



Tratamiento de datos personales

Marco regulatorio nacional aplicable a organismos públicos

Autor

James Wilkins Binder

jwilkins@bcn.cl

Resumen

Las modificaciones introducidas a la Ley N° 19.628 sobre protección de la vida privada por el proyecto de ley -despachado por el Congreso- que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, supone el establecimiento de un nuevo régimen de tratamiento de datos personales. En lo que se refiere al tratamiento por parte de organismos públicos, el nuevo marco permite dicho tratamiento sin consentimiento previo del titular, siempre que este se alinee con las funciones legales y siempre que se encuentre dentro de las competencias de estos organismos. Además, en este punto, el texto aprobado facilita la comunicación de datos entre organismos públicos para evitar duplicidad de trámites, y establece que la transferencia de datos a entidades privadas es posible con el consentimiento del titular, a menos que sea necesario para cumplir funciones específicas. Destaca, también, el establecimiento de un régimen de tratamiento especial de datos personales por organismos públicos para determinadas categorías de datos personales.

N° SUP: 143295

En cuanto al tratamiento de datos personales relativos a niños, niñas y adolescentes, el texto aprobado establece un régimen de tratamiento especial, que considera, entre otras reglas: a) que sólo puede realizarse atendiendo al interés superior de niños, niñas y adolescente, y al respeto de su autonomía progresiva; b) la exigencia de consentimiento otorgado por sus padres o representantes legales, salvo que expresamente lo autorice o mandate la ley; c) la autorización para tratar los datos personales de los adolescentes de acuerdo a las normas de autorización previstas para los adultos, salvo datos personales sensibles de menores de 16 años; d) la obligación de establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, de velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.

Finalmente, en relación a la protección de datos personales y el desarrollo de sistemas de inteligencia artificial, se encuentra en discusión en la Cámara de Diputadas y Diputados el Proyecto de Ley que regula los sistemas de Inteligencia Artificial, ingresado en mayo de 2024. En materia de protección de datos personales, la iniciativa propone: establecer como uno de los principios generales a ser observados por los operadores, la privacidad y gobernanza de datos; clasificar los sistemas de IA de acuerdo con su riesgo, considerando especialmente para ello factores relacionados a la protección de datos personales, y encomendar la labor de fiscalización y cumplimiento normativo a la Agencia encargada de la Protección de Datos Personales.

Introducción

A solicitud parlamentaria se analiza la legislación nacional sobre tratamiento de protección de datos por organismos públicos, con especial énfasis en el tratamiento de datos relacionados a niños, niñas y adolescentes. Asimismo, se revisan las normas del Proyecto de Ley que regula los sistemas de inteligencia artificial, haciendo referencia a la Ley Europea de inteligencia artificial.

El tema que aborda este informe y sus contenidos están delimitados por los parámetros de análisis de Asesoría Técnica Parlamentaria y por los plazos e información disponibles. No se trata de un documento académico y se enmarca en los criterios de neutralidad, pertinencia, síntesis y oportunidad en su entrega.

Las traducciones y negrillas son propias.

I. Tratamiento de datos personales por organismos públicos en Chile

La legislación chilena relativa a la protección de datos personales por parte de organismos públicos sufrirá próximamente un marcado cambio regulatorio, que se materializará mediante la incorporación de diversas modificaciones a la Ley N° 19.628 sobre protección de la vida privada, por parte del proyecto de ley, aprobado y despachado por el Congreso Nacional¹, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, correspondiente a los Boletines N°s 11.144-07 y 11.092-07, refundidos.

Debido a lo anterior, el detalle normativo que se entrega para la revisión del régimen de protección de datos personales por parte de organismos públicos, corresponde al texto aprobado y despachado por el Congreso Nacional, lo mismo en relación con aspectos regulatorios generales que se citan para contextualizar el tema.

1. Antecedentes generales

El 27 de agosto de 2024, el Senado aprobó el informe de la Comisión Mixta del Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletines 11144-07 y 11092-07, refundidos. Con ello finalizó, después de siete años- el trámite legislativo de esta iniciativa, al no haber sido objeto de veto por parte del Presidente de la República.

El objetivo del proyecto de ley aprobado es perfeccionar las normas relativas al tratamiento de los datos personales de las personas naturales, de manera que éste se realice con el consentimiento del titular de dichos datos o en los casos que lo autorice la ley, garantizando estándares de calidad, información, transparencia y seguridad. Asimismo, la iniciativa crea la Agencia de Protección de Datos Personales, organismo público encargado de velar por la protección de los datos personales.

¹ El Tribunal Constitucional, por sentencia de control de constitucionalidad de fecha 14 de noviembre de 2024, declaró la constitucionalidad del proyecto de ley. Sentencia disponible en: <https://tramitacion.tcchile.cl/tc/download/343075?inlineifpossible=true> (Noviembre, 2024).

a. Definiciones

Las principales definiciones claves para la aplicación de la Ley sobre Protección de Datos Personales en encuentran establecidos en su artículo 2º:

- a) **Dato personal.** cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- b) **Datos personales sensibles.** tendrán esta condición aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.
- c) **Base de datos personales.** conjunto organizado de datos personales, cualquiera sea la finalidad, forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar su tratamiento.
Responsable de datos o responsable: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.
- d) **Titular de datos o titular.** persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.
- e) **Tratamiento de datos.** cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.”.

b. Principios que rigen el tratamiento de datos personales

El artículo 3º consagra un catálogo de principios de deben regir el tratamiento de datos personales. Entre estos, se encuentran:

- a) **Principios de licitud y lealtad.** De acuerdo con este principio, los datos personales sólo pueden tratarse de manera lícita y leal.
- b) **Principio de finalidad.** Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.
- c) **Principio de proporcionalidad.** El tratamiento de datos personales debe limitarse estrictamente a aquellos datos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento.
- d) **Principio de calidad.** Los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento.

- e) **Principio de responsabilidad.** Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios contenidos en este artículo y de las obligaciones y deberes de conformidad a la ley.
- f) **Principio de seguridad.** En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción.
- g) **Principio de transparencia e información.** El responsable debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que establece la ley, incluyendo las políticas y las prácticas sobre el tratamiento de los datos personales, las que además deberán encontrarse permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.
- h) **Principio de confidencialidad.** El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.”.

2. Tratamiento de datos personales por organismos públicos

Al igual que la legislación vigente, la iniciativa aprobada dispone de normas especiales para regular el tratamiento de datos por parte de organismos públicos. Conforme con éstas normas, el tratamiento de datos por parte de organismos de dicha naturaleza se encuentra sujeto, entre otras, a las siguientes reglas:

La ley autoriza el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza bajo los siguientes supuestos (art. 20):

- para el cumplimiento de sus funciones legales,
- dentro del ámbito de sus competencias,
- de conformidad a las normas establecidas en la ley sobre protección de datos personales

En tales casos, los órganos públicos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales.

Lo órganos públicos deben evitar la duplicación de procedimientos y trámites entre los organismos públicos y entre éstos y los titulares de la información(art. 21).

En este sentido, los órganos públicos están facultados para comunicar o ceder datos personales específicos, o todo o parte de sus bases de datos o conjuntos de datos, a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de sus funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los puede utilizar para otros fines (art. 22).

Asimismo, se faculta a los organismos públicos a ceder datos o bases de datos personales entre organismos públicos, solo cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar

beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares (art. 22).

El órgano público receptor de los datos sólo puede conservarlos por el tiempo necesario para efectuar el tratamiento específico para el cual fueron requeridos, luego de lo cual deberán ser suprimidos o anonimizados (art. 22).

Los organismos públicos, solo podrán comunicar o ceder datos personales a personas o entidades privadas, cuando cuenten con el consentimiento del titular, salvo que la comunicación o cesión de datos sea necesaria para cumplir las funciones del organismo público en materia de fiscalización o inspección (art. 22).

Por otra parte, la ley aprobada establece la obligación de los organismos públicos de informar mensualmente a través de su página web institucional los convenios suscritos con otros organismos públicos y con entidades privadas relativos a cesión o transferencia de datos personales. Esta obligación será fiscalizada por la Agencia de Protección de Datos Personales (art. 22).

Sin perjuicio de estas reglas, la ley dispone de un régimen de tratamiento especial de datos personales por organismos públicos para determinadas categorías de datos personales. Estos son, los datos personales sensibles y los datos relativos a infracciones penales, administrativas y disciplinarias. Para ambos casos el texto aprobado establece supuestos habilitantes para su tratamiento por parte de estos organismos, limitándolo a determinados casos, según la categoría del dato (art. 24 y 25).

Finalmente, el texto aprobado delega en un reglamento la determinación de las condiciones, modalidades e instrumentos para la comunicación o cesión de datos personales entre organismos públicos y con personas u organismos privados, el que debe ser expedido por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro de Hacienda y por el Ministro de Economía, Fomento y Turismo, previo informe de la Agencia.

II. Tratamiento de datos personales relativos a los niños, niñas y adolescentes

La legislación nacional ha dispuesto de normas específicas para el tratamiento de datos personales referidos a niños, niñas y adolescentes. Ello lo encontramos, en primer término, en la Ley sobre Protección de Datos Personales, modificada conforme con el nuevo texto aprobado; y en la Ley 21.430 sobre garantías y protección de derechos de la niñez y adolescencia.

1. Nuevo texto aprobado de la Ley de Protección de Datos Personales

El texto aprobado considera regímenes de tratamiento especial para determinadas categorías de datos, entre las que se encuentran los datos personales relativos a niños, niñas y adolescentes. Las principales reglas aplicables bajo este régimen son:

- El tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes, sólo puede realizarse atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.
- El tratamiento de datos personales de los niños y niñas requiere el consentimiento otorgado por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal del niño o niña, salvo que expresamente lo autorice o mandate la ley.
- Los datos personales de los adolescentes se podrán tratar de acuerdo a las normas de autorización previstas para los adultos, salvo tratándose de datos personales sensibles de adolescentes menores de 16 años, que requiere el consentimiento otorgado por sus padres o representantes legales o quien tiene a su cargo el cuidado personal del menor, salvo que expresamente lo autorice o mandate la ley.
- Para los efectos de esta ley, se consideran niños o niñas a los menores de catorce años, y adolescentes, a los mayores de catorce y menores de dieciocho años.
- Se establece la obligación de los establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, incluido quienes ejercen su cuidado personal, velar por el uso lícito y la protección de la información personal que concierna a los niños, niñas y adolescentes.

2. Ley sobre garantías y protección de los derechos de la niñez y adolescencia

De acuerdo al artículo 33 de la Ley N° 21.430, los niños, niñas y adolescentes tienen derecho a la protección de sus datos personales, así como a impedir su tratamiento o cesión.

El mismo artículo establece la obligación de que la información dirigida a niños, niñas y adolescentes referente al tratamiento de sus datos personales, debe expresarse en un lenguaje que les sea fácilmente comprensible.

Asimismo, la ley establece el deber de funcionarios públicos, organizaciones de la sociedad civil que se relacionen con la niñez y su personal, de guardar reserva y confidencialidad sobre los datos personales de los niños, niñas y adolescentes a los que tengan acceso, a menos que su divulgación resulte indispensable para la protección de sus derechos y siempre que se tomen los resguardos necesarios para evitar un daño mayor (art. 33).

El artículo 64 en tanto, amplía el citado deber de reserva y confidencialidad a los organismos, entidades e instituciones públicas y privadas, a quienes se les exige actuar con la obligada reserva en el ámbito de la atención y protección a la infancia y la adolescencia, debiendo adoptar las medidas oportunas para garantizar la efectividad de su derecho a la vida privada, a la honra y propia imagen en el tratamiento confidencial de la información con la que cuenten y de los registros en los que conste dicha información.

El mismo deber de reserva lo hace extensivo, ahora, a las autoridades y personas que, por su profesión o función, conozcan de casos en los que exista o pudiere existir una situación de amenaza o de vulneración, o que tengan acceso a la información citada en el inciso anterior, quienes deberán abstenerse de utilizar dicha información con una finalidad distinta de las funciones legales que les corresponda desempeñar o utilizarla en beneficio propio o de terceros (art. 64).

En cuanto a registros (base de datos), la ley califica de “especialmente sujetos a reserva” los registros jurídicos, médicos y escolares de los niños, niñas y adolescentes, salvo requerimiento judicial. Sin perjuicio del derecho del niño, niña o adolescente, su familia, o quien lo tenga legalmente a su cuidado o su abogado, de solicitar al juez de familia conocer los datos o información personal que se halle en poder de cualquier entidad pública o privada.

La ley, finalmente, excepciona del deber de reserva a la información referida a niños, niñas y adolescentes que se guarde en registros públicos o de organismos privados colaboradores del Estado cuando sea utilizada de forma innominado, para fines científicos o de investigación (art. 64).

III. Tratamiento de datos personales e inteligencia artificial

El Mensaje del proyecto de ley sobre Inteligencia Artificial (IA) la define como “un conjunto de sistemas basado en máquinas que infieren, a partir de información de entrada, determinada información de salida, que puede consistir en predicciones, contenidos, recomendaciones o decisiones capaces de influenciar espacios físicos o virtuales”.

De acuerdo con Natalia Passalacqua (2024), la relación entre la protección de datos personales y la inteligencia artificial se manifiesta en el hecho de que IA busca que los ordenadores actúen de forma inteligente, imitando el conocimiento humano a través de procesos simbólicos o conexionistas, al detectar patrones en grandes volúmenes de datos que pueden procesar rápidamente.

Agrega la autora antes citada que el big data se ha convertido en un recurso valioso, planteando riesgos para la integridad de muchos datos personales que, diariamente, compartimos de manera impulsiva al aceptar términos y condiciones de varias aplicaciones.

La protección de datos personales enfrenta desafíos por el rápido avance de la IA, ya que su uso y aprendizaje implican el tratamiento masivo de datos, incluidas diferentes categorías de datos personales, lo que son esenciales no solo para el desarrollo de la IA, sino también para evitar sesgos y errores en los procesos automatizados.

A raíz de lo anterior, la protección de datos personales se ha constituido en un factor insoslayable al momento de regular el desarrollo de la inteligencia artificial. Así ha ocurrido recientemente con la aprobación del Reglamento Europeo de Inteligencia Artificial y, a nivel local, con el Proyecto de Ley de Inteligencia Artificial que ingresó al Congreso en mayo de 2024.

1. Proyecto de ley de inteligencia artificial

En mayo de 2024 ingresó a la Cámara de Diputadas y Diputados el proyecto de ley, iniciado en mensaje, que regula los sistemas de inteligencia artificial, Boletín N° 16821-19.

De acuerdo con los fundamentos del Mensaje, la IA ofrece un extraordinario potencial para incrementar el bienestar de las personas, por la vía de acceder a nuevos descubrimientos científicos que amplían

los límites del conocimiento humano; optimizar el uso de recursos finitos que nos ayudan en tareas cotidianas; y ampliar el acceso a la educación, así como al goce de diversos derechos fundamentales, entre otros.

Agrega el Mensaje que la IA puede contribuir de manera significativa en la transición de los países hacia un futuro socialmente más justo y ecológico de la mano de la tecnología. En el ámbito económico, puede facilitar la consecución de resultados positivos desde el punto de vista social y medioambiental, proporcionando grandes ventajas competitivas a las empresas y la economía nacional, lo que sería especialmente necesario en sectores de gran impacto como el cambio climático, el medio ambiente y la salud, el sector público, las finanzas, la movilidad y la agricultura.

Con todo, señala el Mensaje, la materialización de dichos beneficios pararía por garantizar que la IA se desarrolle y utilice de forma ética y responsable. Encontrándose al servicio de las personas, debe observar valores y principios rectores que orienten tanto sus usos, como el diseño de políticas públicas a su respecto. Entre ellos, señala el Mensaje, es fundamental el respeto, protección y promoción de los derechos fundamentales y de principios matrices como la supervisión humana, la transparencia y explicabilidad, la diversidad, no discriminación y equidad y la protección de datos personales, entre otros que se citan.

Así, en lo que respecta a la protección de datos personales, el proyecto de ley se hace cargo de lo siguiente:

- a) Establece como uno de los principios generales a ser observados por los operadores, la privacidad y gobernanza de datos, que persigue que los sistemas de IA sean desarrollados y utilizados de conformidad con las normas vigentes en materia de privacidad y protección de datos personales, procurando que los mismos sean interoperables (art. 4).
- b) Clasifica los sistemas de IA de acuerdo con su riesgo en sistemas de IA de riesgo inaceptable; de alto riesgo; de riesgo limitado, y sin riesgo evidente. Dentro de los sistemas de riesgo inaceptable, y por tanto prohibidos, se encuentran los siguientes:
 - Sistemas de manipulación subliminal, referidos a aquellos sistemas que se sirven de técnicas imperceptibles para las personas afectadas y que tienen como objeto o efecto directo la inducción de acciones que causan daños a la salud física y/o mental de la persona afectada.
 - Sistemas que explotan vulnerabilidades de las personas para generar comportamientos dañinos. Se refiere a aquellos sistemas que aprovechan o explotan alguna de las vulnerabilidades de una persona o un grupo específico de personas —incluidas las características conocidas de los rasgos de personalidad, situación social o económica de esa persona o grupo, la edad y la capacidad física o mental— que tenga por objeto alterar de manera sustancial su comportamiento o limitar su voluntad y provoque perjuicios, actuales o potenciales, a esa persona o a terceros. Considera también los sistemas de IA que sean dañinos y/o afecten la honra, la integridad y el libre desarrollo de la sexualidad de las personas, en particular la de niños, niñas y adolescentes.

- Sistemas de categorización biométrica de personas basadas en datos personales sensibles, esto es, que clasifiquen e identifiquen a personas naturales con arreglo a datos personales sensibles, o que partan de la base de una inferencia respecto a dichos atributos o características, de modo tal que dicha categorización provoque un trato perjudicial o injustificadamente discriminatorio sobre ellas.
 - Sistemas de calificación social genérica, que tengan por finalidad evaluar o clasificar a personas o grupos de personas naturales en función de su comportamiento social, su nivel socioeconómico o sus características personales o de personalidad conocidas o inferidas, de modo tal que su calificación resultante provoque un trato perjudicial o injustificadamente discriminatorio sobre dichas personas o grupos de personas.
 - Sistemas de identificación biométrica remota en espacios de acceso público en tiempo real, destinados al análisis de imágenes de vídeo en espacios de acceso público que emplean sistemas de identificación biométrica remota en tiempo real.
 - Sistemas de extracción no selectiva de imágenes faciales, es decir, que crean o amplían bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir de internet o de imágenes de circuito cerrado de televisión.
 - Sistemas de evaluación de los estados emocionales de una persona, destinados a inferir las emociones de una persona natural en los ámbitos de la aplicación de la ley penal, procesal penal y la gestión de fronteras, en lugares de trabajo y en centros educativos.
- c) A objeto de resguardar los derechos y libertades de las personas y la adecuada observancia de las prohibiciones y reglas establecidas en la ley, se encomienda la labor de fiscalización y cumplimiento normativo a la Agencia encargada de la Protección de Datos Personales

2. Ley de inteligencia artificial Unión Europea

El 01 de agosto de 2024 entró en vigencia el Reglamento Europeo de Inteligencia Artificial, que, de acuerdo al Consejo Europeo, tiene por objeto garantizar que los sistemas de IA se desarrollen y utilicen de manera responsable, imponiendo obligaciones a los proveedores y los responsables del despliegue de tecnologías de IA y regulando la autorización de los sistemas de inteligencia artificial en el mercado único.

Al igual que el Proyecto de Ley chileno, que se basa en la norma europea, el reglamento de la UE aborda los riesgos relacionados con la IA, como los sesgos, la discriminación y las lagunas en la rendición de cuentas, promueve la innovación y fomenta la adopción de la IA.

De forma similar a la propuesta chilena, el Reglamento aborda los riesgos asociados a usos específicos de la IA, clasificándolos en cuatro niveles de riesgo y estableciendo normas diferentes para cada nivel. En términos generales, los cuatro niveles de riesgo y sus reglas correspondientes son:

- Riesgo mínimo o nulo: La mayoría de los sistemas de IA no plantean riesgos. Los juegos o los filtros de correo no deseado basados en la IA pueden utilizarse libremente, puesto que no están regulados ni se ven afectados por el Reglamento de IA de la UE.
- Riesgo limitado: os sistemas de IA que comportan un riesgo limitado, como los chatbots o los sistemas de IA generadores de contenido, están sujetos a obligaciones de transparencia, como

la de informar a los usuarios de que su contenido se ha generado mediante IA para que puedan tomar decisiones con conocimiento de causa sobre su uso posterior.

- **Riesgo alto:** los sistemas de IA de alto riesgo, como los utilizados en el diagnóstico de enfermedades, la conducción autónoma y la identificación biométrica de personas implicadas en actividades delictivas u objeto de investigaciones penales, deben cumplir unos requisitos y obligaciones estrictos para acceder al mercado de la UE. Entre ellos se incluyen unas pruebas rigurosas, transparencia y supervisión humana.
- **Riesgo inaceptable:** Está prohibido en la UE el uso de sistemas de IA que supongan una amenaza para la seguridad, los derechos o los medios de subsistencia de las personas. Están prohibidos, por ejemplo, la manipulación cognitiva conductual, la actuación policial predictiva, el reconocimiento de emociones en lugares de trabajo y centros educativos, y la puntuación ciudadana, así como —con algunas excepciones— el uso en los espacios públicos, por parte de las autoridades garantes del cumplimiento del Derecho, de sistemas de identificación biométrica remota en tiempo real, como el reconocimiento facial.

En cuanto a la institucionalidad de supervisión, de acuerdo con el Ministerio de Asuntos Económicos y Transformación Digital de España, el Reglamento dispone que debe existir una autoridad nacional notificante y al menos una autoridad de supervisión de mercado como autoridades nacionales competentes. A estas últimas corresponde monitorear el correcto funcionamiento de sistemas de IA de alto riesgo, identificando riesgos sobrevenidos, incidentes u otras situaciones que exijan tomar medidas sobre los sistemas de IA de alto riesgo.

La autoridad notificante, en tanto, habilita a organismos de evaluación para hacer las evaluaciones de conformidad en materia de IA a productos que quieran comercializar o poner en funcionamiento los proveedores.

Finalmente, a nivel europeo, se constituyó un Comité Europeo de Inteligencia Artificial, donde participan representantes de cada Estado miembro. Este Comité se encuentra encargado de orientar a los Estados Miembros sobre la implementación del Reglamento, elaborar guías y establecer las reglas básicas para elaborar sandboxes.

Referencias

Passalacqua, Natalia. (2024). “Sana convivencia entre el desarrollo de la Inteligencia Artificial y la protección de datos personales, por Natalia Passalacqua”. Disponible en: <https://c.bcn.cl/pw3yXn> (noviembre, 2024).

Ministerio de Asuntos Económicos y Transformación Digital de España. El Reglamento de Europeo de IA. Disponible en: <https://c.bcn.cl/qV785H> (noviembre, 2024).

Textos normativos

1. Chile

Ley N° 19.628 Ley N° 19.628 sobre protección de la vida privada. Disponible en: <https://bcn.cl/2eqfn> (noviembre, 2024).

Ley N° 21.430 sobre garantías y protección de derechos de la niñez y adolescencia. Disponible en: <https://bcn.cl/2yieq> (noviembre, 2024).

Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, correspondiente a los Boletines N°s 11.144-07 y 11.092-07, refundidos. Disponible en: <https://c.bcn.cl/0pDNJy> (noviembre, 2024).

Proyecto de ley que regula los sistemas de inteligencia artificial. Boletín N° 16.821-19. Disponible en: <https://c.bcn.cl/36DanN> (noviembre, 2024).

2. Unión Europea

Reglamento de Inteligencia Artificial. Disponible en: <https://c.bcn.cl/rG3xJE> (noviembre, 2024).

EU Artificial Intelligence Act. La Ley de Inteligencia Artificial de la UE. Evolución y análisis actualizados de la Ley de AI de la UE. Disponible en: <https://artificialintelligenceact.eu/es/> (noviembre, 2024).

Nota aclaratoria

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.