

Videovigilancia, control biométrico y seguimiento geolocalizado de trabajadores: Tratamiento de datos personales a la luz de la ley 21.719

Video surveillance, biometric control and geolocated tracking of workers: Processing of personal data in accordance with Law 21.719

PABLO VIOLLIER*

Universidad Central de Chile, Santiago, Chile

pablo.viollier@alumnos.ucentral.cl | <http://orcid.org/0000-0001-9893-7974>

PABLO CONTRERAS**

Universidad Central de Chile, Santiago, Chile

pablo.contreras@ucentral.cl | <https://orcid.org/0000-0002-1131-182X>



Recibido: 20/08/2025 | Aceptado: 12/12/2025 | Publicado: 15/01/2026

Resumen. El tratamiento de datos personales en el ámbito laboral representa hoy un desafío clave para el derecho del trabajo y el compliance corporativo. En Chile, la doctrina laboral ha estudiado la potestad de control del empleador frente a derechos fundamentales, pero sin integrar de forma sistemática el derecho a la autodeterminación informativa, reconocido constitucionalmente desde el año 2018. Este derecho plantea exigencias de licitud, proporcionalidad y transparencia en el uso de datos con fines de control.

Este trabajo analiza tres actividades frecuentes y de alto riesgo regulatorio: tratamiento de datos biométricos para control de asistencia y acceso, videovigilancia y uso de datos de geolocalización a la luz de las nuevas obligaciones contenidas en la ley N° 21.719. Se identifican bases de licitud, obligaciones de transparencia, proporcionalidad y seguridad, advirtiendo que la inobservancia de estas reglas puede implicar multas severas. El estudio

* Abogado y diplomado en ciberseguridad de la Universidad de Chile. Advanced LLM in Law and Digital Technologies de la Universidad de Leiden. Estudiante del programa de Doctorado en Derecho de la Universidad Central de Chile y la Universidad de Sevilla.

** Doctor en derecho, Northwestern University. Director del Doctorado en Derecho de la Universidad Central de Chile y director de la Cátedra Legal Tech UCentral.

propone lineamientos para compatibilizar las facultades de control empresarial con la nueva regulación y estándares internacionales.

Abstract. Processing personal data in the workplace is now a key challenge for labor law and corporate compliance. In Chile, labor doctrine has examined the extent of an employer's control over fundamental rights. However, it has not systematically incorporated the constitutionally recognized right to informational self-determination, established in 2018. This right requires the use of data for control purposes to be legal, proportional, and transparent.

This paper analyzes three frequent, high-risk regulatory activities: processing biometric data for attendance and access control, video surveillance, and using geolocation data while complying with the standard contained in Law N° 21.719. The paper identifies bases for legality and obligations of transparency, proportionality, and security. It warns that failure to comply with these rules may result in severe fines. The study proposes guidelines for reconciling corporate control powers with the new regulation and international standards.

Palabras clave. datos biométricos; videovigilancia; geolocalización; ley 21.719; datos personales

Keywords. biometric data; video surveillance; geolocation; law 21,719; personal data

1. Introducción

El tratamiento de datos personales en el ámbito laboral constituye, en la actualidad, uno de los desafíos regulatorios más relevantes para el derecho del trabajo y para las exigencias de cumplimiento o *compliance* corporativo. Si bien en Chile la literatura jurídica ha abordado con cierta profundidad el alcance y límites de la potestad de control del empleador —particularmente en relación con la intimidad y otros derechos fundamentales de los trabajadores—, persiste un vacío significativo en el examen sistemático de cómo dichas facultades interactúan con el derecho constitucional a la autodeterminación informativa. Este derecho, entendido como la facultad “de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad” (Del Castillo, 2007, p. 214) es de reconocimiento relativamente reciente en el ordenamiento nacional (Contreras, 2020, p. 89) y plantea interrogantes sustantivos sobre la licitud, proporcionalidad y transparencia en el uso de información personal con fines de control empresarial.

Las investigaciones doctrinales del laboralismo chileno han contribuido a mapear las tensiones entre tecnología, condiciones laborales y derechos fundamentales¹. No obstante, estas aproximaciones tienden a situarse en un plano general, abordando fenómenos

¹ Véase *infra* §2.

como la desconexión digital, la vigilancia en el trabajo o la transformación del concepto de subordinación, sin desarrollar en profundidad las implicancias jurídicas específicas que emergen de tratamientos concretos de datos personales —por ejemplo, biométricos, de videovigilancia o de geolocalización—. Sin embargo, y pese a que la autodeterminación informativa fue incorporada como derecho fundamental en nuestra Constitución (Contreras, 2020), todavía existe un terreno escasamente explorado en la intersección entre derecho del trabajo y derecho de protección de datos.

A nivel comparado, la doctrina europea y ciertos desarrollos normativos, como el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés), han generado criterios detallados sobre licitud, limitación de la finalidad y minimización de datos en contextos laborales. Asimismo, organismos como la Agencia Española de Protección de Datos (AEPD) y el European Data Protection Board (EDPB por sus siglas en inglés) han emitido guías y dictámenes que clarifican la naturaleza jurídica de los datos biométricos, los estándares para la videovigilancia y el uso legítimo de datos de localización en el empleo. Sin embargo, la adaptación de estos estándares al contexto normativo y cultural chileno no ha sido objeto de un trabajo sistemático, lo que genera un déficit de lineamientos claros para empleadores y trabajadores.

En el plano normativo interno, la ley 19.628, sobre protección de la vida privada, conforme a lo reformado por el artículo primero de la ley 21.719, que regula la protección de los datos personales y crea la Agencia de Protección de Datos Personales, establece un marco más robusto para la protección de datos personales, incorporando definiciones y categorías antes ausentes, como la de datos biométricos y datos de geolocalización. Este avance plantea oportunidades para reforzar la eficacia horizontal de los derechos fundamentales en la relación laboral, pero también introduce complejidades operativas para las empresas. La calificación de ciertos datos como sensibles, las exigencias de evaluaciones de impacto y las limitaciones a las bases de licitud disponibles para su tratamiento imponen exigencias técnicas y organizativas que pueden entrar en tensión con las prácticas habituales de control.

En este escenario, el presente trabajo se propone aportar un análisis jurídico detallado de tres actividades de tratamiento de datos especialmente relevantes en el ámbito laboral: el tratamiento de datos biométricos para control de asistencia y acceso; el tratamiento de datos obtenidos mediante sistemas de videovigilancia; y el tratamiento de datos de geolocalización con fines de supervisión y control.

La elección de estos tres tipos de actividades de tratamiento responde a su alta frecuencia de uso en la práctica empresarial y a la ausencia de un estudio doctrinal exhaustivo que vincule su operativa concreta con las exigencias de la nueva legislación chilena en materia de protección de datos. Además, permiten identificar, de forma comparada y transversal, patrones comunes de riesgo regulatorio y desafíos de *compliance* que trascienden el caso particular de cada tecnología.

Para estructurar el análisis dogmático de las disposiciones legales y reglamentarias pertinentes, hemos recurrido a la revisión de guías técnicas y pronunciamientos administrativos nacionales e internacionales. En particular, nos enfocamos en guías técnicas y pronunciamientos administrativos europeos, producto de la fuerte inspiración que la ley 21.719 tiene en el GDPR (Bordachar, 2022, p. 398). Ello permite no solo identificar las bases de licitud aplicables en cada caso, sino también precisar las obligaciones de transparencia, proporcionalidad y medidas de seguridad que resultan exigibles.

Con ello, este estudio busca llenar un doble vacío en la literatura nacional. Primero, el déficit de análisis específico sobre tratamientos concretos de datos personales en el contexto laboral, más allá de consideraciones generales sobre vigilancia o control. Y segundo, la falta de propuestas claras para la implementación de prácticas empresariales compatibles con la nueva regulación y con estándares internacionales consolidados.

Bajo la ley 21.719, el incumplimiento de las nuevas reglas de tratamiento de datos personales puede acarrear sanciones significativamente más altas que aquellas que se derivan del incumplimiento de normas laborales. En efecto, el incumplimiento de la base de licitud aplicable a una determinada actividad de tratamiento de datos personales puede constituir una infracción grave, conforme al artículo 34 ter, letra a), sancionable con hasta 10.000 unidades tributarias mensuales (más de 660 millones de pesos, aproximadamente)². Este tipo de nuevas reglas cambian radicalmente la práctica organizacional que, hasta el momento, ha conducido la gestión y procesamiento de información personal de los trabajadores. Por ello, este texto pretende ilustrar cómo la nueva regulación de protección de datos personales afectará directamente el alcance de las facultades de control y supervisión del empleador y que nivel de injerencia tendrá la Agencia de Protección de Datos Personales en modular la tutela de la autodeterminación informativa en la relación laboral.

El nuevo régimen de la protección de datos personales suma un componente relevante en materia de litigios laborales. El empleador que procese datos personales de un trabajador, con infracción a la normativa, no solo arriesga la imposición de las multas contenidas en la ley 21.719, sino que dicho tratamiento constituye una potencial afectación al derecho fundamental de la autodeterminación informativa, susceptible de ser perseguida mediante el procedimiento de tutela laboral conforme al artículo 485 del Código del Trabajo, en concordancia con el artículo 19 n.º 4 de la Constitución.

El trabajo se estructura de la siguiente forma. Primero, se explica en términos generales cómo se ha abordado hasta el momento el fenómeno de la protección de datos de los trabajadores y su tratamiento. Aquí se describe el estado del arte desde el punto de vista de la doctrina laboral y su estrecho enfoque basado en la tutela de privacidad y la intimidad de los trabajadores. Por ello, el texto plantea que es necesario avanzar en el

²En caso de que el infractor corresponda a una empresa distinta de aquellas definidas como empresas de menor tamaño en el artículo segundo de la ley 20.416, que reincide en dicha infracción, la multa podrá alcanzar el monto correspondiente al 2% de los ingresos anuales por ventas y servicios y otras actividades del giro en el último año calendario. En caso de infracciones gravísimas la multa puede alcanzar el 4%.

análisis de las reglas generales y especiales sobre el tratamiento de datos personales, de manera tal de hacer converger la nueva regulación al ámbito del Derecho del Trabajo. Luego, el artículo se divide en tres secciones, cada una enfocada en una actividad de tratamiento de datos específico: el tratamiento de datos biométricos, la videovigilancia y el procesamiento de datos de geolocalización. En cada uno de estos casos es posible determinar que la información personal del trabajador es necesaria para que el empleador pueda controlar al mismo individuo, sus instalaciones y los bienes o terceros. Para cada una de estas secciones se explica el tipo de dato involucrado, su base de licitud y las reglas aplicables en materia de protección de datos. El artículo concluye que el detalle y aterrizaje de las reglas de protección de datos complejizan el análisis que hasta el momento se ha hecho respecto del uso y procesamiento de información de los trabajadores y que, de no abordarlo adecuadamente, las organizaciones se exponen a serias multas por los incumplimientos regulatorios que pudieren suscitarse.

2. Tratamiento de datos personales en el ámbito laboral y el control a través del tratamiento de información personal

La literatura mayoritaria en Chile ha estudiado el control que ejerce el empleador y cómo esta potestad puede colisionar con otros derechos fundamentales (Ugarte 2018, Gamonal Contreras y Guidi Moggia 2020). Sin embargo, no ha profundizado sobre cómo lo hace respecto de un relativo nuevo derecho constitucional: el derecho a la autodeterminación informativa y el uso de la información personal (Contreras, 2020; 2022)³. Algunos trabajos como el de Lizama y Lizama (2020) y Castro (2020) han recogido aspectos centrales de la relación entre tecnología y derecho del trabajo, especialmente respecto de su impacto en el ejercicio de derechos fundamentales como la intimidad y con referencias a la protección de datos personales en conexión a la privacidad. Lo mismo ocurre con trabajos que destacan el impacto de la tecnología en las condiciones del trabajo, como en materia de teletrabajo (Guidi Moggia, 2023, pp. 137 y ss.), desconexión digital (Varas Marchant, 2024), la subordinación o dependencia (Sierra Herrero, 2022; Ugarte, 2020; Pérez, 2022, pp. 71-102), el control o vigilancia (Debesa, 2021), o la configuración misma del trabajo (Coddou Mc Manus y Padilla Parga, 2024, pp. 1-34).

Por otro lado, se ha prestado atención a cómo la gestión algorítmica del trabajo requiere un uso intensivo de datos personales, con consecuencias en su tutela directa (Contreras, 2022; Viollier y Velasco, 2021) y con externalidades que impactan en otros derechos, como la igualdad laboral (Coddou, 2022; Herrera, 2022). Esto se da especialmente en trabajos como aquellos prestados vía plataformas digitales (Palomo Vélez et al., 2022, pp. 59-99; Irureta Uriarte, 2023, pp. 1092-1095; Asenjo Cruz et al., 2023). Por otro lado, el control a partir del uso de información personal ha sido siempre uno de los mecanismos para

³ A nivel comparado ver Rodríguez (2021); Todolí y Rodríguez-Piñero (2020).

ejercer las facultades del empleador, con distintos tipos de registros (Pasquinelli, 2023), los cuales ahora son de corte digital.

Algunos pocos trabajos han hecho un énfasis en la protección de datos personales en materia laboral. A nivel de interpretación administrativa, Neira Reyes (2022) ha demostrado cómo la Dirección del Trabajo ha comenzado a internalizar ciertos criterios de protección de datos bajo el marco del Código de Trabajo, especialmente en materia de vigilancia por parte del empleador y del resguardo de la información personal de los trabajadores. Publicaciones recientes buscan acomodar los aspectos de la nueva ley 21.719 a la realidad laboral, como lo que plantean Cárdenas Oyarzún y Uribe Conejeros (2025). Estos autores describen el nuevo régimen legal de protección de datos personales y, a su vez, lo consideran como parte de la eficacia horizontal de los derechos fundamentales y las limitaciones de las facultades del empleador, apremiando la necesidad de generar una cultura de cumplimiento o *compliance* en la materia.

La ausencia de discusiones específicas sobre ciertos tratamientos de datos, en el ámbito laboral y empresarial, es parte del panorama de la literatura chilena. Por ello, las implicancias para la gestión del trabajo y, a su vez, el cumplimiento en materia de datos personales exige un análisis detallado de ciertas actividades de tratamiento que suelen ser comunes en la actividad empresarial pero que no han sido suficientemente atendidas por la doctrina.

Al tratarse de impactos prácticos que repercuten en un derecho fundamental del trabajador, por un lado, y la organización empresarial, por la otra, en las secciones que siguen analizaremos tres tipos de tratamientos de datos personales que son efectuados por las empresas, bajo el prisma de la ley 21.719, con el objeto de considerar su mejor intelección para la práctica jurídica local. Para ello, abordaremos los tratamientos de datos biométricos, de videovigilancia y de geolocalización por separado.

3. Tratamiento de datos biométricos para el control de asistencia

3.1. Naturaleza del dato biométrico

La definición de *dato biométrico* es una novedad de la ley 21.719 y que no contemplaba el texto original de la ley 19.628 (Becker Castellaro y Garrido Iglesias, 2017, p. 68). Bajo el nuevo marco legal, el artículo 16 ter define a los datos personales biométricos como “aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella”. A continuación, entrega una lista ejemplar de datos que siempre deben ser considerados como biométricos, entre ellos el iris, los rasgos de la mano o faciales y la voz.

Un dato biométrico siempre deberá ser considerado un dato personal de carácter sensible (Garrido y Sáenz, 2024, p. 7), por dos razones. Primero, porque el artículo 16 ter se encuentra en el Párrafo Segundo de la nueva legislación, titulado “Del tratamiento de los datos personales sensibles”. Segundo, porque se encuentra explícitamente

mencionado en la definición de dato sensible contenida en el artículo 2 letra g)⁴. Por tanto, los datos biométricos deben ser considerados como un subconjunto de datos personales sensibles. Entre las consecuencias jurídicas de que los datos biométricos sean calificados como datos sensibles se encuentran:

- a) En caso de que exista una filtración de datos personales sensibles, el responsable no solo deberá reportar este incidente a la Agencia de Protección de Datos Personales, sino que también a los titulares afectados (artículo 14 sexies, inciso final).
- b) Si los datos sensibles son tratados en una hipótesis de excepción al consentimiento, será obligatorio la realización de una Evaluación de Impacto en los términos del artículo 15 ter letra d).
- c) Un catálogo de bases de licitud para el tratamiento más acotado y estricto.
- d) Sanciones más estrictas y de mayor cuantía (infracciones gravísimas).

A fin de evitar una interpretación excesivamente expansiva de qué información debe ser considerada como dato biométrico, y por tanto cumplir con todos los requisitos establecidos para los datos sensibles, es importante distinguir entre un dato personal contenidos en fotografías y grabaciones de video de un dato biométrico propiamente tal.

La particularidad de un dato biométrico es que ha sido obtenido a través de un tratamiento técnico específico, el que a su vez debe permitir identificar o confirmar la identidad única de una persona (Jasserand, 2016, p. 5). De este modo, si bien una imagen fotográfica o de grabación en video contendrá datos personales (las características físicas de una persona que permitan identificarla), el tratamiento de dichos datos no necesariamente cumple con el estándar para ser considerado como un dato biométrico⁵.

En este sentido, el considerando 51 del GDPR ha señalado que

el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas *con medios técnicos específicos* permita la identificación o la autenticación unívocas de una persona física⁶.

La *Guía sobre tratamientos de controles de presencia mediante sistemas biométricos*, de la AEPD, profundiza sobre esta distinción desde un punto tecnológico, señalando que

⁴ Dicho artículo establece que serán considerados sensibles 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, 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”. El énfasis es nuestro.

⁵ Sin perjuicio de esto, véase la opinión de Cárdenas Oyarzún y Uribe Conejeros, 2025, p. 12, que plantea que “es posible considerar como datos sensibles las fotografías institucionales”.

⁶ El énfasis es nuestro.

un dato biométrico no se almacena en un medio leíble por un ser humano (como una fotografía o video), sino que se “almacena en forma de una plantilla o patrón biométrico. Una plantilla biométrica es una forma de escritura de una característica biométrica humana, como un rostro o una huella dactilar, de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados. La plantilla biométrica no está orientada a ser interpretada por una persona, como una fotografía, sino que está orientada a ser tratada en un proceso automatizado, es decir, ser eficiente y eficazmente interpretable por una máquina” (AEPD, 2023, p. 5).

Para complementar esta diferencia cualitativa entre la biometría y la simple captura de datos a través de fotografías y grabaciones de video, es interesante notar que las Guidelines 05/2022 del EDPB sobre el uso de tecnología de reconocimiento facial, en el área, señala que la tecnología de biometría cuenta con dos particularidades. Primero, se requiere que el procesamiento de datos personales se realice de forma automatizada. Segundo, describe la biometría como una tecnología “probabilística”, es decir, que a partir del tratamiento automatizado de datos es capaz de predecir con cierto nivel de certeza la identidad de la persona analizada, sin necesidad de intervención humana (EDPB, 2022, p. 9). En definitiva, solo estaremos ante un tratamiento de datos biométricos cuando la recolección de datos sea tratada de forma automatizada y probabilística, transformando las imágenes o videos en un formato de “plantilla” solo leíble por una máquina y que permita de forma automatizada y probabilística identificar o autenticar a una persona.

Esta distinción es reconocida explícitamente por el EDPB (2022) al señalar que

algunas cámaras de vídeo pueden filmar a personas en un área definida, en particular sus rostros, pero no pueden utilizarse como tales para reconocer automáticamente a las personas. Lo mismo ocurre con la fotografía simple: una cámara no es un sistema de reconocimiento facial porque las fotografías de personas deben procesarse de una manera específica para extraer datos biométricos. (p. 10)

El EDPB reconoce el tratamiento de datos biométricos, tanto para identificación⁷ como para autenticación⁸, como un tratamiento de alto riesgo que involucra el procesamiento

⁷ La identificación es un proceso que tiene como objetivo “encontrar a una persona entre un grupo de individuos, en una zona determinada, una imagen o una base de datos. En este caso, el sistema debe procesar cada rostro capturado para generar una plantilla biométrica y, a continuación, comprobar si coincide con una persona conocida por el sistema. Esta función se basa, por tanto, en la comparación de una plantilla con una base de datos de plantillas o muestras (línea de base). Esto también se denomina identificación de uno a muchos. Por ejemplo, puede vincular un registro de nombre personal (apellido, nombre) a un rostro, si la comparación se realiza con una base de datos de fotografías asociadas a apellidos y nombres. También puede implicar seguir a una persona a través de una multitud, sin establecer necesariamente el vínculo con la identidad civil de la persona” (EDPB, 2022, p. 9).

⁸ La autenticación es un proceso que tiene como objetivo “verificar que una persona es quien dice ser. En este caso, el sistema comparará una plantilla o muestra biométrica previamente registrada (por ejemplo, almacenada en una tarjeta inteligente o pasaporte biométrico) con una sola cara, como la de una persona que se presenta en un puesto de control, para verificar si se trata de la misma persona. Por lo tanto, esta función se basa en la comparación de dos plantillas. Esto también se denomina verificación 1 a 1” (EDPB, 2022, p. 9).

de datos sensibles. Por tanto, para poder tratar dichos datos es necesario que exista una circunstancia que levante la prohibición de su tratamiento y, además, una condición que lo legitime. Es importante notar que, de acuerdo al considerando 51 del GDPR, tanto la actividad de autenticar como de identificar deben ser consideradas como tratamiento de datos de carácter biométrico.

3.2. Base de licitud para el tratamiento de datos biométricos

La base de licitud es la puerta de entrada para el tratamiento de datos personales (Contreras et al., 2024, pp. 59 y ss.). Es necesario determinar cuáles de las fuentes de licitud, contenidas en la nueva ley de datos personales, habilitarán legitimar la recolección de datos biométricos para la finalidad de control de asistencia y control horario. Al respecto, es importante tener en consideración que la nueva regulación entregó un alto nivel de resguardo a esta categoría de datos, mas no una prohibición de tratamiento (Pino, 2025, pp. 257-258). Esto se ve reflejado en el hecho de que el artículo 16 ter estableció que la regla general para el tratamiento de estos datos será el contar con el consentimiento del titular, en los términos establecidos en el artículo 12, es decir, libre, informado y específico en cuanto a su finalidad o finalidades.

En cuanto a las bases de licitud distintas al consentimiento, la nueva regulación eleva el nivel de protección establecido para el tratamiento de datos personales biométricos. Así, el tratamiento de datos biométricos no se podrá amparar en las bases de licitud contenidas en el artículo 16 (reservada para los datos sensibles en general), sino que en una categoría incluso más estricta y reservada para una subcategoría de datos sensibles: la contenida en el artículo 16 bis, que regula las bases de licitud para el tratamiento de datos de salud y el perfil biológico humano.

Al revisar el catálogo de excepciones contenidas en el artículo 16 bis es posible verificar que este es extremadamente restrictivo y que establece circunstancias excepcionales en donde un empleador podrá invocar dichas causales para legitimar el tratamiento de datos biométricos de sus trabajadores. El artículo 16 bis establece las siguientes causales:

Artículo 16 bis.- Datos personales sensibles relativos a la salud y al perfil biológico humano. [...] Solo se podrá tratar los datos personales sensibles relativos a la salud del titular y a su perfil biológico, sin contar con su consentimiento, respetando los principios y reglas establecidos en la presente ley, en los siguientes casos:

- a) Cuando éste resulte indispensable para salvaguardar la vida o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.
- b) En casos de alerta sanitaria legalmente decretada.

- c) Cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, o para el desarrollo de productos o insumos médicos que no podrían desarrollarse de otra manera. Los resultados de los estudios e investigaciones científicas que utilicen datos personales relativos a la salud o al perfil biológico, pueden ser publicados o difundidos libremente, debiendo previamente anonimizarse los datos que se publiquen.
- d) Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia o un órgano administrativo.
- e) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de sistemas y servicios de asistencia sanitaria y social.
- f) Cuando la ley así lo permita e indique expresamente la finalidad que deberá tener dicho tratamiento.

Como es posible apreciar, la gran mayoría de las empresas que busquen utilizar biometría cómo mecanismo de control de asistencia no podrán invocar alguna de estas causales de excepción al requisito de contar con el consentimiento del titular para el tratamiento de sus datos biométricos⁹. En la mayoría de los casos, la empresa deberá basarse en el consentimiento del trabajador o invocar la causal de excepción del artículo 16 bis, letra f), que señala que se podrán tratar datos biométricos sin consentimiento “cuando la ley así lo permita e indique expresamente la finalidad que deberá tener dicho tratamiento”.

Por lo tanto, la base de licitud por defecto para legitimar el tratamiento de datos biométricos de los trabajadores la mayoría de las veces será obtener su consentimiento expreso, previo, libre, informado y específico. Sin embargo, esta base de licitud tiene una serie de inconvenientes que es necesario explorar.

3.1.1. El consentimiento es esencialmente revocable

Una de las características del consentimiento como base de licitud para el tratamiento de datos personales es que este es esencialmente revocable (Politou et al., 2018, p. 5). El artículo 12 inciso tercero de la ley 21.719 así lo establece explícitamente al señalar que “[e]l titular puede revocar el consentimiento otorgado en cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento.

⁹ La interpretación administrativa bajo la ley 19.628 de 1999, ha exigido el consentimiento previo del titular. Véase el Dictamen N°2927/58 de 28.12.2021, de la Dirección del Trabajo.

La revocación del consentimiento no tendrá efectos retroactivos”¹⁰. El hecho de que los titulares o trabajadores siempre tengan la prerrogativa de retirar su consentimiento y, por tanto, poner fin a la actividad de tratamiento implica un problema práctico para la implementación y funcionamiento de un sistema de control horario y de asistencia que utilice biometría en el contexto laboral. En particular, porque implicaría que un porcentaje de los trabajadores podría revocar su consentimiento para el tratamiento de sus datos y quedar exento de este mecanismo de control.

Esta característica del consentimiento hace particularmente relevante elegir de forma precisa y rigurosa la base de licitud que se invocará para el tratamiento de datos. Así, si la base de licitud invocada es el consentimiento, no se podrá invocar de forma subsidiaria otras bases de licitud que no permitan retrotraer el consentimiento. Esto, porque implicaría darle al titular la ilusión de que sus datos están siendo tratados en base a su consentimiento, pero al momento de hacer efectiva la revocación de su consentimiento —bajo la premisa de que eso implica detener el procesamiento—, este procesamiento podría mantenerse en base a otra base de licitud alternativa o subsidiaria. Dicho esquema sería contrario al principio de lealtad, puesto que implicaría darle una impresión equivocada al titular respecto de los efectos que el retiro de su consentimiento tendría en el tratamiento de datos¹¹.

3.1.2. Libertad para otorgar el consentimiento

Uno de los requisitos para que el consentimiento sea válido como una base de licitud para el tratamiento de datos personales es que este haya sido otorgado libremente¹². En la ley 21.719, esta condición se manifiesta en la definición de consentimiento contenida en el Artículo 2 letra p), el que lo conceptualiza como una “[m]anifestación de voluntad libre, específica, inequívoca e informada”. Adicionalmente, el inciso segundo del artículo 2 señala que “[e]l consentimiento del titular debe ser libre, informado y específico en cuanto a su finalidad o finalidades”. Sin embargo, la relación laboral es, por definición, una relación sujeta a condiciones de subordinación y dependencia (Ugarte, 2005, p. 25). En este sentido, varios comentaristas y organismos internacionales han señalado la dificultad de determinar si dentro de la relación laboral los trabajadores efectivamente con la libertad real

¹⁰ Asimismo, el artículo 14 ter letra k) establece la obligación de los responsables de informar a los titulares de “la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada”.

¹¹ Un caso similar tuvo lugar en Suecia, en donde un colegio fue multado con 20.000 euros por implementar un sistema de control biométrico, sin poder demostrar que los titulares entregaron su consentimiento de forma libre y por no cumplir con el principio de minimización de datos. En dicho caso, el colegio también intentó invocar dos causales distintas (consentimiento y cumplimiento de una función de interés pública amparada por el derecho de la Unión), lo que implicaría que los titulares no podían realmente revocar su consentimiento. Sentencia de la Corte de Apelaciones de Estocolmo, dictada el 1 de marzo de 2021, KamR Stockholm - Case No. 5888-20.

¹² Ver. por ejemplo, Jurczuk y Suprunowicz, 2025, p. 181; Schermer et al., 2014, p. 4; Nettesheim, 2024, p. 2 y Tschider, 2021, p. 677. Respecto al requisito de libertad en el otorgamiento del consentimiento, el Comité Europeo de Protección ha señalado que se “deben considerarse también las situaciones concretas en las que el consentimiento se supedita a la ejecución de contratos o a la prestación de un servicio” (EDPB, 2020, p. 7).

de consentir al tratamiento de sus datos personales, análisis que siempre dependerá del contexto del tratamiento, las condiciones en que se solicita el consentimiento (de Nieves Nieto, 2020, p. 334). Es un examen que necesariamente deberá hacerse caso a caso.

Así, el considerando 43 del GDPR establece que “para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto *en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento*, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular”¹³.

Si bien la ley 21.719 no contiene el concepto de desequilibrio ostensible, el artículo 12 inciso quinto establece que “se presume que el consentimiento para tratar datos *no ha sido libremente otorgado* cuando el responsable lo recaba en el marco de la ejecución de un contrato o la prestación de un servicio en que no es necesario efectuar esa recolección”. En este sentido, los trabajadores podrían argumentar que consentir en el tratamiento de datos biométricos no es realmente necesario para ejecutar el contrato laboral, existiendo otras medidas que permitan el control horario y de asistencia, por lo que el consentimiento no ha sido realmente entregado de forma libre.

Este punto es reforzado por el EDPB en sus Directrices 5/2020 sobre el consentimiento señaló que

en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento de su empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar impresos de evaluación, sin sentirse presionado a dar su consentimiento. (EDPB, 2020, p. 9)

3.1.3. Sistema de alternativas

Lo anterior no implica que nunca podrá implementarse un sistema de registro biométrico basado en el consentimiento de los trabajadores, sino más bien que este deberá operar en circunstancias que aseguren que su consentimiento ha sido entregado de forma libre y con el menor nivel de afectación posible en su derecho a la autodeterminación informativa.

Así, la ya citada guía del EDPB concluye que

¹³ El énfasis es nuestro.

esto no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas. (EDPB, 2020, p. 9)

Del mismo modo, la Agencia Española de Protección de Datos Personales concluye, en su guía antes citada, que la única forma de podría considerarse la existencia de un consentimiento libre a un tratamiento adicional de datos, en este caso biométricos, si el interesado dispone de una alternativa de libre elección para cumplir con dicha obligación (AEPD, 2023, p. 20)¹⁴. Cuando existan opciones realmente equivalentes y disponibles para todos los trabajadores, entonces efectivamente es posible argumentar que el consentimiento ha sido entregado de forma libre.

La Dirección del Trabajo de Chile parece haber seguido esta misma lógica al publicar su resolución exenta 38 el 09 de mayo de 2024, cuyo artículo 7 letra g) obliga a los empleadores a contar con dos alternativas diferentes de reconocimiento. Asimismo, el inciso tercero del mismo artículo establece que “a lo menos una de las alternativas de reconocimiento no deberá utilizar parámetros biométricos ni datos personales de los trabajadores, por ejemplo; claves, patrones o tarjetas de aproximación” (Dirección del Trabajo, Resolución Exenta 38 del 05 de mayo de 2024, artículo 7, letra g). De esta forma, la Dirección del Trabajo parece haber seguido la tendencia internacional en la materia, asegurando que los trabajadores puedan consentir de forma libre al establecer un sistema de alternativas en donde, al menos una de ellas, no debe contemplar el tratamiento de datos personales.

En definitiva, el carácter restrictivo de las bases de licitud contenidas en el artículo 16 ter indica que el consentimiento se presenta como la principal base legal del tratamiento para otorgar legitimidad a la actividad de control de asistencia y horaria con tecnología de biometría. Sin embargo, para poder garantizar que dicho consentimiento sea otorgado de forma libre en el contexto de una relación laboral, será necesario otorgar un mecanismo alternativo de autenticación a los trabajadores que no involucre el tratamiento de sus datos biométricos. Esto puede tomar la forma de una tarjeta de identificación, la revisión de la cédula de identidad por el encargado de seguridad al interior de la faena u otro mecanismo equivalente.

¹⁴ En el mismo sentido el EDPB ha argumentado que “[e]l responsable del tratamiento podría argumentar que su organización ofrece a los interesados una elección real si estos pudieran escoger entre un servicio que incluya el consentimiento para el uso de datos personales con fines adicionales, y un servicio equivalente ofrecido por el mismo responsable que no implicara prestar el consentimiento para el uso de datos con fines adicionales. Siempre que exista una posibilidad de que dicho responsable del tratamiento ejecute el contrato o preste los servicios contratados sin el consentimiento para el otro uso o el uso adicional de los datos en cuestión, significará que ya no hay condicionalidad con respecto al servicio. No obstante, ambos servicios deben ser realmente equivalentes” (EDPB, 2020, p. 11).

3.3. Requisitos legales adicionales

Por último, y por tratarse los datos biométricos de información especialmente sensible y protegida, la nueva regulación establece una serie de requisitos adicionales que deben cumplirse para su recolección y tratamiento (Contreras et al., 2024, pp. 37-38).

Así, el artículo 16 ter establece que, independiente de la base legal de tratamiento que se invoque, para tratar los datos biométricos, el titular deberá ser informado de los siguientes aspectos:

- a) La identificación del sistema biométrico usado.
- b) La finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados.
- c) El período durante el cual los datos biométricos serán utilizados.
- d) La forma en que el titular puede ejercer sus derechos.

Para cumplir con estos requisitos adicionales de información se sugiere que los trabajadores que ya cuenten con un contrato laboral vigente firmen un anexo de contrato en donde declaren haber sido informados de todos estos antecedentes, así como incorporar dicha información de forma desagregada en el Reglamento Interno de Orden, Higiene y Seguridad.

El tratamiento deberá cumplir con los distintos principios establecidos en el artículo 3 de la nueva ley de protección de datos personales. En particular, la recolección y procesamiento de datos biométricos deberá cumplir con el principio de proporcionalidad. Para ello el responsable deberá demostrar que no se están recolectando datos excesivos o innecesarios para la finalidad declarada, realizando para ello un análisis de idoneidad, necesidad y proporcionalidad de la medida, en un sentido muy similar al test de proporcionalidad estricta elaborado por el Tribunal Constitucional chileno¹⁵. El principio de proporcionalidad también exige que la información biométrica sea eliminada o anonimizada una vez que deje de cumplir el objetivo por la cual fue recolectada¹⁶.

Por último, será necesario realizar una evaluación de impacto en protección de datos personales, en los términos establecidos en el artículo 15 ter, letra c). Dicha norma establece que se deberá realizar esta evaluación cuando el “tratamiento que implique observación o monitoreo sistemático de una zona de acceso público”.

¹⁵ Esto implica limitar el uso de control biométrico a “casos de clara necesidad, es decir, cuando la ganancia en seguridad supera claramente una posible interferencia con los derechos humanos y si el uso de otras técnicas menos intrusivas no es suficiente” (Gayrel, 2016, pp. 450). Del mismo modo, en un reciente pronunciamiento la AEPD (2025) estableció como criterio que la proporcionalidad “exige que, en caso de existir varias medidas igualmente adecuadas, en el ámbito de conocimiento y decisión del responsable del tratamiento, se opte por la menos gravosa”.

¹⁶ Así, por ejemplo, la Dirección del Trabajo en su Dictamen N°2927/58 de 28.12.2021 estableció que la información biométrica recolectada con ocasión del control de asistencia de una empresa debe ser eliminada en un plazo de 120 días luego de terminada la relación contractual entre el trabajador y el empleador.

4. Tratamiento de datos para efectos de videovigilancia

4.1. Los datos tratados en materia de videovigilancia

Tal como revisamos en la sección 2, la videovigilancia es una materia de control y disciplina laboral que ya ha ocupado a la doctrina nacional. Sin embargo, el énfasis estaba radicado en la determinación de la afectación de la intimidad o el respeto y protección de la vida privada de los trabajadores. Tras la aprobación de la reforma constitucional que consagró el derecho fundamental a la protección de datos personales, en 2018, este enfoque no ha variado considerablemente. En este apartado nos enfocaremos en la videovigilancia como una *actividad de tratamiento de datos personales*, con el consiguiente análisis de riesgos regulatorios para las organizaciones.

La utilización de cámaras de videovigilancia para la obtención de imágenes o videos implica el tratamiento de datos personales. A menos que el funcionamiento de estas cámaras cumpla con ciertos estándares técnicos específicos, no necesariamente implica la recolección y tratamiento de datos biométricos.

A pesar de que la recolección realizada por estos sistemas de vigilancia solo involucre el tratamiento de datos personales —y no necesariamente datos sensibles—, de todas maneras, este tratamiento deberá cumplir con todos los resguardos y requisitos establecidos en la nueva regulación de protección de datos personales.

La calificación de una imagen o videograbación como dato personal sensible dependerá del caso concreto y del contexto del tratamiento de datos personales. De esta forma, esta imagen o videograbación podrán ser considerados como datos sensibles en la medida que revele alguna de las características protegidas establecidas de forma taxativa¹⁷ en el Artículo 2 letra g)¹⁸, a saber:

el origen étnico o racial, la afiliación política, sindical o gremial, 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.

Las organizaciones pueden externalizar los servicios de videovigilancia y, además, establecer exigencias de comunicación con empresas de seguridad privada¹⁹. Por lo mismo, los procedimientos de seguridad y vigilancia deben identificar a los responsables y encargados del tratamiento de datos, todos los recintos que cuentan con circuitos cerrados de televisión (CCTV) y el tipo de personal a cargo de la seguridad por esta vía.

¹⁷ La historia de la ley muestra que durante la tramitación legislativa la definición de dato personal sensible cambió de una definición amplia, similar a la contenida en la Ley N° 19.628 del año 1.999 al listado taxativo contenido en la versión final de la Ley N° 21.719 (Biblioteca del Congreso Nacional, 2024, pp. 1530-1532 9.

¹⁸ Una interpretación similar puede encontrarse en el Considerando 51 del GDPR. Ver nota 7.

¹⁹ Véase, con referencias, Debasa, 2021.

4.2. Base de licitud para el tratamiento de datos de videovigilancia

Puesto que la captación de imágenes de los trabajadores constituye información que los puede identificar, entonces necesariamente implica la recolección de datos personales. Por lo mismo, su tratamiento siempre deberá estar amparada en alguna de las bases de licitud contenidas en el artículo 12 o 13 de la nueva regulación.

La utilización del consentimiento como base de licitud para el tratamiento de datos obtenidos a través de cámaras de vigilancia es desaconsejado por las razones ya expuestas anteriormente: el titular o trabajador siempre tendrá la capacidad de retractar su consentimiento y, además, resulta muy difícil demostrar que el consentimiento ha sido entregado de forma libre al interior de una relación laboral de subordinación y dependencia. Además, no siempre será factible requerir el consentimiento de terceros que no tienen un vínculo laboral con la empresa.

Por tanto, será necesario acudir a alguna de las bases de licitud consistentes en excepciones al requisito del consentimiento contenidas en el artículo 13. Sin embargo, la elección de la base de licitud dependerá de la finalidad con la cual el sistema de vigilancia ha sido implementado.

4.3. Sistemas de videovigilancia con fines de prevención de delitos

En aquellos casos en donde el sistema de vigilancia tenga como finalidad específica el garantizar la seguridad de personas, bienes e instalaciones, entonces la existencia de un interés legítimo de la compañía como responsable de datos puede ser invocado.

El artículo 13 letra d) señala que no será necesario contar con el consentimiento del titular cuando

el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular. En todo caso, el titular podrá exigir siempre ser informado sobre el tratamiento que lo afecta y cuál es el interés legítimo en base al cual se efectúa dicho tratamiento.

En este caso, el interés legítimo de la empresa que legitimaría el tratamiento de datos personales de los trabajadores y de terceros sin contar con su consentimiento sería el garantizar la seguridad de personas, bienes e instalaciones (Goñi Stein, 2021, p. 4137).

Ahora bien, para poder invocar el interés legítimo se debe realizar una evaluación basada en el “triple test” (Contreras Vásquez y Trigo Kramcsák, 2019), consistente en el cumplimiento de tres condiciones copulativas (EDPB, 2024).

- a) El responsable debe realizar el tratamiento persiguiendo la satisfacción de un interés legítimo, ya sea suyo o de un tercero.
- b) Debe existir una necesidad de procesar datos personales para los fines del interés legítimo perseguido, y

- c) Los intereses o las libertades y derechos fundamentales de los titulares no deben prevalecer sobre el interés legítimo del responsable del tratamiento o de un tercero. Adicionalmente, el Artículo 13 letra d) establece como condición que “que con ello no se afecten los derechos y libertades del titular”.

En otras palabras, se debe realizar un ejercicio de ponderación entre la afectación que la actividad de tratamiento puede significar para el titular y el bien perseguido por el responsable en la persecución de este interés legítimo. De esta forma, el derecho a la protección de datos personales debe ser ponderado con otros intereses, derechos y valores reconocidos jurídicamente, así como también con los medios e instrumentos empleados (Contreras Vásquez y Trigo Kramcsák, 2019, pp. 69-106). Es importante notar que la misma Agencia Española de Protección de Datos Personales establece que el interés legítimo es una base de licitud que puede justificar la videovigilancia para efectos de garantizar la seguridad de personas, bienes e instalaciones (AEPD, 2018, p. 12). En la misma línea la EDPB ha señalado que “en una situación real de peligro, la finalidad de proteger la propiedad frente a robos, hurtos o vandalismo puede constituir un interés legítimo para la videovigilancia” (EDPB, 2020, p. 11). Del mismo modo, esta base de licitud es adecuada, puesto que la finalidad de resguardo de la seguridad justamente busca legitimar la recolección de imágenes de los trabajadores, pero también de externos que puedan ingresar a las faenas de la compañía a realizar ilícitos.

Por último, en aquellos casos en que la empresa esté obligada legalmente a implementar medidas de seguridad, ya sea por una norma o por el regulador sectorial, entonces no será necesario invocar un interés legítimo y bastará la causal contenida en el artículo 13 letra a): “cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley”.

4.4. Sistemas de videovigilancia con fines de control laboral

En el caso de las cámaras de vigilancia implementadas para el control de las actividades laborales de los trabajadores²⁰, la base de licitud que debe ser invocada corresponde a la contenida en el artículo 13, letra c), el que establece que no será necesario el consentimiento del titular o trabajador cuando “el tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular”.

En este caso, esta causal de tratamiento debe ser invocada con la finalidad específica de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, que deberán guardar la consideración debida a la dignidad humana.

²⁰ Bajo la actual legislación de protección de datos, la Dirección del Trabajo reconoce que el poder de dirección permite al empleador adoptar una serie de medidas organizativas y productivas. Véase Dictamen N°2852/158 de 30.08.2002, de la Dirección del Trabajo. Para los problemas sobre el tipo de tratamiento de datos y los alcances respecto del consentimiento del trabajador, véase Neira (2022), pp. 26-28. Sobre el poder de dirección del empleador, véase Fernández Toledo (2019).

4.5. Medidas adicionales y buenas prácticas

Junto con contar con una base de licitud que legitime la recolección de datos a través de cámaras de video vigilancia, la legislación establece el deber de cumplir con otros requisitos:

- a) El responsable tendrá un deber de reserva respecto a las imágenes captadas y no podrá divulgarlas sin una causal que habilite dicha comunicación (Artículo 3 letra h).
- b) El responsable deberá responder a las solicitudes de acceso, rectificación, cancelación y oposición que los titulares realicen (Artículo 11).
- c) Deberá implementar medidas técnicas y organizativas para garantizar la seguridad de la información recolectada (Artículo 14 quinquies).
- d) Se deberá establecer un período de almacenamiento y posterior supresión que resulte proporcional al fin buscado (Artículo 3 c) inciso segundo).
- e) Se deberá cumplir con las distintas medidas de transparencia y entrega de información a los titulares. En el caso de que el tratamiento esté basado en el interés legítimo, los titulares tendrán derecho a que se le informe cuál es dicho interés público que fundamenta el tratamiento (Artículo 14 ter).
- f) Tanto para la videovigilancia para fines de seguridad como control laboral será necesario realizar una evaluación de impacto en materia de protección de datos personales cuando dicho tratamiento implique observación o monitoreo sistemático de una zona de acceso público (Artículo 15 ter letra c).

Adicionalmente, existen buenas prácticas en la utilización de tecnología de videovigilancia que se recomienda poner en práctica, tales como (AEPD, 2024):

- a) Instalar carteles claramente visibles en los puntos de acceso a las áreas vigiladas, que informen de manera explícita la identidad del responsable de la instalación, los datos de contacto para ejercer los derechos contemplados en la normativa de protección de datos y el lugar donde puede obtenerse información adicional sobre el tratamiento de los datos personales.
- b) Se sugiere que los trabajadores que ya cuenten con un contrato laboral vigente firmen un anexo de contrato en donde declaren haber sido informados de todos estos antecedentes, así como incorporar dicha información de forma desagregada en el Reglamento Interno de Orden, Higiene y Seguridad.
- c) Las cámaras de vigilancia deben limitarse a capturar imágenes exclusivamente de las áreas necesarias para el control laboral y ojalá a través de ángulos panorámicos. En ningún caso podrán instalarse en vestuarios, baños o espacios destinados al descanso de los trabajadores.
- d) En caso de utilizar cámaras con capacidad de orientación y/o *zoom*, será obligatorio implementar máscaras de privacidad que impidan la captación de imágenes de

la vía pública, terrenos, viviendas o cualquier otro espacio que no corresponda al ámbito objeto de vigilancia.

- e) No se deben capturar conversaciones de carácter privado.
- f) El sistema de grabación deberá ubicarse en un lugar protegido, vigilado o con acceso restringido.
- g) El acceso a las imágenes grabadas estará limitado exclusivamente al personal autorizado.
- h) Si el sistema permite el acceso remoto a través de Internet, este deberá estar protegido mediante un código de usuario y contraseña (u otro mecanismo que garantice la identificación y autenticación única), conocidos únicamente por las personas autorizadas.
- i) En caso de que las imágenes sean necesarias para denunciar delitos o infracciones, estas deberán acompañar la denuncia y conservarse para su entrega a Carabineros o a los Tribunales competentes, estando prohibido utilizarlas para otros fines.
- j) Las solicitudes de acceso a las imágenes por parte de Tribunales o Fuerzas de Seguridad deberán realizarse en el marco de actuaciones judiciales o policiales.

Para ello, se aconseja que estas medidas se incorporen en el Reglamento Interno de Orden, Higiene y Seguridad, el cual debería regular el funcionamiento de cámaras de vigilancia (CCTV) por motivos técnicos productivos y/o de seguridad de la empresa y de sus colaboradores.

5. Tratamiento de datos de geolocalización para el control de jornada de trabajo

Uno de los mecanismos de control que han empezado a masificarse son aquellos que emplean datos georreferenciados de los trabajadores en base a un dispositivo móvil o fijo, por ejemplo, para el control de asistencia o de cumplimiento de la jornada de trabajo (Baranski y Mirosławski, 2023, p. 3). Estos mecanismos, en ocasiones, suponen un software que puede ser instalado en un dispositivo personal del trabajador o de propiedad de la empresa²¹. Este tipo de software suele requerir un consentimiento para su uso; particularmente se exige para su funcionamiento que los trabajadores entreguen acceso al sistema de geolocalización de GPS de sus dispositivos como condición para

²¹ De acuerdo a la Organización Internacional del Trabajo (OIT) el control de geolocalización constituye monitoreo en el contexto laboral, el que “Incluye, pero no se limita a, el uso de dispositivos tales como computadoras, equipos de video, dispositivos de sonido, teléfonos y otros equipos de comunicación, varios métodos para establecer identidad y ubicación, o cualquier otro método de vigilancia”. (OIT, 1997, p. 1).

que este opere. Este dato de geolocalización es utilizado para vincular la ubicación del trabajador con el horario en que este marca asistencia.

La ley 21.719 no define qué se entiende por un dato personal que refiera a la geolocalización de un titular. El artículo 16 sexies es la única norma que se aboca específicamente al tratamiento de datos de geolocalización, limitándose exclusivamente a establecer las bases de licitud para el tratamiento de dichos datos, así como los deberes específicos de información que debe ser entregada a los titulares.

Sin embargo, para discernir las obligaciones legales que deben cumplirse para tratar datos personales de localización existe una serie de puntos jurídicos que deben ser examinados.

5.1. Naturaleza del dato de geolocalización

La geolocalización de una persona natural siempre debe ser considerada como un dato personal, a pesar de no encontrarse explícitamente mencionada en la definición contenida en el artículo 2 letra f) de la nueva ley de datos personales, puesto que cumple con los supuestos jurídicos de dicha definición, al tratarse de información referida a una persona natural identificada e identificable²².

Adicionalmente, la geolocalización del titular no solo debe ser considerada como un dato personal, sino como una categoría especial de dato personal. El hecho de que se trata de una categoría especial de datos personales tiene como fundamento dos elementos. Primero, el hecho de que el artículo 16 sexies se encuentra ubicado en el Párrafo Tercera de la nueva ley, titulado “Del tratamiento de categorías especiales de datos personales”. Y segundo, dicho artículo agrega condiciones especiales que el responsable de datos debe cumplir para poder tratar o procesar el dato de geolocalización de un titular. Del mismo modo, se trata de un dato personal, pero no de un dato personal sensible²³.

Se debe distinguir entre categorías especiales de datos y datos personales sensibles. Puesto que el Párrafo Tercero contiene la regulación de los datos de niños, niñas y adolescentes (artículo 16 quáter) se suele confundir el concepto de categoría especial de datos con los datos sensibles. Sin embargo, son categorías distintas. Los datos personales sensibles hacen referencia a todos los datos que cumplen con la definición

²² En contraposición, el artículo 4 del Reglamento general de protección de datos personales de la Unión Europea (GDPR), menciona específicamente los datos de ubicación en su definición de datos personales, señalar que se trata de “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, *datos de localización*, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”. El énfasis es nuestro.

²³ Esta conclusión se basa en que los datos de geolocalización se regulan en el artículo 16 sexies, el que se encuentra en el Párrafo tercero del Título II, titulado “Del tratamiento de categorías especiales de datos personales” y no en el Párrafo segundo, titulado “Del tratamiento de los datos personales sensibles”. En esto la ley 21.719 se aparta del GDPR, el que utiliza el término categoría especial de dato como sinónimo de dato sensible, como lo muestra el contenido del considerando 10 y el artículo 9 de dicho cuerpo legal.

contenida en el artículo 2 letra g), así como los datos personales relativos a la salud del titular, incluyendo su perfil biológico (artículo 16 bis) y los datos biométricos (artículo 16 ter). En todos estos casos, se trata de información que, por su naturaleza, es particularmente susceptible de provocar daños en el titular si es tratada de forma indebida, por lo que se establecen medidas adicionales de resguardo, en particular, limitando las bases de licitud que pueden ser invocadas para su tratamiento.

En contraposición, las categorías especiales de datos no necesariamente versan sobre datos sensibles, sino que sobre datos que tienen reglas específicas para su tratamiento. Así, en esta categoría encontramos datos que tienen reglas para elevar el nivel de protección en su tratamiento (datos de niñas, niñas y adolescentes) pero también datos cuyas reglas buscan facilitar su tratamiento, como lo es la presunción de interés legítimo establecida en favor del tratamiento de datos con fines históricos, estadísticos, científicos y de estudios o investigaciones (artículo 16 quinquies).

En definitiva, el dato de geolocalización es un dato personal que pertenece a una categoría especial de datos, con reglas que establecen requisitos específicos para su tratamiento para proteger a los titulares, pero sin que sea un dato personal sensible. Es por ello que artículo 16 sexies establece que los datos de geolocalización pueden ser tratados bajo las mismas fuentes de licitud establecidas en los artículos 12 y 13 (es decir, las mismas bases de licitud que para los datos personales) y no exige que sean invocadas las bases de licitud más restrictivas reservadas para los datos personales sensibles, que están contenidas en el artículo 16.

Estas reglas especiales tienen su justificación en el potencial que tienen los datos de geolocalización para extraer o derivar otro tipo de informaciones, “no estrictamente locativas, y que abarquen aspectos especialmente protegidos de la intimidad o que puedan proporcionar información que permita posteriores actos contrarios a los derechos fundamentales o libertades públicas del interesado” (Calvo Gallego, 2021, pp. 4166-4167). La derivación de patrones o hábitos, junto con la posibilidad de perfilar a personas, intensifica el tipo de control que la información georreferenciada presta a un responsable del tratamiento de datos.

Respecto a la utilización de la geolocalización como mecanismo de control, la Dirección del Trabajo —en un dictamen del año 2022— llegó a la conclusión de que

no existe inconveniente jurídico para utilizar la geolocalización como parte de una medida de control, en la medida que aquella no vulnere los derechos fundamentales de los trabajadores, ni se transforme en un verdadero mecanismo de vigilancia de cada uno de ellos, en virtud del tipo de funciones desarrollados. (Dirección del Trabajo, 2022, p. 6)

En el caso específico analizado en dicho dictamen, los trabajadores debían enviar su georreferencia al momento de visitar a un cliente en terreno.

5.2. Distinción entre geolocalización y ubicación

A fin de evitar una interpretación excesivamente expansiva de qué información debe ser considerada como geolocalización, es necesario distinguir entre el dato referente a la ubicación y el dato de geolocalización del titular. En el caso de la ubicación, no es exigido cumplir las reglas especiales y requisitos adicionales contenidos en el artículo 16 sexies.

La ubicación es un dato que será de carácter personal en la medida que pueda ser vinculada con un titular en específico, como un trabajador individualizado. Se trata de un dato que da cuenta del lugar en donde se encuentra un trabajador en un momento específico. Así, por ejemplo, si al momento de entrar a las instalaciones de la empresa el trabajador registra su ingreso, este registro permitiría inferir el lugar y hora donde se encontraba dicho trabajador en el momento específico del registro de asistencia, mas no su geolocalización²⁴.

La ubicación no necesariamente detalla su geolocalización, puesto que esta última corresponde a un concepto de carácter técnico que requiere la utilización de procesos tecnológicos en el procesamiento de dicha información.

A falta de una definición chilena del concepto de geolocalización, podemos recurrir al artículo 2 de la Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE. Dicho instrumento los define como “cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público” (Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE, artículo 2). Del mismo modo, el considerando 14 de la misma directiva establece que esta categoría especial de dato puede referirse a

la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada. (Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE, artículo 2)

De esta forma, es posible concluir que la mera inferencia de la ubicación de un trabajador en un momento determinado no implica necesariamente un dato de geolocalización, sino que este requiere un registro de las coordenadas u otro mecanismo técnico de seguimiento preciso del equipo terminal utilizado por el trabajador. La regla general para determinar la geolocalización es la utilización de coordenadas. Sin embargo, también podría tomar

²⁴ Es posible pensar en otro escenario hipotético: si una boleta impresa registra la hora en que un consumidor compra un bien junto con la dirección de la tienda, entonces será posible inferir la ubicación del consumidor a una hora y fecha específica. Sin embargo, esto no implica que la boleta impresa registró la geolocalización de dicho consumidor.

forma de vectores, rásters, puntos multitemporales, direcciones hasta triangulación basada en señales de radio o localización de direcciones IP. En este sentido, la utilización de equipos GPS para rastrear la ubicación en tiempo real de los dispositivos personales de los trabajadores o dispositivos de rastreo ubicados en vehículos de la empresa debe considerarse como un dato de geolocalización, mientras que el registro de encontrarse un trabajador en cierto lugar en cierto momento del día, sin seguimiento en tiempo real de dicha ubicación constituiría un mero dato personal de ubicación del trabajador, pero no un dato de geolocalización.

5.3. Base de licitud para el tratamiento de datos de geolocalización

El principio de licitud establece que todo tratamiento de datos personales debe estar amparado por una base de licitud, al mismo tiempo, el artículo 16 sexies establece que los datos de geolocalización pueden ser tratados bajo las mismas fuentes de licitud establecidas en los artículos 12 y 13. Por tanto, la empresa deberá optar por una base de licitud que legitime el tratamiento de este tipo de datos para realizar control de asistencia y cumplimiento de la jornada laboral en base a geolocalización.

Una opción es optar por el consentimiento de los trabajadores como base de licitud para el tratamiento de sus datos de geolocalización, en los términos establecidos en el artículo 12 de la ley reformada. Sin embargo, esta alternativa es desaconsejable puesto que el consentimiento es inherentemente revocable, lo que implicaría que un trabajador podría optar por retirar su autorización para tratar sus datos de geolocalización, los que deberán dejar de ser procesados e incluso podrían ser objeto de una solicitud de supresión.

El artículo 13, por su lado, establece aquellas bases de licitud que pueden ser invocadas sin requerir el consentimiento del titular. De estas bases de licitud, la que se ajustará de forma más común al tratamiento de datos personales que una empresa realice de los datos de geolocalización de sus trabajadores es la contenida en el artículo 13 letra c). Dicho artículo establece que no será necesario el consentimiento del titular cuando el “tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular”.

En la medida que el control de asistencia y cumplimiento de la jornada laboral es una actividad necesaria para que el empleador verifique que el trabajador está cumpliendo su obligación contractual de asistir a su lugar de trabajo, el tratamiento del dato de geolocalización se vuelve necesario para el cumplimiento de la ejecución del contrato laboral entre el trabajador y el empleador. Esto es especialmente relevante en aquellos casos en donde el trabajador no cumple su jornada laboral en una oficina permanente, sino que en faenas u obras que pueden estar sujetas a cambios en su ubicación.

Sin embargo, cómo ha advertido el Grupo de Trabajo del Artículo 29 de la Unión Europea, esta base de licitud puede dejar de ser efectiva si la recolección de esta información es utilizada para finalidades distintas a las realmente necesarias para la ejecución del contrato,

como, por ejemplo, la evaluación del desempeño laboral del trabajador (Article 29 Data Protection Working Party, 2017).

Del mismo modo, el interés legítimo (artículo 13, letra d) también puede ser invocado como base de licitud para el tratamiento de datos de geolocalización. Sin embargo, su efectividad deberá ser analizada caso a caso. Asimismo, el responsable debe demostrar que para cada actividad de tratamiento los medios utilizados cumplen con el requisito de ser necesarios, proporcionados e implementados de la manera menos intrusiva posible. El empleador deberá probar que se han implementado medidas apropiadas para garantizar un equilibrio con los derechos y libertades fundamentales de los empleados (Article 29 Data Protection Working Party, 2017, Sección 3.1.1).

En aquellos casos en que la geolocalización de los trabajadores o vehículos no es recolectada para efectos de control de asistencia, sino que, para efectos del resguardo de la seguridad de determinados recintos o la prevención de delitos, se deberá realizar una evaluación caso a caso de la base de licitud que se debe invocar. Si el resguardo del vehículo o instalación se realiza en el cumplimiento de una obligación legal o reglamentaria, entonces se podrá invocar la causal contenida en el artículo 13 letra b). De lo contrario, será posible invocar la existencia de un interés legítimo del empleador para realizar este seguimiento, sin embargo, será necesario demostrar el cumplimiento de los requisitos señalados en el párrafo anterior.

5.4. Riesgos de perfilamiento

Determinados tratamientos de carácter automatizado de información relativos a la ubicación o movimientos de una persona natural pueden constituir perfilamiento de un titular de datos personales, acarreando una serie de consecuencias jurídicas potencialmente indeseables.

El artículo 2, letra w) define perfilamiento como “toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural”.

De dicha definición se puede colegir que el tratamiento de datos solo constituirá perfilamiento en la medida que se utilicen para i) evaluar, ii) analizar o iii) predecir la ubicación o movimientos del titular.

Si el tratamiento de datos es catalogado como una forma de perfilamiento, este produciría las siguientes consecuencias jurídicas:

- a) De acuerdo el artículo 8 bis este solo se podría realizar en la medida que sea necesaria para la celebración o ejecución de un contrato, cuando exista consentimiento previo y expreso del titular y cuando lo disponga la ley, excluyendo toda otra base de licitud.

- b) El titular tendrá derecho a obtener una explicación, la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión.
- c) Se vuelve obligatorio realizar una evaluación de impacto en protección de datos personales, de acuerdo a lo establecido en el artículo 15 ter letra a).

Producto de lo anterior, es recomendable realizar una recolección y tratamiento de datos de geolocalización de forma tal que no pueda ser catalogado como perfilamiento del titular o trabajador. De esta forma, la recolección de información de geolocalización de los trabajadores con la finalidad específica de control de asistencia no constituirá perfilamiento en la medida que se utilice exclusivamente para fiscalizar la ubicación del trabajador al entrar y salir de su jornada laboral. En este sentido, la Resolución Exenta 38 de la Dirección del Trabajo antes citada establece en su artículo 53 letra e) que “[d]ada la finalidad de los sistemas, es decir, controlar asistencia y horas de trabajo, no se ajusta a Derecho exigir que se encuentre encendida durante toda la jornada”. El mismo artículo establece que mantener una geolocalización permanente del trabajador solo será posible en las siguientes circunstancias excepcionales: i) Cuando la geolocalización forme parte de una maquinaria o medio de transporte y se justifique por la seguridad de las personas, por ejemplo, en las naves o aeronaves, o por razones de seguridad de los trabajadores, como ocurriría con los vehículos de transporte de valores. ii) Cuando una norma legal así lo establezca.

5.5. Requisitos legales adicionales

Por último, y como hemos señalado precedentemente, el dato de geolocalización no es un dato de carácter sensible, pero sí un dato que es especialmente resguardado por la nueva ley de datos personales. En este sentido, se deben cumplir con todos los requisitos y garantías que se deben cumplir para el tratamiento de un dato personal, pero además de las obligaciones especiales para el tratamiento de datos de geolocalización contenidas en el artículo 16 sexies.

De esta forma, el tratamiento de datos de geolocalización podrá realizarse invocando alguna de las bases de licitud ya mencionadas, pero el empleador tendrá la obligación adicional de entregar la siguiente información al trabajador: i) El tipo de datos de geolocalización que serán tratados, ii) La finalidad y duración del tratamiento y iii) Si los datos se comunicarán o cederán a un tercero para la prestación de un servicio con valor añadido. De acuerdo a lo establecido en el artículo 16 sexies inciso segundo, esta información debe ser entregada a los trabajadores de manera clara, suficiente y oportuna. Para ello, será recomendable que el empleador suscriba anexos de contrato en donde los trabajadores declaren haber sido informados de todos estos antecedentes, así como incorporar dicha información de forma desagregada en el Reglamento Interno de Orden Higiene y Seguridad.

6. Conclusiones

A lo largo de las distintas secciones hemos intentado evidenciar la alta complejidad que el tratamiento de datos personales en el ámbito laboral presenta para las empresas en Chile. La reforma introducida por la ley 21.719 redefine el marco de actuación de los empleadores, elevando los estándares de licitud, lealtad, finalidad y transparencia, y otorgando mayor densidad normativa al derecho a la autodeterminación informativa. En este nuevo escenario, el cumplimiento normativo no puede abordarse como una mera cuestión formal o documental, sino como un proceso continuo de gestión de riesgos jurídicos, técnicos y reputacionales.

En el caso de los datos biométricos, la exigencia de contar, por regla general, con el consentimiento previo, libre, informado y específico del trabajador, junto con la obligación de ofrecer mecanismos alternativos de control, obliga a replantear sistemas ya instalados en muchas organizaciones. Las dificultades inherentes a la revocabilidad del consentimiento y a la ausencia de plena libertad, en la relación laboral, demandan soluciones creativas que combinen medidas técnicas y organizativas para garantizar la validez de la base legal invocada.

En materia de videovigilancia, el reto central radica en justificar jurídicamente el tratamiento bajo bases de licitud distintas al consentimiento, ponderando adecuadamente intereses legítimos o el cumplimiento de obligaciones contractuales o legales. A ello se suman exigencias de transparencia, limitación temporal en la conservación de imágenes y medidas estrictas de seguridad. La instalación de cámaras, su ubicación y sus capacidades técnicas deben diseñarse bajo un principio de mínima intrusión, evitando áreas de privacidad reforzada y asegurando que la vigilancia no se convierta en un mecanismo de control abusivo. Tanto en materia de control biométrico de acceso y asistencia, así como videovigilancia será necesario que la empresa realice una evaluación de impacto en protección de datos personales, en la medida que dicho tratamiento implique la observación o monitoreo sistemático de una zona de acceso público.

Respecto de la geolocalización, la principal dificultad estriba en diferenciarla de la mera ubicación y en aplicar correctamente las reglas especiales del artículo 16 sexies. La utilización de tecnologías de seguimiento continuo de trabajadores plantea un riesgo elevado de vigilancia excesiva y eventual perfilamiento, que solo puede mitigarse a través de una definición precisa de finalidades, límites temporales estrictos y opciones de desactivación fuera de la jornada y faena laboral.

En términos generales, las empresas deberán considerar los siguientes desafíos de *compliance* regulatorio. Primero, la determinación precisa y correcta de la base de licitud para el tratamiento de datos, caso a caso, y previa documentación. En segundo lugar, es necesario considerar las evaluaciones de impacto, para identificar tempranamente los tratamientos de alto riesgo y adoptar medidas de mitigación. En tercer término, es necesario que las obligaciones de información del responsable del tratamiento se traduzcan en avisos claros, comprensibles y específicos, evitando fórmulas genéricas

que diluyen la comprensión del trabajador. Solo así el empleador podrá asegurarse que el tratamiento de datos personales de sus trabajadores se realice de forma lícita, evitando la incurrencia en infracciones que puedan implicar la imposición de las multas contenida en la nueva legislación de datos personales o la infracción del derecho fundamental a la autodeterminación informativa de los trabajadores, perseguida a través del proceso de tutela laboral.

Acerca del artículo

Notas de conflicto de interés. Los autores declaran no tener ningún conflicto de interés en relación con la publicación de este artículo.

Contribución en el trabajo. Ambos autores contribuyeron en los roles de Writing (original draft) y review&editing.

Financiación. Este trabajo es parte de la investigación financiada por Fondecyt Regular No 1230895, de la cual el autor Pablo Contreras es investigador principal y Pablo Viollier co-investigador; y del proyecto “Claves para una justicia digital y algorítmica con perspectiva de género” (expediente: PID2021-123170OB-I00), financiado por el Ministerio de Ciencia e Innovación de España).

Bibliografía

- AEPD. (2023). *Guía sobre tratamientos de controles de presencia mediante sistemas biométricos*. <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>
- AEPD. (2025). Respuesta a consulta pública (Art. 36 RPDG) Ref. REGAGE25e00024730156, p. 10. <https://www.aepd.es/documento/regage25e00024730156.pdf>
- Article 29 Data Protection Working Party. (2017). WP29 opinion on data processing at work. Opinion 2/2017 WP249, sección 5.5. https://ec.europa.eu/newsroom/document.cfm?doc_id=45631
- Asenjo Cruz, A., Coddou Mc Manus, A. y Dhir, R. K. (2023). *The platform economy and transformations in the world of work: The case of delivery platform workers in Santiago, Chile*. ILO Working Paper, No. 100. International Labour Organization (ILO). <https://doi.org/10.54394/JCVG2192>.
- Baranski, M. y Mirosławski, T. (2023). Geolocation Monitoring of an Employee from the Perspective of Article 8 of the ECHR. *Acta Universitatis Sapientiae Legal Studies* (12), 1-17. <https://doi.org/10.47745/AUSLEG.2023.12.2.01>
- Becker Castellaro, S. y Garrido Iglesias, R. (2017). La biometría en Chile y sus riesgos. *Revista Chilena de Derecho y Tecnología*, 6(1). <https://doi.org/10.5354/0719-2584.2017.45825>.
- Biblioteca del Congreso Nacional. (2024). *Historia de la Ley N° 21.719*. <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8352>

- Bordachar, B. M. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales: deficiencias e inconsistencias en los derechos ARCO. *Revista Chilena de Derecho y Tecnología*, 11(1), 395-412. <https://doi.org/10.5354/0719-2584.2022.67205>
- Calvo Gallego, F. J. (2021). Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (Comentario al artículo 90 LOPDGDD). En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 4166-4167). Thomson-Civitas.
- Cárdenas Oyarzún, H. y Uribe Conejeros, M. (2025). La protección de datos personales tras la Ley 21.719: Implicancias para las empresas en las relaciones laborales. *Revista de Derecho Aplicado LLM UC* (15). <https://doi.org/10.7764/rda.15.91346>
- Castro, J. F. (2020). *La protección de la intimidad del trabajador*. Der Ediciones.
- CE. Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE.
- Coddou, A. (2022). Discriminación algorítmica en las plataformas digitales de trabajo. En R. Palomo Vélez (Ed.), *El trabajo a través de plataformas digitales. Problemas y desafíos en Chile*. Tirant lo Blanch.
- Coddou Mc Manus, A. y Padilla Parga, R. (2024). Discriminación algorítmica en los procesos automatizados de reclutamiento y selección de personal. *Revista Chilena de Derecho y Tecnología* (13), 1-34. <https://doi.org/10.5354/0719-2584.2024.71312>.
- Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios Constitucionales* 18(2). <http://dx.doi.org/10.4067/S0718-52002020000200087>
- Contreras, P. (2022). La protección de datos personales de trabajadores de empresas de plataformas digitales de servicios y la regulación de la gestión algorítmica del trabajo bajo la Ley 21.431. En R. Palomo Vélez (Ed.), *El trabajo a través de plataformas digitales. Problemas y desafíos en Chile*. Tirant lo Blanch.
- Contreras, P. et al. (2024). *Compliance y protección de datos personales*. Der Ediciones.
- Contreras Vásquez, P. y Trigo Kramcsák, P. (2019). Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. *Revista Chilena de Derecho y Tecnología*, 8(1), 69-106. <https://doi.org/10.5354/0719-2584.2019.52915>.
- Debesa Arregui, L. M. (2021). Privacidad y videovigilancia laboral en Chile: un análisis de los requisitos necesarios para la legitimación de la medida. *Ius et Praxis* 27(3), 82-106. <http://dx.doi.org/10.4067/S0718-00122021000300082>
- Del Castillo, C. (2007). Protección de datos: Cuestiones constitucionales y administrativas. Thomson-Civitas.
- EDPB. (2020) Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 4 de mayo de 2020.
- EDPB. (2022). Guidelines on the use of facial recognition technology in the area of law enforcement (05/2022).

- EDPB. (2024). Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, adoptadas el 8 de octubre de 2024.
- Fernández Toledo, R. (2019). Configuración del poder de dirección del empleador; denominación, naturaleza jurídica, fundamento y contenido. *Rev. derecho (Concepc.)*, 87(245), 51-97. <http://dx.doi.org/10.4067/S0718-591X2019000100051>
- Gamonal Contreras, S. y Guidi Moggia, C. (2020). *La tutela de derechos fundamentales en el derecho del trabajo*. Der Ediciones.
- Garrido, R. y Sáenz, B. (2024), *Ley de protección de datos personales: Aspectos claves y desafíos*. Der Ediciones.
- Gayrel, C. (2016). The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations. *Computer Law & Security Review* 32(3), 450-461. <https://doi.org/10.1016/j.clsr.2016.01.013>
- Goñi Stein, J. L. (2021): El derecho a la privacidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (Comentario al artículo 89 LOPDGGDD). En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (p. 4137). Thompson-Reuters Civitas.
- Guidi Moggia, C. (2023). *Teletrabajo, trabajo a distancia y nuevas formas de organización. Actualizado con la Ley No. 21.561*. Der Ediciones.
- Herrera, P. (2022). Discriminación de género por mecanismos automatizados de toma de decisiones: el caso de las conductoras de Uber. En R. Palomo Vélez (Ed.), *El trabajo a través de plataformas digitales. Problemas y desafíos en Chile*. Tirant lo Blanch.
- Irureta Uriarte, P. (2023). *Derecho del trabajo chileno. Derecho individual*. Tirant lo Blanch.
- Jasserand, C. (2016) Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data'. *European Data Protection Law Review*, 2(3), 297-311. <https://ssrn.com/abstract=3230342>
- Jurczuk, M. y Supronowicz, M.(2025). Consent in Data Privacy: A General Comparison of GDPR and HIPAA. *Prezglad Prawniczy Uniwersytetu in. Adam Mickiewicza*, 16, 173-194. <https://doi.org/10.14746/ppuam.2024.16.07>
- Lizama, L. y Lizama, D. (2020). *El derecho del trabajo en las nuevas tecnologías*. Der Ediciones.
- Neira Reyes, F. (2022). *El tratamiento de los datos personales de los trabajadores. Un análisis dogmático de la jurisprudencia administrativa* [tesis de magíster]. Universidad de Talca.
- Nettesheim, M. (2024). *EU Data Protection Law and Pay-or-Consent Business Models* <http://dx.doi.org/10.2139/ssrn.4768419>
- Nieves Nieto, N. (2020). El derecho a la protección de los datos personales en el marco de la relación de trabajo. En Monreal Bringsvaer et al. (Coords.), *Derecho del trabajo y nuevas tecnologías. Estudios en homenaje al profesor Pérez de los Cobos Orihuel (en su 25 aniversario como catedrático de derecho del trabajo)*. Tirant lo Blanch.

- OIT (1997). *Protection of Workers' Personal Data. An ILO Code of Practice*. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_protect/%40protrav/%40safework/documents/normativeinstrument/wcms_107797.pdf
- Pablo Pérez, R. (2022). Trabajo humano y plataformas: el problema de la calificación laboral en el derecho comparado. *Revista Chilena de Derecho y Tecnología*, 11(1), 71-102. <https://doi.org/10.5354/0719-2584.2022.60733>.
- Palomo Vélez, R. et al. (2022). El debate sobre la laboralidad del trabajo vía plataformas digitales en Chile y algunos problemas conexos. *Revista Latinoamericana de Derecho Social* (35), 59-99.
- Pasquinelli, M. (2023). *The eye of the master. A social history of Artificial Intelligence*. Verso.
- Pino, F. (2025). *Nuevas tendencias regulatorias: Tratamiento y protección de datos personales en Chile. Esquema y comentarios prospectivos*. Rubicón editores.
- Politou, E., Alepis, E. y Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions. *Journal of Cybersecurity* 4(1), ty001. <https://doi.org/10.1093/cybsec/tyy001>
- Rodríguez Iniesta, G. (2011). Facultades Empresariales de Control y Vigilancia de la Salud “versus” Derecho a la Intimidad de los Trabajadores. En C. Sánchez-Trigueros y F. González Díaz, *Libertad de empresa y poder de dirección del empresario en las relaciones laborales*. Thomson-Aranzadi.
- Schermer, B. W., Custers, B. y Van der Hof, S. (2024). The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology*, 16, 171-182. <https://doi.org/10.1007/s10676-014-9343-8>
- Sierra Herrero, A. (2022). Sobre la distinción entre el trabajador de plataformas digitales dependiente y el trabajador de plataformas digitales independiente. Análisis crítico de la Ley No. 21.413. En R. Palomo Vélez (Ed.), *El trabajo a través de plataformas digitales. Problemas y desafíos en Chile*. Tirant lo Blanch.
- Todolí Signes, A. y Rodríguez-Piñero Royo, M. (Eds.). (2020). *Vigilancia y control en el derecho del trabajo digital*. Aranzadi.
- Tschider, C. (2021). *Meaningful Choice: A History of Consent and Alternatives to the Consent*. Myth.
- Ugarte, J. L. (2005). La subordinación jurídica y los desafíos del nuevo mundo del trabajo. *Gaceta Laboral*, 11(1), 23-50.
- Ugarte, J. L. (2018). *Derechos fundamentales, tutela y trabajo*. Thomson Reuters.
- Ugarte, J. L. (2020). Trabajo en empresas de plataforma: Subordinación y más allá. *Revista Chilena de Derecho Privado*, (35), 17-49. <http://dx.doi.org/10.4067/S0718-80722020000200017>
- Varas Marchant, K. (2024). El impacto de las TIC en los tiempos de trabajo y descanso. *Revista Chilena de Derecho y Tecnología*, (13). <https://doi.org/10.5354/0719-2584.2024.74527>.

Viollier, P. y Velasco, P. (2021). El uso de toma de decisiones automatizadas para la selección de personal. En *Derechos fundamentales de la persona del trabajador: Vida privada, honra, inviolabilidad de las comunicaciones y protección de datos*. Tirant Lo Blanch.

Jurisprudencia citada

Sentencia de la Corte de Apelaciones de Estocolmo, Suecia, dictada el 1 de marzo de 2021, KamR Stockholm - Case No. 5888-20.

Dictamen de la Dirección del Trabajo. (30 de agosto de 2002). Dictamen Ordinario N.º 2852/158.

Dictamen de la Dirección del Trabajo. (28 de diciembre de 2021). Dictamen Ordinario N.º 146.

Dictamen de la Dirección del Trabajo. (26 de enero de 2022). Dictamen Ordinario N.º 146.
Dirección del Trabajo. (05 de mayo de 2024). Resolución Exenta 38.