampoco de instruir a los órganos de la Administración del Estado; por ello, solo se reconoce la dictación de recomendaciones²⁴.

²¹ [Senado.\(2012\).Capítulo III: De Los Derechos y Deberes Constitucionales.](#)

²² [Ley N° 19.628, de Protección de la Vida Privada.](#)

²³ [Ley N°20.285, sobre el acceso a la información pública.](#)

²⁴ [Concejo para la transparencia.\(s.f\).Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado.](#)

Además, Chile ha ratificado tratados y acuerdos internacionales con diferentes organismos donde se compromete a proteger los datos de carácter personal:

- Organización para la Cooperación y el Desarrollo Económicos (OCDE): directrices relativas a la protección de la privacidad y el flujo transfronterizo de datos de carácter personal²⁵.
- Asia-Pacific Economic Cooperation (APEC): marco de privacidad del Foro de Cooperación Económica Asia Pacífico²⁶.
- Acuerdo de Asociación de Economía Digital (DEPA)²⁷.

La legislación chilena ha tenido un lento avance en los últimos 14 años, y no se ha perfeccionado la protección de datos de carácter personal. La OCDE realizó una advertencia a Chile, pues junto con Turquía, son los únicos países que están incumpliendo los acuerdos adoptados referidos a la materia, sin haber mejorado en nada su legislación²⁸.

En la región latinoamericana, Chile fue pionero en dictar una normativa sobre protección de datos en el año 1999, luego Argentina en el año 2000 y con posterioridad otros países avanzaron en sus regulaciones. No obstante, el país es de los pocos que no cuenta con una institucionalidad que regule la materia, junto con Venezuela, Bolivia, Paraguay y Cuba. En términos generales, la región cuenta con marcos legales y autoridades de control, que han actualizado estos conforme a los estándares del Reglamento General de Protección de Datos europeo, adherido al Convenio 108 de Europa, entre otros, por lo que se recomienda seguir el camino de México, Uruguay y de la Unión Europea, pues se plantea la protección de los datos de carácter personal como un derecho humano fundamental que han incluido en sus constituciones.

La Ley N°19.628 no permite proteger el derecho a la protección de los datos de carácter personal, no considera un sistema de fiscalización adecuado y ha sido sobrepasada por los avances tecnológicos, pues no protege adecuadamente el consentimiento informado de las personas, debido a que regula la comercialización y no la protección de los datos de carácter personal, entre otras fallas. Según los expertos, las principales falencias dicen relación con la poca efectividad en la protección de las personas, la ausencia de una autoridad de control, el concepto y aplicación indiscriminada de fuente de acceso público; la falta de un catálogo de infracciones y sanciones poco efectivas; la falta de precisión por el concepto de datos sensibles; así como su obsolescencia, entendida como la falta de adaptación a las normativas internacionales, incapacidad de adaptación a los nuevos escenarios tecnológicos, entre otros²⁹.

²⁵ [OECD\(1980\). Directrices relativas a la protección de la privacidad y el flujo transfronterizo de datos de carácter personal.](#)

²⁶ [APEC\(2005\).Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico.](#)

²⁷ [Ministerio de Relaciones Exteriores.\(s.f\).Acuerdo de Asociación de Economía Digital.](#)

²⁸ [Alonso.C. \(23 de Julio 2015\).OCDE envía carta de advertencia a Chile por retraso en protección de datos de carácter personal. La Tercera](#)

²⁹ [BCN\(2018\).Reporte: Consulta experta sobre la Ley de Protección de la vida Privada de las Personas.](#)

Cabe destacar además, desde un punto de vista práctico, que esta falta de un catálogo de infracciones, de sanciones efectivas y de precisión de los conceptos de datos de carácter personal y sensibles, dificulta la determinación efectiva de responsabilidad. Si a esta complejidad le sumamos la probabilidad acotada de un fallo positivo y los costos elevados asociados a una causa de esta naturaleza, lo que se observa es una aplicación marginal de la normativa actual puesto que es poco atractiva y de difícil acceso para las potenciales partes demandantes³⁰.

Finalmente, observando lo señalado por la Ley 20.575 que establece el principio de finalidad en el tratamiento de datos, así como el actual proyecto de ley en discusión que se inspira de manera importante en la actual legislación europea, se ha hecho la observación que hacer recaer la carga de la responsabilidad de la protección de los datos de carácter personal, de manera exclusiva en los responsables de tratamiento de datos. Esto podría tener como resultado, más que proteger efectivamente los datos de carácter personal, el generalizar la legitimidad de su tratamiento³¹.

Una normativa de protección de datos de carácter personal vaga e incompleta³² crea una ilusión de protección en las personas cuyo efecto perverso es producir exactamente lo contrario³³.

Existen ejemplos claros de la necesidad de que Chile cuente con una regulación que garantice de manera efectiva la protección de los datos de carácter personal:

- En 2008, se comprometieron los datos de carácter personal de 6 millones de personas en una filtración las bases de datos del Servicio Electoral, de la Dirección General de Movilización Nacional (los encargados del reclutamiento militar y control de armas), del Ministerio de Educación (toda la información de los pases escolares), de las y los inscritos en la PSU el año 2005 y de una guía telefónica comercial de Santiago con 2 millones de nombres, direcciones y teléfonos. Todos, exceptuando la última, son responsabilidad del Gobierno³⁴.
- Hasta marzo del año 2016 hubo al menos 3 millones de archivos desprotegidos desde la plataforma computacional del Ministerio de Salud, de pacientes con VIH, mujeres que pidieron la píldora del día después, personas con enfermedades mentales, todas con nombre, RUT y domicilio estaban totalmente vulnerables en la red. Cerca de 100 mil funcionarias y funcionarios del MINSAL, e incluso personas externas, podían acceder a esa información privada. Se trata de la peor vulneración de seguridad informática en el ámbito de la salud³⁵.

³⁰ [Ley 19.628 - Dictámenes relacionados.](#)

³¹ Sibony, A., & Helleringer, G. (2015). Protección del consumidor y ciencias del comportamiento en la UE: ¿Revolución o reforma? en A. Alemanno & A. Sibony. *Nudge and the law*(pp. 209–234). London: Hart Publishing.

³² [Diario Oficial de la República Francesa, Debates parlamentarios, Asamblea Nacional, 5ª legislatura, 5 de octubre de 1977, No. 79.](#)

³³ [Netter,E.\(2019\).Sanción de 50 millones de euros: más allá de Google, la CNIL aborda las políticas de privacidad oscuras y los «consentimientos vacíos».Daloz IP/IT, Daloz, 2019, pp.165. \(hal-02314524\)](#)

³⁴ [Prieto,L.\(11 de mayo 2008\).Gobierno comienza investigación de filtración de datos de carácter personal de 6 millones de chilenos.FayerWayer.](#)

³⁵ [Carvajal,V. Jara,M.\(5 de mayo 2016\).Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes. Ciper.](#)

- En 2016, la Fundación Datos Protegidos, Derechos Digitales y Corporación Fundamental presentaron un recurso de protección en contra de las municipalidades de Las Condes y Lo Barnechea por la implementación de un sistema de vigilancia en espacios públicos consistente en globos aerostáticos con cámaras de alta tecnología. El caso fue fallado por la Corte Suprema y constituye el primer antecedente de discusión sobre privacidad en espacios públicos y videovigilancia. Luego fue el turno de los drones de vigilancia en la comuna de Las Condes³⁶.
- En mayo de 2020 el medio digital Interferencia publicó un artículo que entregaba información georreferenciada de las personas que resultaron positivo al examen de COVID-19. Consistía de una serie de mapas de distintas comunas de la Región Metropolitana, y de otras regiones, con información actualizada del Ministerio de Salud (MINSAL). Estos mapas señalaban la ubicación de quienes tenían o tuvieron la enfermedad³⁷.
- En 2021 se tuvo conocimiento de la explotación de una vulnerabilidad en los sistemas de Facebook que permitía ver el número de teléfono vinculado a cada cuenta de los usuarios, creando una base de datos que contenía la información de 533 millones de usuarios en todos los países, 7 millones corresponden a usuarios chilenos³⁸.

³⁶ [Malamud, S. \(2018\). Videovigilancia y privacidad. Consideraciones en torno a los casos “Globos” y “Drones”. Revista Chilena de Derecho y Tecnología, 7\(2\), 137-162. doi:10.5354/0719-2584.2018.49097](#)

³⁷ [INDH \(12 de mayo 2020\). Consejo INDH: Publicación de datos georreferenciados de pacientes con COVID-19 vulnera el derecho a la privacidad y a la protección de los datos de carácter personal.](#)

³⁸ [Quintero, P\(3 de abril 2021\). Los datos privados de casi 7 millones de usuarios chilenos de Facebook están comprometidos. La Tercera.](#)

Definiciones, principios, rol del Estado y nueva institucionalidad

Entenderemos por datos de carácter personal toda información relativa a una persona natural que permita su identificación directa o indirecta, es decir, que permita su identificación ya sea por la naturaleza de las informaciones, el modo en que estas hayan sido recolectadas o mediante algún tipo de operación más o menos complejo, incluso algorítmico, **cuando este establezca un vínculo entre la información y la persona**. La identidad puede ser física, fisiológica, psíquica, económica, cultural o social. Esto incluye, pero no se limita, a los nombres, apellidos, firma, foto, número de identificación personal, número de pasaporte, dirección postal, dirección de correo electrónico, número de teléfono, dirección IP³⁹, trazadores de navegación en Internet (cookies), hábitos personales como de desplazamiento, de consumo, de alimentación, etc.

Entenderemos por datos sensibles una categoría especial de datos de carácter personal, relativos a características, hechos o circunstancias de la vida privada de una persona o que puedan hacerla objeto de algún tipo de discriminación. Tales como el supuesto origen racial o étnico, las opiniones políticas, las creencias religiosas, filosóficas, la pertenencia a un sindicato, los datos genéticos y/o biométricos, los estados de salud, la vida sexual o el género. Esto incluye pero no se limita al número de hoja médica, condición genética o médica, o toda información a disposición de un profesional de la salud, de un laboratorio, de un hospital, de una clínica, u otro establecimiento de salud. Así también, huellas dactilares, código genético, iris de los ojos, mapas de venas, cadencia al caminar, reconocimiento facial, etc.

Se entiende por algoritmo a un conjunto de reglas de funcionamiento, cuya aplicación permite resolver un problema planteado mediante un número finito de operaciones⁴⁰. Un algoritmo es independiente de un tratamiento informático: una hoja de cálculos en papel puede considerarse como un algoritmo. Por inteligencia artificial, se entiende un tipo de algoritmo. Los algoritmos públicos son los utilizados por las autoridades públicas, que operan al servicio del interés general, se utilizan para ejecutar o hacer cumplir la ley y suelen ser inevitables. Los algoritmos públicos son una forma de acto administrativo y las autoridades públicas que los utilizan están sujetas a la “responsabilidad administrativa”.

Primero, puesto que los datos de carácter personal son informaciones relativas a la persona, cuya protección debe estar garantizada por un conjunto de derechos vinculados a esta y al respeto que se le debe, **el nuevo modelo global de protección de datos parte de la base que la protección de los datos de carácter personal es un principio desde el diseño y por defecto**. Además, que su recolección y tratamiento es una excepción concreta, explícita, realizada de manera transparente,

³⁹ [GDPRhub. \(s.f\).CJEU - C-582/14 - Patrick Breyer.](#)

⁴⁰ [CNIL \(2017\).¿Cómo podemos permitir que los humanos sigan teniendo el control? Los retos éticos de los algoritmos y la inteligencia artificial.](#)

que permite en todo momento la intervención humana y bajo estricto control democrático. Los datos sensibles requieren una protección acentuada y suplementaria, su recolección debe ser realizada por autoridades públicas y su tratamiento debe estar circunscrito a la estadística pública realizada por autoridades públicas y a la investigación científica e histórica.

Segundo, considerando la responsabilidad del Estado respecto de la promoción del interés general y observando el proyecto de Ley de Gobernanza de Datos del Parlamento Europeo y del Consejo⁴¹ se propone que el Estado participe y promueva activamente el desarrollo e implementación de las infraestructuras que permitan un tratamiento seguro y auditable de los datos de carácter personal, los que podrá imponer, si su protección, así como también, los derechos fundamentales y las libertades públicas se vean amenazadas y que tenga la responsabilidad exclusiva en cuanto a la recolección de los datos sensibles de las personas⁴².

Algunas infraestructuras son *esenciales*, ya que sin ellas el Estado no puede cumplir con su misión de interés general; y *críticas*, ya que su malfuncionamiento, intencional o no, «*trae como consecuencia el riesgo de paralización de los servicios del Estado, lo que se puede traducir en la cesación de muchas prestaciones públicas, desde los servicios básicos hasta la gestión de información en la entrega de prestaciones sociales*»⁴³.

Tercero, puesto que se hace necesario vigilar al vigilante y en coherencia con las obligaciones establecidas por el Convenio 108, se propone establecer una autoridad independiente, especializada y autónoma que lleve a cabo sus tareas de manera libre de influencias externas para garantizar debidamente la eficacia y fiabilidad de la supervisión, fiscalización y sanción a las infracciones al derecho a la protección de los datos de carácter personal⁴⁴.

⁴¹ [Comisión Europea. \(2020\). Proyecto de Ley de Gobernanza de Datos del Parlamento Europeo y del Consejo \(2020/0340\).](#)

⁴² Respecto al tratamiento de los datos sensibles ver *supra*.

⁴³ [Derecho Informático, Centro de Estudios en. \(2021\). Constitución digital: Documento para el debate constituyente en Chile. Revista chilena de derecho y tecnología, 10\(1\), 1-8. <https://dx.doi.org/10.5354/0719-2584.2021.64228>](#)

⁴⁴ [Minuta redactada por Jessica Matus, presentada ante la Comisión de Economía de la Cámara de Diputados en la discusión del proyecto de ley que establece medidas para incentivar la protección de los derechos de los consumidores. Boletín Nº 12.409-3.](#)

Desafíos presentes y futuros en el uso de las tecnologías y el tratamiento de los datos⁴⁵

Los principales desafíos que representa el tratamiento de la información y su interconexión con los algoritmos y la inteligencia artificial, vienen dados por: los sesgos, discriminación y exclusión de personas y grupos; el perfilado algorítmico, que aumenta las amenazas por la personalización; el reto de la selección de datos, donde debe buscarse la cantidad, precisión y la ausencia de sesgos; las máquinas autónomas, su responsabilidad y la amenaza a libertad por la toma de decisiones de carácter automatizado. Todos estos tópicos han sido planteados por las autoridades de datos en Europa.

Además, el Ethics Advisory Group del Supervisor Europeo de Protección de Datos⁴⁶, redactó un informe en el que recogen los desafíos que plantea el tratamiento de la información: digitalización de las personas; de la gobernanza de las instituciones a la gobernabilidad a través de los datos; de una sociedad de riesgo a una sociedad punteada; de la autonomía humana y su convergencia con las máquinas; y de la justicia penal a la justicia preventiva.

Estos tópicos dicen relación con la triangularización de los datos a través de múltiples fuentes, la observación del comportamiento mediante perfiles algorítmicos que transforman gradualmente la forma en que se puede gobernar, evaluaciones de riesgo más individualizadas que hacen necesaria la transparencia de los algoritmos y la posibilidad de impugnar las decisiones por parte de las personas que son clasificadas, una nueva ética digital para intentar predecir el comportamiento criminal de antemano utilizando el resultado del análisis basado en big data y algoritmos. Por último, el papel del consentimiento de las personas, conocido como consentimiento informado, donde estas no siempre leen ni entienden completamente las condiciones y términos que acepta y la posibilidad de que sus datos sean reutilizados posteriormente para finalidades que inicialmente no estaban previstas.

⁴⁵ «La ética en el tratamiento de los datos digitales para un futuro sostenible», Ortíz Lopez, P. En: *Ellas. Retos, amenazas y oportunidades en un mundo conectado*. Madrid, 2019. Editorial Wolters Kluwer.

⁴⁶ [Unión Europea. \(2016\). Decisión del supervisor Europeo de protección de datos.](#)

Es por todo lo antes mencionado, que se propone:

Articulado

Artículo X1. Toda persona tiene derecho a la protección de sus datos de carácter personal, a saber qué información se conserva respecto a ella así como a decidir y controlar su uso y a no ser objeto de una decisión basada únicamente en un tratamiento automatizado que afecte sus derechos.

Artículo X2. Toda recolección y tratamiento de datos de carácter personal se realiza de manera excepcional según las condiciones que disponga la ley, siempre conforme a los principios de licitud, lealtad, transparencia, seguridad y limitación de la finalidad.

Artículo X3. Toda recolección y tratamiento de datos sensibles está prohibido, salvo en los casos específicos que disponga la ley.

Artículo X4. Los organismos públicos, dentro del marco de sus competencias legales, podrán operar y desarrollar infraestructuras de recolección, tratamiento, acceso y reutilización de datos de carácter personal que garanticen el respeto de los derechos fundamentales.

Artículo X5. Una ley creará una entidad jurídica de derecho público, con patrimonio propio, autónoma, especializada e independiente.

Esta entidad tendrá como misión proteger los datos de carácter personal, garantizar los derechos y libertades fundamentales de las personas naturales en lo que respecta a la recolección y tratamiento de estos, facilitar la libre circulación de la información, participar al debate social sobre gestión ética de datos, dialogar con los ecosistemas de innovación, promover el desarrollo de tecnologías respetuosas de las personas y asesorar a quienes las desarrollen para que integren la privacidad desde el diseño.

Esta institución estará dotada de las facultades necesarias para controlar a todo organismo público y privado que recolecte o trate datos de carácter personal, así como para investigar, fiscalizar, aplicar sanciones administrativas cuando corresponda, y demás facultades que le pueda conferir la ley.

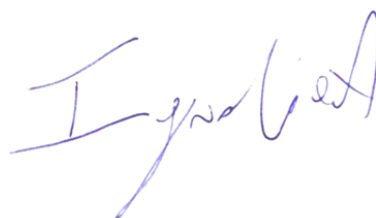
PATROCINAN



1- Francisco Caamaño Rojas



2- Carolina Videla Osorio



3- Ignacio Achurra Díaz



4- Alexis Caiguan Ancapan



5- Paulina Valenzuela Río



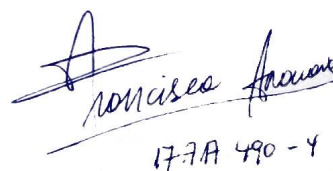
6- Loreto Vidal Hernández



7- Malucha Pinto Solari



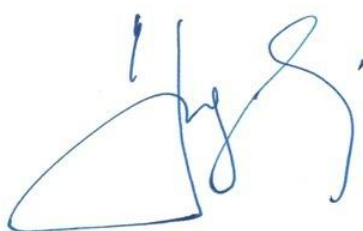
8- Ingrid Villena Narbona



9- Francisca Arauna Urrutia



10- Daniel Bravo Silva



11- Hugo Gutierrez Gálvez