Desafíos y oportunidades del proyecto de ley de protección de datos personales en chile: el reconocimiento de los datos laborales

Rosario Letelier[1]

La legislación chilena vigente en materia de protección de datos personales data desde el año 1999, pero recién en 2018, por la Ley N° 21.096, el Derecho de Protección de Datos Personales adquiere reconocimiento constitucional. Esto ha conllevado a que varios sectores, hayan tenido que dictar normas generales para suplir las falencias de nuestra actual ley. Particularmente, en el ámbito de la protección de niños, niñas y adolescentes, su regulación se encuentra omitida hasta el año 2022, con la Ley N°21.430 sobre Garantías y Protección Integral de los Derechos de la Niñez y Adolescencia, que introdujo normas específicas al respecto. Actualmente, tampoco existe en la ley una definición de datos laborales, lo que ha requerido la aplicación de normas o directrices generales para su manejo por organismos no especializados. En cuanto a los datos personales de especial protección, llamados "sensibles" – tales como los biométricos – tampoco se encuentran expresamente reconocidos en la actual ley, a diferencia de lo que propone el proyecto ley, que sí los incluye en la definición de datos sensibles.

El Proyecto de Ley de Protección de Datos Personales (el "Proyecto") que establece un periodo de implementación de 24 meses desde su publicación de la ley en el Diario Oficial, supone un enorme desafío para todos los sectores en Chile, especialmente para el sector privado. El Proyecto busca regular aspectos que quedaron "al debe" en nuestra legislación actual, adoptando el estándar del Reglamento de Protección de Datos Personales (RGPD) de la Unión Europea. El Proyecto introduce nuevas bases legales para el tratamiento de datos, y principios renovados para el tratamiento. Un cambio significativo del Proyecto es que la carga de la prueba ahora recae sobre el responsable de los datos, quién debe demostrar su cumplimiento con la normativa. De gran relevancia es la creación de una Agencia de Protección de Datos, que actuará como la autoridad reguladora, responsable de sancionar, incluso de oficio, a quienes infrinjan la ley y certificar modelos de prevención de infracciones, validando estándares de cumplimiento, que servirán como atenuantes en caso de sanciones por incumplimiento.

[1] Gerenta Legal y de Cumplimiento en Defontana.

Ante la inminente aprobación del Proyecto, las empresas enfrentan el reto de comenzar el inventario de los datos que tratan, conocido como "registro de actividades de tratamiento" según el RGPD. Aunque el Proyecto solo lo menciona superficialmente, este registro es fundamental. Las empresas deben empezar, como punto de partida, por identificar los datos de sus trabajadores. Desde las etapas de preselección laboral hasta el procesamiento de nóminas y la terminación de la relación laboral. Es increíble la cantidad de datos que almacenan las empresas sobre sus trabajadores, desde afiliación sindical, datos financieros, biométricos, hasta datos de salud de hijos de los trabajadores, entre otros, muchos más de los necesarios para cumplir con la ley.

El artículo 154 bis del Código del Trabajo obliga al empleador a mantener reserva de toda la información y datos privados del trabajador a que tiene acceso en virtud de la relación laboral. Con la pandemia, se aceleró la adopción de tecnologías para el teletrabajo y los sistemas digitales de control y asistencia. El dictamen de la Dirección del Trabajo N° 2927/58 de diciembre de 2021 autoriza el uso de sistemas digitales que incluyen biometría, siempre y cuando se cumplan ciertos requisitos legales y técnicos, a diferencia de lo que ocurre en Europa donde el RGPD no permite la utilización de sistemas biométricos para fines laborales. La Agencia Española de Protección de Datos limita el uso de sistemas biométricos para fines laborales, y debe justificarse su uso demostrando que el sistema es necesario y proporcional. Establece que habrá que ponderar si existen medidas técnicas que puedan ser menos intrusivas.

Los sistemas de geolocalización para el registro de asistencia, según el mencionado dictamen, están permitidos con el consentimiento expreso del trabajador y sólo para registrar su asistencia. Es decir, un sistema de geolocalización no debe usarse para monitorear la ubicación de un trabajador en todo momento, y se deben tomar medidas para proteger su información como utilizar para estos efectos obligatoriamente los correos electrónicos personales de los trabajadores en vez de los corporativos. El dictamen incluye un apartado especial dedicado a garantizar la protección de los derechos fundamentales en el uso de estos sistemas. Es crucial la moderación en la intensidad del control; por tanto, no se considerarán ajustados a derecho aquellos sistemas que permitan una vigilancia constante a los trabajadores. Además, no se ajusta a derecho exigir que el GPS este activo durante toda la jornada laboral,

dado que no se conciben como sistemas de vigilancia continua y sólo se permite su uso excepcionalmente en casos específicos.

De igual manera, se enfatiza en la protección de los datos personales del trabajador. Los sistemas que requieran datos personales, como la huella digital o el número de teléfono personal, deben obtener el consentimiento explícito del trabajador, plasmado en el contrato de trabajo o un anexo al mismo. Este documento debe especificar claramente la finalidad del tratamiento de los datos. Además, es imperativo que los datos personales recopilados sean destruidos por el sistema en un plazo no menor a 90 días ni mayor a 120 días tras la terminación de la relación laboral, salvo que se requiera mantenerlos temporalmente por requerimientos judiciales. El dictamen también establece que los trabajadores tienen en todo momento el derecho de solicitar la eliminación de sus datos del sistema, y que los empleadores serán responsables de cumplir con las normas sobre el tratamiento de datos personales.

Es común que tanto los sistemas de control y asistencia como el pago de nóminas se deleguen a terceros proveedores especializados en ofrecer estos servicios a las empresas. No obstante, surgen preguntas: ¿Quién es el responsable ante los trabajadores respecto a estos datos, la empresa empleadora o el tercero?

A pesar que estos datos sean gestionados por un proveedor externo, típicamente mediante un software, el responsable del tratamiento, es decir, quién define los fines y los medios del tratamiento, sigue siendo el empleador. Este tercero, el proveedor, actúa como encargado del tratamiento bajo la dirección y en nombre del responsable, siempre y cuando cumpla con los fines para los que le han sido encomendados. Para ello, debe existir un contrato de encargado de tratamiento en que regule sus obligaciones, las cuales son esencialmente las mismas impuestas al responsable, incluyendo altos estándares de seguridad en el manejo de datos para garantizar la integridad, disponibilidad y confidencialidad de los datos. Este contrato también, debe exigir al tercero que cuente con políticas al respecto, como por ejemplo una política de eliminación de datos.

En consecuencia, es crucial que tanto el responsable como el encargado cuenten con robustas políticas de seguridad de la información para sus colaboradores, definiendo claramente los perfiles de cada cargo, sus funciones y responsabilidades, políticas de privacidad para sus usuarios y que las empresas de software que ofrecen estos servicios contemplan la protección desde el diseño y por defecto en el desarrollo de sus productos. Es fundamental la formación y sensibilización de estas materias, dado que el incumplimiento puede poner en riesgo los derechos fundamentales de los trabajadores, y potencialmente, la reputación de la empresa.