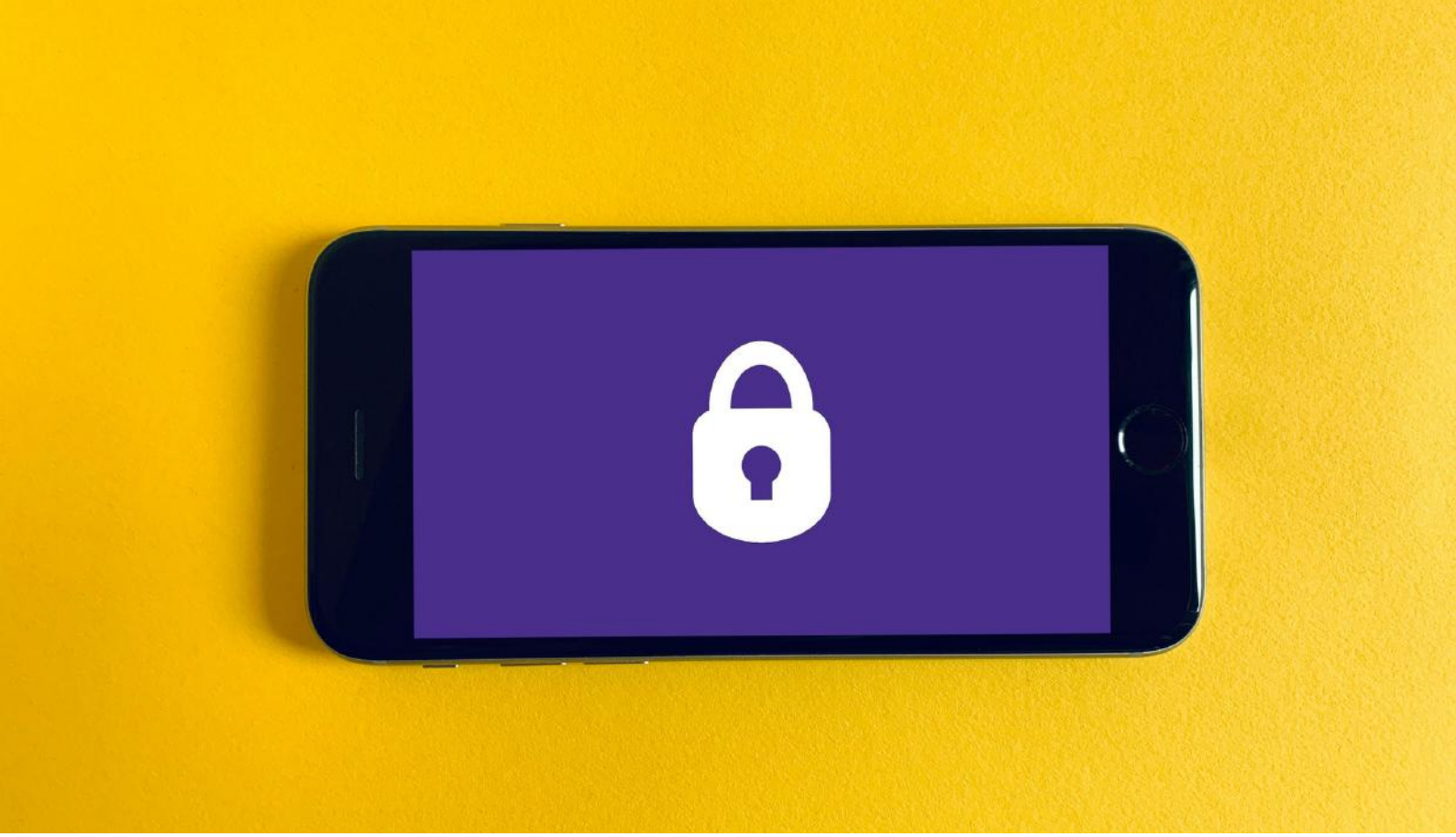

Protección de datos personales: ¿Qué esperar tras la entrada en vigencia de la nueva ley?

Beatriz Mercado, Magíster en Gestión de Personas en Organizaciones de la Universidad Alberto Hurtado, Chile. Directora de carrera Gestión de Información, Bibliotecología y Archivística, Facultad de Economía y Negocios, UAH.
Correo electrónico: bmercado@uahurtado.cl

Si bien Chile fue pionero en América Latina al promulgar en 1999 la Ley 19.628 sobre Protección de la Vida Privada, con el auge de las tecnologías digitales las limitaciones de dicha ley se hicieron evidentes: falta de sanciones efectivas a la vulneración de las normas, ausencia de regulación del flujo transfronterizo de los datos personales, uso de datos para marketing directo sin autorización del titular, falta de registro de bases de datos privadas, ausencia de una autoridad pública de control, excepciones amplias al consentimiento para el tratamiento de datos y falta de mecanismos procedimentales de resguardo efectivo. (Viollier, 2017).

A fines de 2024, Chile dio otro paso en su alineación con estándares y experiencias internacionales en políticas públicas, al publicar la nueva ley de Protección de Datos Personales. La Ley 21.719 de 2024 (que entrará en vigencia el 1 de diciembre de 2026) es una actualización largamente esperada. A través de esta nueva normativa, Chile fortalece los derechos de los ciudadanos en materia de datos personales, establece un régimen de sanciones para quienes incumplan la ley y crea la Agencia de Protección de Datos Personales, un organismo clave para la supervisión y cumplimiento de la normativa. Sin embargo, uno de los aspectos más destacados de esta nueva ley es su alineación con regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (Martínez, 2025).

El dato personal

Uno de los cambios más significativos que introdujo la nueva ley está centrada en la propia definición de dato personal sensible[1], estableciendo que 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 (Ley No. 21719, Art. 1).

De forma consistente con los avances de la ciencia y la tecnología, las características de biométricos y genéticos quizás sean las más novedosas de esta definición de dato personal. En su esencia, los datos biométricos son conjuntos de información que se generan a de características únicas y medibles del cuerpo humano o de su comportamiento. Estos datos se recogen a través de tecnologías especializadas para su posterior análisis y uso, utilizándose principalmente para la identificación y autenticación de individuos en una amplia variedad de contextos. Entre los datos biométricos más clásicos es posible mencionar las huellas dactilares, el reconocimiento facial, la retina y escaneo de iris e, incluso, la geometría de la mano. Sin embargo, hay otros datos biométricos menos comunes pero que ya se están utilizando en múltiples tecnologías y que se podrían denominar como “conductuales”. Entre ellos, la dinámica de la firma, es decir, no solo la forma de la firma, sino también cómo una persona firma (velocidad, presión, etc.); también son un dato biométrico los patrones de tecleo (velocidad y el ritmo que una persona utiliza al teclear en un teclado) y el reconocimiento de voz, que va más allá del simple reconocimiento del habla y analiza patrones acústicos y tonales que son únicos para cada individuo (Signaturite Group, 2025).

Por otra parte, los datos genéticos son aquellos que, obtenidos de un examen biológico, permiten conocer las características genéticas de una persona, heredadas o adquiridas[2], así como información única sobre sus cualidades fisiológicas o salud.

[1] Aquel que afecta la esfera más íntima de una persona y cuya utilización indebida puede dar lugar a discriminación o conllevar un riesgo grave para el titular.
[2] Las características genéticas adquiridas son cambios en la estructura o función de un organismo que ocurren durante su vida debido a factores ambientales, como la exposición al sol o el ejercicio físico.

En general, estos datos se obtienen por análisis de muestras y los más comunes son el análisis cromosómico, el análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN). Si bien estos datos podrían incluirse perfectamente dentro de la categoría más amplia de "datos relativos a la salud", la distinción es importante, ya que permiten, por ejemplo, determinar de qué países provienen los ancestros de una persona.

El consentimiento

El texto de la nueva Ley 21.719 define el consentimiento como una manifestación de voluntad libre, específica, inequívoca e informada, otorgada mediante declaración o clara acción afirmativa. Esto implica que quien pide el consentimiento debe asegurar que el individuo que va a proporcionar sus datos entienda el propósito, la base legal, destinatarios, plazos de conservación y sus derechos antes de otorgar su consentimiento. Cabe señalar que, como se mencionó anteriormente, la Ley 19.628 sobre Protección de la Vida Privada no contiene una definición explícita de consentimiento, una de sus principales debilidades.

"Uno de los ejes centrales de la nueva ley es el fortalecimiento efectivo de los derechos de los titulares de datos, permitiendo que las personas no solo sepan qué información se utiliza sobre ellas, sino que también puedan controlar su uso, exigir transparencia y tomar decisiones informadas respecto de su propia información personal"

Así, el consentimiento debe otorgarse mediante una acción afirmativa y un lenguaje claro (por ejemplo: marcar una casilla no pre-marcada, firmar un formulario, presionar "Acepto"). Para esto, los textos deben ser breves, específicos y comprensibles y se debe evitar el "consentimiento empaquetado" para múltiples finalidades. De igual forma, la revocación del consentimiento debe ser posible en cualquier momento, sin expresión de causa y por medios expeditos equivalentes a los de otorgamiento. Lo anterior no tiene efecto retroactivo sobre tratamientos ya efectuados lícitamente, pero obliga a cesar los posteriores basados en ese consentimiento (KPMG Auditores Consultores Limitada, 2025).

Por otra parte, es vital el registro y evidencia del consentimiento. La trazabilidad permitirá demostrar cumplimiento ante la autoridad y facilitará responder a las personas, por lo que se exige conservar evidencia suficiente del consentimiento: identidad del titular, fecha/hora, canal, versión del aviso mostrado y alcance (KPMG Auditores Consultores Limitada, 2025).

Derecho de acceso y portabilidad

La nueva ley refuerza significativamente los derechos de los titulares de datos personales en términos de acceso a sus propios datos, permitiendo a los ciudadanos/as conocer qué información personal se está tratando, con qué finalidad y quiénes son sus destinatarios.

Para ejercer este derecho, es necesario presentar una solicitud formal al responsable del tratamiento, quien debe responder en un plazo de 30 días corridos. Este fortalecimiento de la transparencia busca garantizar que las personas puedan supervisar y validar el uso de su información (Legal Prisma, 2024).

Otra de las novedades más relevantes de esta legislación es el derecho a la portabilidad de los datos. Esto significa que los titulares pueden solicitar la transferencia de su información personal a otro responsable del tratamiento en un formato estructurado y de uso común. Este derecho resulta especialmente útil en sectores como telecomunicaciones, servicios financieros o tecnología, donde las personas suelen cambiar de proveedor y necesitan trasladar su información sin perderla. Es importante destacar que, si el titular desea que sus datos sean eliminados del sistema una vez portados, debe realizar la solicitud de forma conjunta con la portabilidad (Legal Prisma, 2024).

Medidas de seguridad

En la nueva ley, las medidas de seguridad son los procedimientos y controles administrativos, técnicos y físicos que deben implementar las organizaciones para proteger los datos personales contra el acceso, pérdida, alteración o tratamiento no autorizado. Estas medidas son proporcionales a los riesgos identificados y garantizan la confidencialidad, integridad y disponibilidad de los datos.

Las medidas técnicas implican el uso de tecnología para proteger la información, como el cifrado de datos, el control de acceso mediante contraseñas o la implementación de firewalls y sistemas de detección de intrusiones. Por otra parte, las medidas organizativas incluyen la creación de políticas y normativas internas para el manejo de datos, la clasificación de la información según su criticidad y la capacitación del personal. Finalmente, las medidas físicas se refieren a la protección de los espacios físicos donde se almacenan o procesan los datos, como el control de acceso a las instalaciones y la custodia de documentos en papel (Twind, 2025).

Lo anterior implica obligaciones clave para las organizaciones como la seguridad desde el diseño, es decir, la privacidad y la seguridad deben considerarse desde el inicio del diseño de cualquier sistema o proceso que trate datos personales y no como una adición posterior. Por otra parte, la ley exige que las medidas sean "apropiadas", es decir, que se basen en una evaluación de riesgos y se adecuen a factores como el tipo de datos (especialmente los sensibles), el volumen, la finalidad y los costos de aplicación.

Adicionalmente, las medidas deben asegurar que los sistemas puedan recuperarse de incidentes y seguir operando de manera segura. Por supuesto, el manejo de incidentes es otro tema clave, ya que las organizaciones están obligadas a notificar incidentes de seguridad que afecten los datos personales y a tomar las medidas necesarias para mitigarlos (Twind, 2025).

Notificación de incidentes

En efecto, uno de los ejes centrales -y también uno de los más desafiantes- es la obligación de notificar las brechas de seguridad que puedan poner en riesgo los datos personales. Comprender esta exigencia y prepararse adecuadamente no es sólo es una cuestión de cumplimiento legal, sino que, además, constituye un paso clave para fortalecer la confianza digital.

La ley define la brecha de seguridad como cualquier incidente que comprometa la seguridad de los datos personales, afectando su confidencialidad, integridad o disponibilidad. Es decir, cualquier situación que ponga en riesgo el resguardo adecuado de la información de las personas. Estos incidentes pueden adoptar distintas formas, tales como accesos no autorizados a bases de datos o sistemas que contienen datos personales, filtraciones o fugas de información, pérdida o robo de dispositivos con información almacenada (laptops, discos duros, pendrives, etc.), ciberataques (ransomware, phishing, malware) y eliminación accidental de datos críticos (Datlia, 2025).

En estos casos, la ley exige que el responsable del tratamiento de los datos deberá reportar a la Agencia de Protección de Datos Personales, "por los medios más expeditos posibles y sin dilaciones indebidas", las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional (Datlia, 2025).

¿Y si no se cumple? La Ley 21.719 establece un régimen sancionatorio progresivo, y omitir las comunicaciones o los registros en los casos de vulneración de las medidas de seguridad establecidas constituye una infracción grave cuyas multas pueden alcanzar las 20.000 UTM, especialmente cuando exista negligencia en la gestión de la seguridad (Datlia, 2025).

En este contexto es que cobra mayor relevancia el Delegado de Protección de Datos (DPO), una nueva figura incorporada en la Ley 21.719 que, pese a no ser obligatoria en todos los casos, sí altamente recomendada, ya que, en la práctica, el DPO se convierte en el elemento clave para garantizar el cumplimiento de la ley, actuar como enlace con la Agencia de Protección de Datos,

gestionar consultas o reclamos de los titulares de datos y ser un atenuante de responsabilidad ante incidentes de seguridad (Carey, s.f.).

¿Por qué dos años de implementación?

El estado actual en el tema plantea desafíos que van más allá de la mera implementación de una ley. Por un lado, la creación de una Agencia de Protección de Datos Personales como entidad de control implica no solo garantizar su independencia, sino también dotarla de recursos suficientes y personal altamente capacitado. Esta agencia debe ser capaz de monitorear y sancionar de manera efectiva, lo cual representa un desafío logístico y político considerable (Lara, 2025).

Por otro lado, y tal como lo expresa Lara (2025), "la regulación enfrenta la tarea de adaptarse a un ecosistema tecnológico que evoluciona a un ritmo vertiginoso. Tecnologías emergentes como la inteligencia artificial y la biometría están redefiniendo los límites de lo que consideramos una intrusión aceptable en nuestra autonomía, nuestra vida privada y el control sobre nuestro propio cuerpo. Por ejemplo, la utilización masiva de datos biométricos en sistemas de autenticación plantea interrogantes sobre el alcance y la seguridad de estas prácticas. Asimismo, el creciente uso de algoritmos para procesar grandes volúmenes de datos personales introduce riesgos significativos en términos de discriminación algorítmica y falta de transparencia".

Esta actualización normativa no es menor y es necesario tomarle el debido peso; representa el cambio más importante en esta materia desde la Ley 19.628 de 1999. Implica un rediseño completo del enfoque legal y operativo con el que las organizaciones deben tratar los datos de sus usuarios, clientes y colaboradores.

Por ejemplo, uno de los desafíos más relevantes para las organizaciones es el desconocimiento de la localización y volumen de los datos personales que maneja. Esto abarca desde sistemas internos y bases de datos hasta correos electrónicos, documentos compartidos o respaldos en la nube. Realizar este levantamiento no es una tarea sencilla ni mucho menos de rápida ejecución. Se tiene que recorrer cada una de las áreas en búsqueda de tratamiento de datos personales (Ortiz, 2025).

Otro gran desafío es la falta de trazabilidad del ciclo de vida de los datos. Las organizaciones no solo deben identificar dónde están los datos personales, sino también tener control sobre lo que ocurre con ellos a lo largo del tiempo. En muchos casos, una vez que los datos ingresan a la organización -por ejemplo, desde un formulario o una plataforma- no existe claridad sobre quién los usa, si se comparten con terceros, si se actualizan, cuánto tiempo se conservan o en qué momento deberían eliminarse. Esta falta de trazabilidad del ciclo de vida del dato genera un riesgo importante: dificulta cumplir con los principios de la ley, y también impide responder de manera ágil ante incidentes o solicitudes de los titulares (Ortiz, 2025).

Por lo anterior, a la fecha, cualquier, institución, organización o empresa que trate datos personales debiera, al menos, estar centrado en las acciones detalladas en la Figura 2.

Fig. 1: Funciones y perfil del Delegado de Protección de Datos (DPO)
Fuente: (Carey, s.f.)

Ámbito	¿Por qué es clave?
Auditoría de datos	Saber qué datos personales se recolectan, cómo y para qué.
Actualización de políticas de privacidad	Deben ser claras, accesibles y adaptadas a la ley.
Consentimiento informado	El consentimiento ya no puede ser tácito o general.
Contratos de terceros	Verificar que los proveedores también cumplen con la ley.
Designación de un DPO	Es obligatorio para ciertos tratamientos o volúmenes de datos.
Gestión de Incidentes	Tener un protocolo para detectar y reportar brechas.

Fig. 2: ¿Qué deberían estar haciendo hoy las empresas?
Fuente: (Tysec, 2025)

Referencias

1. Carey. (s.f.). Importancia del "Delegado de Protección de Datos" en una organización. Obtenido de Carey: https://protecciondedatos.carey.cl/importancia-del-delegado-de-proteccion-de-datos-en-una-organizacion/
2. Datlia. (14 de Abril de 2025). Ley 21.719: ¿estás preparado para notificar una brecha de seguridad? Obtenido de Datlia Abogados Digitales: https://datlia.com/ley-21719-estas-preparado-para-notificar-una-brecha-de-seguridad
3. KPMG Auditores Consultores Limitada. (2025). Consentimiento en la nueva Ley de Protección de Datos: enfoque práctico y recomendaciones de implementación. Obtenido de KPMG: https://assets.kpmg.com/content/dam/kpmg/cl/pdf/2025/10/kpmg-guia-practica-consentimiento.pdf
4. Lara, J. C. (28 de Enero de 2025). Los desafíos de la nueva Ley de Protección de Datos Personales. Obtenido de Ciper: https://www.ciperchile.cl/2025/01/28/los-desafios-de-la-nueva-ley-de-proteccion-de-datos-personales/
5. Legal Prisma. (22 de Diciembre de 2024). Derechos de los ciudadanos bajo la nueva Ley de Protección de Datos Personales en Chile. Obtenido de Legal Prisma: https://www.legalprisma.cl/nueva-ley-de-proteccion-de-datos-personales/#:~:text=Para%20ejercer%20este%20derecho%2C%20es,el%20uso%20de%20su%20informaci%C3%B3n.
6. Martínez, C. (12 de Marzo de 2025). Ley 21.719: El desafío de Chile para alinearse con los estándares globales de privacidad. Obtenido de Infogate: https://infogate.cl/2025/03/ley-21-719-el-desafio-de-chile-para-alinearse-con-los-estandares-globales-de-privacidad/
7. Ortiz, P. (18 de Julio de 2025). Cuatro desafíos que las empresas están enfrentando en la implementación de la ley de protección de datos personales. Obtenido de Forbes Chile: https://forbes.cl/red-forbes/2025-07-18/cuatro-desafios-que-las-empresas-estan-enfrentando-en-la-implementacion-de-la-ley-de-proteccion-de-datos-personales
8. Signaturite Group. (21 de Marzo de 2025). Datos biométricos, ¿qué son, qué tipos hay y cómo se protegen? Obtenido de Signaturite Group: https://www.signaturit.com/es/blog/que-son-datos-biometricos/
9. Twind. (6 de Febrero de 2025). Ley de Protección de Datos Personales en Chile (Ley 21.719): todo lo que debes saber. Obtenido de Twind: https://twind.io/mx/ley-de-proteccion-de-datos-personales-en-chile-ley-21-719-todo-lo-que-debes-saber/#:~:text=Seguridad%20y%20privacidad%20desde%20el,minimizar%20la%20recolecci%C3%B3n%20de%20datos.
10. Tysec. (29 de Julio de 2025). Protección de Datos Personales en Chile: ¿estás realmente preparado para lo que viene? Obtenido de Tysec: https://www.tysec.cl/post/protecci%C3%B3n-de-datos-personales-en-chile-est%C3%A1s-realmente-preparado-para-lo-que-viene
11. Viollier, P. (2017). El estado de la protección de datos personales en Chile. Derechos Digitales. Obtenido de https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf