Datos personales, datos de vida

Patricio Inostroza

Profesor Asistente del Departamento de Ciencias de la Computación de la Universidad de Chile. Docteur en Informatique por la Université Joseph Fourier, Francia, Diplomado en Protección de Datos Personales por la Universidad de Chile e Ingeniero en Computación por la Universidad de Chile. Autor del curso Introducción al Derecho Informático, dictado para la carrera de Ingeniería en Computación, en la Universidad de Chile.

patricio.inostroza@dcc.uchile.cl

Resumen / La Ley 21.719 de Protección de Datos Personales (PDP) de Chile, promulgada en diciembre de 2024, entrará en pleno vigor en diciembre de 2026. Esta ley proactiva devuelve al titular (persona natural) el control sobre sus datos personales, estableciendo que estos derechos son intransferibles e irrenunciables.

La ley se basa en ocho principios fundamentales y seis derechos claves. Define actores específicos: el Responsable (quien responde por el cumplimiento), el Encargado (quien procesa datos), el Delegado (supervisor interno) y la Agencia de Protección de Datos Personales (organismo fiscalizador autónomo).

Todas las instituciones, públicas y privadas, manejan datos personales. El cumplimiento normativo requiere concientización de toda la organización. Si no se logra cumplir con la ley, las sanciones son severas, pudiendo alcanzar los 1.385 millones de pesos.

El 27 de junio de 2025, el diario El País de México informó que el Cartel de Sinaloa hackeó al FBI para asesinar a sus informantes en México: *"...el pirata informático... pudo obtener de su dispositivo el registro de llamadas realizadas y recibidas, así como los datos de geolocalización..."*. Si bien es una noticia sorprendente, cabe señalar que no es la primera vez que los datos personales se usan con fines letales.

Durante la Segunda Guerra Mundial, cuando los nazis invadían un país, enseguida se apoderaban de los registros locales como primer paso para controlar a la población y, en particular, para localizar a los judíos [1].

En mi infancia, el hospital de la región donde nos atendíamos tenía como política que la ficha médica no se entregaba al paciente bajo ninguna circunstancia. Si una persona cambiaba de comuna, se iba sin su ficha, sin la información de su propio historial de salud.

Los ejemplos anteriores muestran que los datos personales no sólo representan un valor económico: su control puede incluso poner en riesgo la vida de las personas.

Cuando el hospital negó el acceso al expediente, generó una dependencia de su "cliente". El paciente no tenía el control de sus propios datos personales. Cuando los nazis tuvieron acceso a los datos locales, pudieron aplicar sus políticas de discriminación y exterminio. Los datos personales les otorgaron un enorme poder sin control. Cuando el cartel de Sinaloa hackeó los datos, puso en evidencia que la seguridad requiere una mirada seria y cuidadosa.

¿Cómo enfrentar estas y otras situaciones donde el uso de los datos personales está en cuestionamiento?

La Ley 21.719 [2] vio la luz el 13 de diciembre de 2024. Conocida como Ley de Protección de Datos Personales (PDP), fue un gran paso para enfrentar las situaciones anteriores. Si bien la ley está en un periodo de transición, este periodo termina en diciembre de 2026. Los dos años que transcurrirán fue el tiempo que la misma ley estableció como suficiente para que las empresas se adapten y alcancen el pleno cumplimiento.

Los datos personales no sólo representan un valor económico: [dan poder y] su control puede incluso poner en riesgo la vida de las personas.

Pero esta ley tiene una sutil diferencia frente a otras leyes que nos gobiernan: es una ley **proactiva**. Pero no nos adelantemos; lo mejor es partir en orden.

El poder de los datos personales

Las situaciones mencionadas al comienzo de este artículo presentan características comunes: los datos personales dan poder. Acumular datos personales es acumular poder; ese poder requiere control, requiere cuidado. Pero ¿quién es el verdadero dueño de los datos personales?, ¿a quién le pertenece ese poder?, ¿quién debe controlarlo?, ¿cómo aseguramos que ese poder no caiga en manos equivocadas? y ¿cómo garantizamos que el cumplimiento sea efectivo?

La Ley 21.719 busca dar respuesta a estas y otras inquietudes.

¿Quién es el titular de los datos personales?

Formalmente, el titular es la persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

Esta definición pone de manifiesto que sólo personas naturales pueden ser titulares de datos personales. Luego, una empresa, organización o institución no será titular de datos personales, ya que no es persona natural.

Más aún, la ley retorna al titular el control y la autonomía de su información personal. Además, establece expresamente que los derechos del titular son intransferibles e irrenunciables.

¿Qué es un dato personal?

La respuesta puede parecer obvia, pero no lo es. Se tiende a pensar en el nombre, en el número del documento de identidad de una persona (RUT en Chile) o en la fecha de nacimiento, lo cual es correcto, pero hay sutilezas a cuidar.

El GPS de una camioneta no sería un dato personal, pero si a la camioneta se le asigna un chofer en particular, ahora el dato del GPS se ha transformado en un dato personal, ya que identifica a una persona. Esto último es la clave de todo.

La ley define: *"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..."*

Por lo tanto, lo que para una empresa es solo un dato industrial, para otra institución puede ser un dato personal. Luego, cada organismo privado o público debe hacer un levantamiento para conocer qué tipo de datos tiene: el primer paso para la clasificación de sus datos.

¿Cómo evitar que la ley se vuelva obsoleta?

A fines de los años ochenta, Chile logró estar conectado a Internet; el mundo comenzó a digitalizarse. En el año 1999 se promulgó la Ley 19.628, Sobre Protección de la Vida Privada. Pero esta ley pronto quedó obsoleta, ya sea porque no cubría todas las situaciones que el mundo digital comenzó a generar, o porque no había un equilibrio entre las sanciones y los beneficios que podía recibir una empresa cuando realizaba un tratamiento de datos personales que no cumplía con la ley. A esto se sumó la falta de una entidad que verificase, de forma proactiva, el cumplimiento de la ley.

Para enfrentar lo señalado, la Ley 21.719 ha establecido con relativa claridad los principios, los derechos y una Agencia para la protección de los datos personales.

¿Para qué sirven los principios en la Ley de PDP?

El espíritu de la Ley 21.719 se ha plasmado en ocho principios. A diferencia de reglas muy detalladas que pueden quedar obsoletas, los principios son más abstractos y perdurables, permitiendo que la ley se mantenga relevante ante cambios tecnológicos y sociales, cambios que son frecuentes en el mundo digital. Los principios establecen los valores o fundamentos rectores que guían cómo debe aplicarse la ley y cómo debe realizarse el tratamiento de datos personales.

Más que detallar qué indica cada principio, el siguiente set de preguntas permite evaluar de forma básica si su empresa o institución ya los cumple[1]:

- **Principio de licitud y lealtad:** ¿Obtuvo los datos personales de forma legal? ¿Hubo alguna triquiñuela para obtener los datos personales?
- **Principio de finalidad:** ¿Ha indicado claramente al titular para qué serán usados los datos personales?
- **Principio de proporcionalidad:** ¿Es realmente necesario contar con cada dato personal que mantiene su organización? ¿Se justifica ese dato para el servicio que se le entrega al titular?
- **Principio de confidencialidad:** ¿Mantiene la confidencialidad siempre, incluso finalizada la relación con el titular de los datos?
- **Principio de seguridad:** ¿Dispone de la seguridad adecuada para evitar fugas o robo de los datos personales? ¿Y cómo está la seguridad de sus proveedores?
- **Principio de transparencia e información:** ¿Ha informado de forma adecuada al titular de lo que hará con los datos personales? ¿Dispone de los medios para que el titular de los datos ejerza sus derechos?
- **Principio de calidad:** ¿Mantiene todos los datos personales actualizados? ¿En todos los sistemas de la empresa?
- **Principio de responsabilidad:** ¿Tiene claro que siempre será el responsable del tratamiento de los datos personales, incluso si delega el tratamiento a un tercero?

1 En rigor, el trabajo de evaluación debe ser realizado por un especialista en Protección de Datos Personales. Este cuestionario sólo tiene como fin mostrar los elementos básicos, por lo que debe ser tomado sólo como un elemento introductorio en el tema.

Al contar con estos ocho principios se tiene una base sólida que permite destrabar situaciones no previstas por la ley. Es un marco que orienta a jueces, autoridades y profesionales al enfrentar nuevas situaciones. Establece cómo debería ser el comportamiento de las instituciones privadas y públicas. Da un marco para enfrentar y adaptarse a nuevas tecnologías. Orienta cómo velar por su cumplimiento. Permite tener una primera aproximación para que profesionales de diversas ramas, como ingenieros, médicos, periodistas y más, puedan evaluar si sus proyectos cumplen con la normativa. Y, sobre todo, protegen al titular de los datos cuando la ley no cubre un caso particular.

¿Cuáles son los derechos en la Ley de PDP?

Al inicio de este artículo presentamos situaciones que mostraban que la relación entre las personas y las organizaciones que recolectaban datos era muy desigual. El titular entregaba su información, pero tenía poca capacidad para saber qué pasaba con ella después.

Seis son los derechos que permiten a las personas ejercer control efectivo sobre sus datos. Gracias a estos derechos, el titular decide qué pasa con su información. Sin estos derechos, el tratamiento quedaría sólo en manos de las empresas u organismos públicos. Ahora las instituciones, bajo solicitud del titular, deben informar qué datos tienen, para qué los usan, si los comparten y cuánto tiempo los conservarán. Con esta información, el titular puede solicitar que se rectifiquen, actualicen o supriman datos con información inexacta, obsoleta o innecesaria. Incluso puede revocar el consentimiento para el tratamiento de sus datos personales, salvo en casos que la misma ley expresamente lo impida.

Frente a la capacidad que tienen las instituciones públicas y privadas para recopilar y procesar grandes volúmenes de datos, los derechos del titular funcionan como un contrapeso que restablece el equilibrio.

- **Derecho de acceso:** El organismo que haga tratamiento de datos personales debe responder al titular si se están tratando sus datos, incluyendo su origen, finalidad y destinatarios.

- **Derecho de rectificación:** Permite al titular solicitar que se modifiquen o complementen datos inexactos, desactualizados o incompletos.

- **Derecho de supresión (o cancelación):** Este derecho permite al titular solicitar que se eliminen los datos cuando ya no sean necesarios, cuando se haya revocado el consentimiento o cuando hayan expirado los plazos de conservación.

La ley retorna al titular el control y la autonomía de su información personal.

- **Derecho de oposición:** Le da derecho al titular de rechazar tratamientos específicos, como decisiones automatizadas o perfiles basados en datos sensibles, salvo excepciones legales.

- **Derecho a la portabilidad:** Si el titular lo solicita, el organismo debe entregar una copia de sus datos personales en formato estructurado. Incluso puede solicitar que se transfieran sus datos a otro responsable (empresa).

- **Derecho de bloqueo:** Finalmente, el titular puede solicitar suspender temporalmente el tratamiento de sus datos personales cuando se impugne su exactitud o se investigue una infracción.

Es necesario hacer presente que no es suficiente que la empresa dé cumplimiento a los derechos solicitados por el titular de los datos personales. En efecto, es importante que además deje registrado todo tratamiento en una plataforma o medio auditable. Toda transacción relacionada con el tratamiento de datos puede ser sometida a cuestionamiento, lo que puede terminar en un litigio y con esto enfrentar un peritaje. Si el registro es digital, el peritaje lo realizaría un informático.

En cada caso deberá demostrar que el requerimiento del titular fue atendido en el plazo estipulado por la ley y que el titular fue informado de la respuesta. Notar que la temporalidad es crucial, es decir, hay que demostrar que la respuesta fue entregada en el plazo que la ley estipula.

¿Cómo la ley protege al titular de los datos personales?

En general, una de las principales falencias de las leyes es que actúan de forma *reactiva*. Sólo cuando una persona u organismo quebranta la ley y es atrapado, se recurre a ella, donde se activa la investigación, la acusación y la defensa. Si lo amerita, recaen las sanciones. Este modelo presenta una grave falencia: a pesar de que puedan existir sanciones, el daño ya está hecho, lo que en muchos casos es irreversible.

La Ley 21.719 ha sido propuesta como una ley *proactiva*, una ley que obliga a cada institución, pública o privada, a velar por el cumplimiento en cada instante. A esto se suman las sanciones, tema que ahondaremos más adelante.

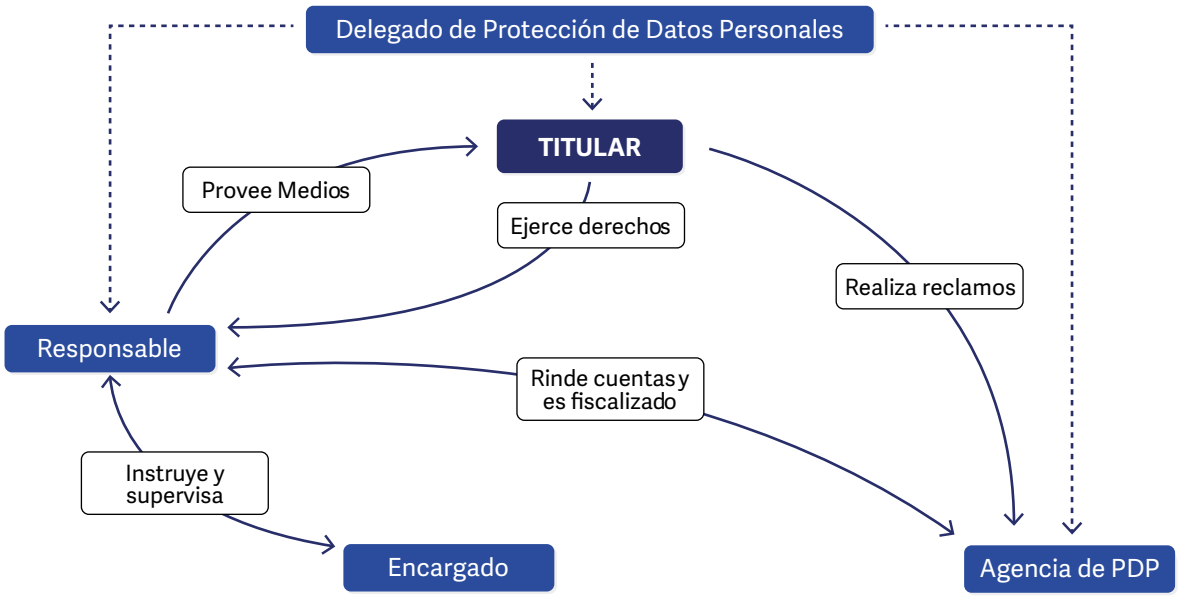

Figura 1 / Esquema simplificado de la interacción de los actores en la Ley 21.719.

¿Cómo es que esta ley tiene actores?

En esencia, la ley crea un sistema donde el *Titular* tiene el poder, el *Responsable* asume la responsabilidad frente a cualquier tratamiento que no cumpla con la ley, el *Encargado* es quien efectúa el tratamiento de datos personales bajo estrictas reglas, donde el *Delegado* asegura una correcta implementación interna. Finalmente, está la *Agencia* de Protección de Datos Personales, encargada de supervisar todo el sistema y de aplicar las sanciones (ver Figura 1).

El titular ya ha sido descrito, por lo que nos centraremos en el resto de los actores.

La empresa o institución debe contar con un *Responsable* y un *Encargado*. El primero es el principal obligado y debe responder por el cumplimiento de la ley. Entre otras actividades, debe velar por el cumplimiento de los derechos del titular, llevar un registro de las operaciones realizadas y, en caso de problemas de seguridad, notificar a la Agencia de Protección de Datos Personales y al titular cuando sea relevante.

A su vez, el *Encargado* es una persona natural o jurídica que trata datos personales. No decide sobre los datos, sólo los procesa siguiendo instrucciones. Cabe señalar que la responsabilidad sigue recayendo sobre el Responsable. Si el Encargado es un servicio tercerizado, será necesario revisar los contratos y velar por que estos cumplan con la ley, es decir, que se preserve la confidencialidad y seguridad de la información, donde además no puedan usar los datos para un fin propio.

Una de las innovaciones más interesantes de la ley corresponde a la creación de la *Agencia* de Protección de Datos Personales. Éste es un organismo público, autónomo y técnico, destinado a supervisar y fiscalizar el cumplimiento de la normativa. Además, media en conflictos entre titulares y responsables, emite instrucciones y guías sobre cómo aplicar la ley e impone severas sanciones (multas), entre otras funciones.

Si bien hay otros actores que escapan del fin de este artículo, hemos dejado para el último al *Delegado* de protección de datos personales. Este es una persona natural designada por el Responsable del tratamiento para actuar como un puente de comunicación entre el Responsable, los Titulares y la Agencia. Su rol es supervisar el cumplimiento interno de la ley y fomentar una cultura de protección de datos dentro de la organización. Su accionar debe ser proactivo y autónomo, teniendo presente que no puede tener conflictos de interés.

Esto último es esencial. Dado que el área TI y el área de recursos humanos realizan tratamiento de datos personales, quedarían inmediatamente excluidos del rol de delegado.

¿Cómo son las sanciones?

Esta ley establece tres tipos de infracciones: leves, graves y gravísimas, donde las multas bordean en su cota superior los 345 millones, 690 millones y 1.385 millones de pesos, respectivamente[2].

Las infracciones leves son de orden administrativo, como incumplir el principio de información y transparencia, no proveer datos para contactar al responsable, dar una respuesta incompleta o fuera de plazo.

En el punto medio, las infracciones graves incluyen problemas como no contar con el consentimiento del titular, tratar datos personales innecesarios, realizar tratamiento de datos personales de niños sin el adecuado resguardo, fallas en la seguridad, vulnerar el secreto o confidencialidad, entre otras.

Y, finalmente, las infracciones gravísimas: tratar datos personales de forma fraudulenta (uso de bases de datos del mercado negro), usar información no veraz, no informar de vulneración en las medidas de seguridad, incluso el incumplir una resolución de la Agencia, son parte de las sanciones más elevadas que puede sufrir una empresa.

¿Y cómo se cumple con la ley?

Cada vez que un empresario, gerente o director de empresa señala que esto es un tema del área de informática, muestra que no ha comprendido lo que implica dar cumplimiento a la ley.

Esta ley afecta a todos los integrantes de la empresa. Si un empleado incumple la ley, si un proveedor que maneja los datos personales sufre una fuga de datos, si recursos humanos recopila los datos de los hijos de los trabajadores para entregar regalos de Navidad pero sin el debido resguardo, la sanción recae en el responsable de la empresa. Notar que en cada ejemplo de este párrafo no intervino el área de TI.

Los principios [que establece la ley] son más abstractos y perdurables, permitiendo que se mantenga relevante ante cambios tecnológicos y sociales.

La palabra clave para dar inicio al cumplimiento de la Ley 21.719 es la *concientización* en el tema, partiendo por la plana mayor y luego a los colaboradores y las empresas o proveedores externos. Sin una adecuada capacitación se genera desconocimiento del problema y aparece la resistencia al cambio.

En paralelo, hay que revisar y actualizar el reglamento interno y los contratos, tanto los de trabajo como los de proveedores. A esto se suma que hay que realizar un levantamiento de los tipos de datos personales que maneja la empresa para verificar que se cumplan los principios. Revisar si los modelos de seguridad interna son los adecuados, si la privacidad se cumple, establecer roles de mínimo acceso a los datos personales. Contar con un registro de cada tratamiento de datos, un registro que soporte una auditoría (peritaje) legal. Muchos de estos temas se cruzan con ISO 27001[5].

La implementación del equivalente de esta ley en Europa y otros países ha generado más de un dolor de cabeza, especialmente a quienes reaccionaron demasiado tarde.

Al momento de publicarse este artículo, restarán pocos meses para cumplir una ley que exige definiciones a nivel de directorio y gerencia, asignación de recursos y una gestión efectiva de los riesgos asociados al tratamiento de datos personales. Esto es un trabajo colaborativo entre abogados, informáticos, asesores, personal de la empresa, proveedores, etc. Poner a todos de acuerdo con el mismo objetivo requiere de planificación. No espere hasta última hora. B

Referencias

[1] Carissa Véliz, "Privacidad es poder: datos, vigilancia y libertad en la era digital". Editor digital: XcUiDi.

[2] Ley 21.719: Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales. https://www.bcn.cl/leychile/navegar?idNorma=1209272.

[3] La Verdadera y Real Historia de Internet en Chile. https://users.dcc.uchile.cl/~ppoblete/sigloxxi-27Feb96.html.

[4] Ley 19.628 Sobre Protección de la Vida Privada. https://www.bcn.cl/leychile/navegar?idNorma=141599.

[5] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001.

2 Valores aproximados a la fecha de la publicación de los 5 mil UTM, 10 mil UTM y 20 mil UTM que efectivamente la ley establece.