consejo para la Transparencia

#ESMI DERECHO SABER

Estudios de Transparencia

La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público

Dirección de Estudios / Dirección Jurídica

Contenidos

I. INTRODUCCIÓN

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

A muy alto nivel, podemos observar que las tecnologías de videovigilancia y de reconocimiento facial las podemos vincular fundamentalmente con dos conceptos intrínsicamente relacionados entre sí: la privacidad o vida privada, y la protección de datos personales.

La **privacidad** siempre ha suscitado un tema de reflexión y preocupación en el desarrollo de las sociedades. En lo privado radica la libertad que cada persona tiene para decidir sobre su propia vida, y las personas solo han cedido parte de esa libertad para construir al Estado como una forma de organización de la convivencia humana (Escalante, 2008). Si bien en la antigüedad la libertad se concebía como una forma de participación en la vida pública -sólo se es libre si se puede participar y tratar de influir en las decisiones colectivas- hoy en día la libertad se ha volcado hacia lo privado, conforme a que el Estado o terceros no deben tener injerencia en las decisiones individuales. La privacidad ocupa la función de proteger al ciudadano de la posibilidad de que el Estado se entrometa en asuntos personales, constituyendo una garantía de ciertas libertades frente a entidades o personas dotadas de poder. La intervención de la autoridad en asuntos familiares, religiosos, íntimos o en todo aquello que se esté habituado a decidir individualmente parece ser algo injusto e ilegítimo. La privacidad, como orden jurídico, se define -en términos generales- como el ***"límite normativo al poder del Estado sobre el individuo, en el cual las personas tienen derecho a hacer lo que les parezca, con la única condición de no interferir con el derecho de las demás personas"*** **(Iosa, 2017, p. 405).**

Actualmente, el derecho a la privacidad ha sido consagrado como un derecho humano en la Declaración Universal de Derechos Humanos (artículo 12), en el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), en la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares (artículo 14) y en la Convención de los Derechos del Niño (artículo 16), como también en otros ordenamientos jurídicos regionales, como el sistema europeo e interamericano, específicamente en la Convención Americana sobre Derechos Humanos (artículo 11.2) y el Convenio para la Protección de los Derechos y Libertades Fundamentales, también denominada Convención Europea de Derechos Humanos (artículo 8) (Maqueo, et al. 2017).

En cuanto a **protección de datos personales**, y de modo muy general, cabe destacar a nivel comparado el Convenio 108+ (2018) y, sobre todo, el Reglamento General de Protección de Datos de la Unión Europea (2018) ("RGPD" o "GDPR", por sus siglas en inglés). Este último se trata de una normativa en el cual el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea actualizaron y unificaron los estándares para la protección de datos personales de todos los ciudadanos pertenecientes a la Unión Europea. Su objetivo principal es ***"dar el control a los ciudadanos y residentes respecto a sus datos personales y simplificar el entorno regulador de los negocios internacionales, unificando la regulación dentro de la Unión Europea".*** El RGPD, que veremos en más detalle a lo largo del trabajo, protege a los ciudadanos cuyos datos personales son almacenados, procesados, transferidos o divulgados por organizaciones o empresas sin su consentimiento, sancionando severamente el incumplimiento de la normativa. Además, incorpora definiciones más precisas de lo que es un dato personal, refiriéndose a las direcciones IP, la información económica, la salud mental o la información biométrica.

En Chile, la Constitución Política, en su artículo 19 N°4, que versa sobre los derechos fundamentales de protección a la vida privada y la protección de datos personales; y la Ley N°19.628 sobre Protección de la Vida Privada, constituyen los cuerpos normativos que amparan la privacidad y el tratamiento de datos por parte de entidades públicas y privadas en nuestro país.

Si bien en distintos Estados se han ido reconociendo los derechos a la privacidad y la protección de datos personales, el desarrollo tecnológico e informático -hasta llegar a la videovigilancia y el reconocimiento facial- ha redimensionado su objetivo, alcanzando nuevos matices. La información personal nunca había estado disponible para ser difundida masivamente como ocurre actualmente a través de dichas tecnologías. Estas, no solo ponen en juego la información nominal, sino que también los datos personales que se circunscriben a otras esferas particulares, como nuestro propio cuerpo o, inclusive, los datos generados por artefactos electrónicos de uso cotidiano, lo que se vincula con lo que ha sido denominado "Internet de las Cosas". Es por todo ello que los derechos a la privacidad y la protección de datos personales adquieren una importancia fundamental frente a los riesgos que puede conllevar estos nuevos desarrollos tecnológicos.

Los riesgos asociados al tratamiento de datos personales han aumentado por la emergencia de tecnologías de información tan complejas como el Big Data o la inteligencia artificial. Las tecnologías actuales permiten generar y procesar magnitudes increíbles de información personal y no solo circunscrita a datos recabados desde las plataformas digitales, sino que también desde nuestra propia biometría como las huellas dactilares o las huellas faciales. Por ello, la masificación de grandes volúmenes de información personal supone un gran reto para las legislaciones actuales, en cuanto a que estas tecnologías y sus algoritmos permiten la identificación de las personas, aun cuando esos datos son considerados anónimos o estadísticos (Gil, 2016).

En Chile, la mayor preocupación por un posible mal uso de información personal se extiende, en primer lugar, hacia el sector privado, a través de transacciones comerciales como las bancarias (61%) y empresas de servicios o grandes tiendas (54%); y, en segundo lugar, hacia el sector público, a través de trámites realizados en algún servicio (48%) o solicitud para algún beneficio estatal (47%). En términos globales, un 83% de la ciudadanía desconfía del cuidado de sus datos personales por parte de instituciones públicas y privadas (ENT, 2020).

El devenir tecnológico ha dispuesto distintas fuentes donde es posible tratar datos personales: redes sociales, aplicaciones móviles, cámaras de vigilancia, internet de las cosas o el comercio digital. El aumento forzado de las transacciones online, producto de la pandemia del Coronavirus, también ha contribuido a una habitualidad en la entrega de información personal. En Chile, durante el 2020, disminuyó un 14% la preocupación de las actividades que se realizan en internet. También disminuyó la lectura sobre las condiciones de privacidad al hacer uso de redes sociales o servicios de internet, especialmente en jóvenes. Esto sin duda representa un problema en cuanto resulta complejo, por ejemplo, informarse acerca de los múltiples consentimientos y autorizaciones que los servicios digitales solicitan, en un lenguaje poco claro y excesivo, para el tratamiento de datos personales, desincentivando al usuario a informarse cómo estos serán tratados.

En resumen, se observa que el contexto actual ha perjudicado el interés ciudadano respecto al cuidado de sus datos, lo cual está asociado a que gran parte de las comunicaciones, transacciones, trámites o compras se realizan por medio de tecnologías digitales a distancia y de uso diario. La ciudadanía en Chile ha disminuido su preocupación por el tratamiento de su información personal que se requiere habitualmente, como en el uso de aplicaciones o situaciones de compra de bienes o servicios y donde se recolectan y tratan, por ejemplo, imágenes propias y de la familia; la dirección del domicilio particular; el RUN; el número de teléfono fijo o móvil; el estado de salud; la dirección de correo electrónico y el estado civil. Sin perjuicio de esto, la menor preocupación asociada a datos personales se observa en temas relativos a la seguridad pública, como en los sistemas de reconocimiento facial para fines de seguridad y la videovigilancia (ENT, 2020).

Esta disminución en la preocupación del tratamiento de datos personales en el contexto de seguridad ciudadana resulta de gran relevancia, en consideración a que, uno de los principales fines de utilización de la videovigilancia y el reconocimiento facial, es precisamente la seguridad pública. En este contexto, podemos ver la habitual dicotomía que se plantea de seguridad o vigilancia versus privacidad como principios intrínsicamente en oposición o tensión, no obstante que una mirada de respeto a los derechos fundamentales bien nos debe hacer buscar un equilibrio en pos de su máxima realización y de garantizar siempre el contenido esencial de los derechos. Es en este escenario, de avance tecnológico, de avance legislativo en temas de privacidad y datos personales alrededor del mundo, de efectos disruptivos a causa de la pandemia del Coronavirus, de una mayor utilización de dispositivos de videovigilancia y reconocimiento facial y, sobre todo, de un contexto en que la seguridad pública resulta ser hoy en día un tema de gran preocupación para la ciudadanía en Chile, que hemos estimado apropiado preparar este trabajo sobre protección de datos personales en contextos de avanzado desarrollo tecnológico con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público.

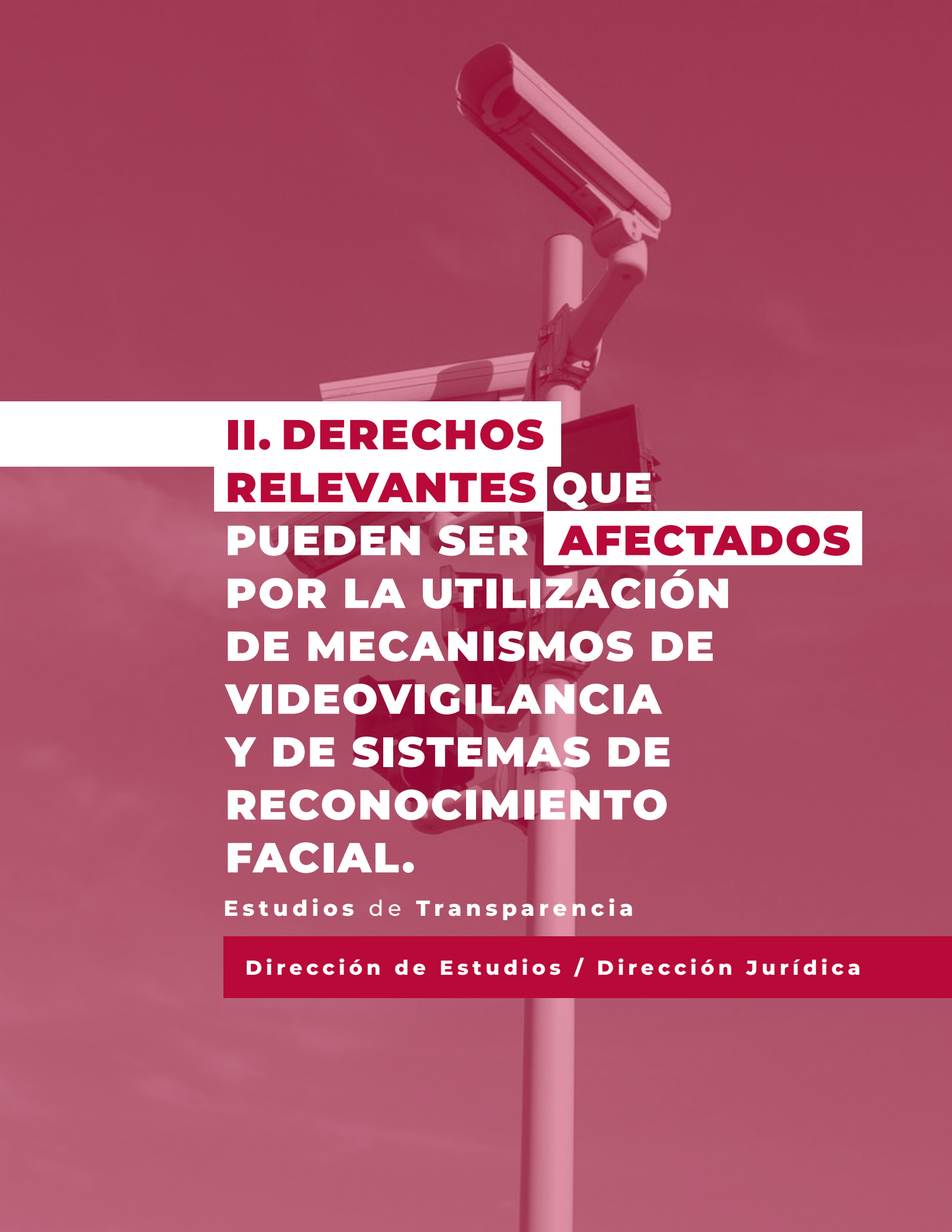
- En el presente documento, se revisarán en primer lugar aquellos derechos relevantes que pueden llegar a ser afectados o amenazados por la utilización de mecanismos de videovigilancia y de sistemas de reconocimiento facial en Chile.

- En segundo lugar, se identifican algunos de los instrumentos más importantes a nivel de marco normativo comparado de protección de datos personales relacionado con el despliegue e implementación de mecanismos de videovigilancia y de reconocimiento facial. Luego de eso se describe la jurisprudencia destacada de las principales entidades y agencias de protección de datos personales en el ámbito internacional.

- Consecutivamente, se expone el marco normativo existente en Chile sobre protección de datos personales, y que aplica tanto para personas naturales y jurídicas públicas y privadas. A continuación, se analiza y detalla la jurisprudencia más relevante en materia de protección de datos, videovigilancia y de sistemas de reconocimiento facial, tanto del Consejo para la Transparencia ("Consejo" o "CPLT") como de los tribunales de justicia. Esta sección se complementa con pronunciamientos y recomendaciones del CPLT en la materia que, si bien no constituyen jurisprudencia administrativa propiamente tal, resultan ser de relevancia por incorporar nuevos criterios asociados a estas tecnologías.

- Posteriormente, se presenta información estadística de estudios realizados en la materia, amparos recibidos en el CPLT y la judicialización de casos, a modo de visualizar el nivel de cumplimiento normativo que tienen los organismos públicos en Chile sobre protección de datos personales.

- Finalmente, a partir del análisis de todos los aspectos revisados y desarrollados en el documento, se presentan recomendaciones con miras a mejorar marcos normativos y prácticas institucionales destinadas a erigir un adecuado marco de protección de datos personales en la utilización de mecanismos de videovigilancia y de sistemas de reconocimiento facial en nuestro país.



II. DERECHOS RELEVANTES QUE PUEDEN SER AFECTADOS POR LA UTILIZACIÓN DE MECANISMOS DE VIDEOVIGILANCIA Y DE SISTEMAS DE RECONOCIMIENTO FACIAL.

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

Dentro de las tecnologías más novedosas, pero que conllevan múltiples desafíos en protección de datos, encontramos a la videovigilancia y al reconocimiento facial. La primera corresponde a un sistema compuesto por cámaras de distinta índole y su uso se enfoca, actualmente, en la seguridad (Ramírez, 2017). En efecto, en Chile, como en otras partes del mundo, el fundamento empleado para la videovigilancia es la supuesta eficacia que tienen en la provisión de la seguridad pública, ya sea en la prevención del delito o la persecución de éste (Ibid.). En un primer momento, la videovigilancia se comenzó a emplear en espacios privados, circunscrita a la gestión empresarial a fin de controlar y vigilar la productividad. Fueron los bancos, empresas, fábricas y algunas tiendas las que empezaron a incorporar circuitos de televisión en espacios cerrados. Posteriormente, es el sector público el que empezó a adoptar cámaras de videovigilancia en diversos sistemas de transporte público con la finalidad de controlar el servicio y reducir los actos vandálicos. Mientras los costos de esta tecnología fueron disminuyendo se fueron expandiendo a otras áreas, y la propia tecnología también fue mejorando en la resolución de las imágenes hasta la actualidad con la inclusión de drones y globos aerostáticos con cámaras de alta definición, aptas para la grabación nocturna y un control biométrico certero (Ibid.). No obstante, cuando se habla de videovigilancia en el ámbito público no se debe cometer el error de domiciliarla al dispositivo de grabación, sino que se entiende como videovigilancia una determinada función que no es intrínseca al dispositivo. Por ello, un sistema de videovigilancia policial va a tener una función distinta que un sistema de videovigilancia de tráfico vehicular. En este sentido, la videovigilancia se debe ceñir a la función por la cual se está vigilando.

Por otra parte, el reconocimiento facial ha florecido producto de nuevas tecnologías de análisis biométrico y, últimamente, también a causa de la pandemia del Coronavirus. En términos muy generales, su funcionamiento se basa en el procesamiento de imágenes del rostro de personas para efectos de su identificación o verificación mediante el uso de huellas faciales. Su campo de aplicación es variado, utilizándose en el control de acceso a la asistencia en puestos laborales, seguridad, finanzas, transporte, teléfonos inteligentes, y también en la gestión gubernamental, entre otros (Li, et. al., 2020). Desde la década de 1960, el reconocimiento facial ha evolucionado utilizando, en primer lugar, la geometría facial y posteriormente, durante la década de 1990, algoritmos más sofisticados como el “Análisis de Componentes Principales (ACP)”, cuya principal función es reducción de la dimensionalidad de los datos. El ACP extrae las características del rostro, conservando las características esenciales de los datos. Para cotejar y clasificar rostros en una base de datos, se utilizan otro tipo de algoritmos como el “Análisis Lineal Discriminante (ALD)”.

Técnicamente la diferencia entre ambos radica en que el ACP requiere que la varianza de los datos después de la reducción de la dimensionalidad sea lo más grande posible para poder dividir los datos lo más ampliamente posible, mientras que el ALD requiere que la varianza dentro de la misma categoría de grupos de datos después de la proyección sea lo más pequeña posible, y que la varianza entre grupos sea lo más grande posible (Ibid.). En la actualidad, han evolucionado otras tecnologías, más fiables y precisas para detectar, identificar y clasificar rostros como las Redes Neuronales o el Deep Learning.

El reconocimiento facial no está exenta de riesgos y complicaciones. Cabe recordar el fracaso en la implementación del sistema de reconocimiento facial implementado por el Servicio de Registro Civil e Identificación ("Registro Civil") para evitar que las personas asistiesen presencialmente a sus oficinas para obtener la clave única. La aplicación fue burlada el mismo día de su puesta en marcha por un usuario demostrando lo fácil que resultaba engañar al sistema para obtener la clave de otra persona. En este sentido el avance tecnológico requiere de políticas fuertes de ciberseguridad, ponderando la facilidad y buena experiencia que puede entregar con los riesgos asociados.

Aun así, los datos personales recabados desde sistemas de videovigilancia y reconocimiento facial, en términos de seguridad, es lo que menos les preocupa a los chilenos (39% y 36% respectivamente). Por el contrario, existe una mayor aprobación del uso de datos personales con dicho fin, lo que se relaciona con que la menor preocupación del uso de sus datos sea por cuestiones de seguridad. En este sentido, un 95% está de acuerdo en usar videovigilancia para prevenir la delincuencia, mayoritariamente en mujeres y quienes viven en la Región Metropolitana.

Por último, hay que reconocer que el Estado es el principal tratador de información personal, toda vez que los servicios públicos, para cumplir sus funciones requieren administrar y procesar computacionalmente información personal (Jijena, 2013). Por ello, le corresponde al derecho público establecer límites y restricciones para que no se vulnere la intimidad de las personas y para que las entidades públicas utilicen los datos personales dentro de su competencia exclusiva y para fines específicos. La Ley N°19.628 sobre Protección de la Vida Privada estipula las responsabilidades de los servicios públicos respecto a las bases de datos que contienen información personal y delimita los derechos de los titulares de los datos. Los servicios públicos, en su calidad de responsables del tratamiento de datos personales, deben dar cumplimiento a todo requerimiento que un titular de los datos haga invocando como fundamento al derecho de acceso a datos personales que lo identifican (Ibid.).

Los servicios públicos también deben considerar que las y los ciudadanos poseen los mecanismos legales para controlar el uso de sus datos personales. La ley permite a los titulares de la información personal solicitar información sobre la procedencia de los datos almacenados, el propósito de dicho almacenamiento, la identidad de los posibles destinatarios a los cuales los datos se les transmitan regularmente. Además, las y los ciudadanos están facultados para solicitar que las entidades que posean bases de datos con información personal de su titular corregirlos, actualizarlos, eliminarlos o bloquearlos, salvo que dicha petición impida o entorpezca el debido cumplimiento de las funciones del servicio, la reserva o secreto establecidos legalmente, o la seguridad y el interés nacional. Estos derechos son conocidos como los derechos ARCO.

Según podemos observar de lo señalado anteriormente, la utilización de mecanismos de videovigilancia y de reconocimiento facial puede generar en Chile la afectación de una serie de derechos de las personas (Contreras, 2021). Entre los más relevantes podemos enumerar los siguientes:

a. Derecho a la protección de la vida privada.

Este derecho se encuentra consagrado en el artículo 19 N°4 de la Constitución Política, asegurando a todas las personas *"El respeto y protección a la vida privada y a la honra de la persona y su familia (...)".*

Este derecho ha sido conceptualizado por diversos autores, y se ha entendido de forma difusa y amplia. Entre algunos aspectos que quedarían cubiertos por este, estaría el cuerpo de los individuos, sus imágenes, su interioridad corporal y psicológica, entre otros (Figueroa, 2014). A juicio de Figueroa (2014, p. 111), el cuerpo *"puede ser entendido como una entidad susceptible de ser captada y revelada. Las fotografías o filmaciones son las instancias más frecuentes de captaciones (...)".* Por su parte, en otras jurisdicciones este derecho se ha vinculado con el género, el nombre, y la información biométrica de las personas, al tener estos aspectos un carácter intrínsicamente privado[1].

En el entendido que la videovigilancia y la tecnología de reconocimiento facial abarcan -precisamente- la captación y utilización de imágenes del cuerpo y rostro de personas naturales, así como el tratamiento de información biométrica, es que el derecho a la protección de la vida privada resulta sumamente relevante[2], pudiendo verse amenazado o perturbado a causa de su implementación.

Por último, cabe señalar que el Tribunal Europeo de Derechos Humanos (TEDH) ya ha señalado expresamente que la videovigilancia constituye una injerencia en el derecho de respeto a la vida privada[3].

[1] Véase "The Queen (on application of Edward Bridges) v. THE CHIEF CONSTABLE OF SOUTH WALES POLICE" (2018) High Court of Justice Queen's Bench Division, Divisional Court, case CO/4085/2018, (2019) EWHC 2341 (Admin).

[2] Cabe destacar que en relación a la dimensión "espacial", el derecho protege no sólo los ámbitos íntimos o domésticos, sino también los "comportamientos realizados públicamente o en lugares públicos", pudiendo extenderse fuera del domicilio o de las dependencias privadas de una persona. (Arzoz, 2015, p. 346).

[3] Peck v. Reino Unido, Ene. 28, 2003.

b. Derecho a la inviolabilidad del hogar.

Este derecho está consagrado en el artículo 19 N°5 de la Constitución Política, asegurando a todas las personas *"la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse (...) en los casos y formas determinados por la ley"*.

La doctrina y la jurisprudencia[4] nacional han entendido una concepción amplia de este derecho fundamental, que comprende incluso la observancia o registro de bienes sin autorización del afectado, así como las diversas formas de afectación que pueden presentar las innovaciones tecnológicas, tales como los drones o los globos de vigilancia (Álvarez, 2019; Cea, 2019).

Lo anterior hace concluir que el uso de sistemas de videovigilancia y de reconocimiento facial -que estén vinculados al funcionamiento de cámaras- bien podrían, en ciertas circunstancias, importar una afectación al derecho fundamental de inviolabilidad del hogar como, por ejemplo, en el caso que las cámaras se encuentren apuntado o sean direccionadas hacia el interior de una vivienda.

[4] Sentencias de Corte Suprema en Roles N°18.458-2016 y N°18.481-2016, ambas de 1 de junio de 2016.

c. Derecho a la protección de datos personales.

Este derecho se encuentra consagrado en el artículo 19 N°4 de la Constitución Política, asegurando a todas las personas *"La protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley"*[5].

Esta consagración establece una reserva legal especial, la cual es especialmente relevante para los órganos del Estado, atendido el principio de legalidad o juridicidad en la actuación del Estado[6] (Pica y Vargas, 2021). Por su parte, cabe destacar que, en virtud de la supremacía constitucional y el principio de tutela de derechos fundamentales, los órganos de la administración del Estado deben reconocer -en todas sus actuaciones- la fuerza obligatoria de la consagración constitucional del derecho de protección de datos personales, así como respetarlo, protegerlo y promoverlo en su calidad de derecho fundamental.

A nivel legal, este derecho se encuentra regulado en la Ley N°19.628 sobre Protección de la Vida Privada (en adelante, "LPVP") que establece las reglas generales sobre tratamiento de datos personales que deben seguir las entidades públicas y privadas que desarrollen esta actividad en Chile, determinando un conjunto de derechos de los titulares y obligaciones para los responsables, además de una acción especial de tutela judicial denominada habeas data. Esta norma será revisada en detalle más adelante en este trabajo.

Como veremos, la utilización de los mecanismos en comento resultan relevantes para este derecho, en cuanto su funcionamiento puede generar, al menos, el almacenamiento y uso de datos personales de carácter sensible, correspondiente a las imágenes de las personas captadas. Además, cabe señalar que no solo la identidad puede determinarse a partir de un rostro, sino que también caracterizas fisiológicas y psicológicas tales como el origen étnico, enfermedades, las emociones y el bienestar, los cuales también son datos personales de carácter sensible (WP29, 2012, p. 23).

[5] La incorporación de este derecho fue efectuada mediante reforma constitucional a través del Artículo único de la Ley N°21.096. Sin perjuicio de esta consagración, anteriormente se entendía este derecho en función del derecho fundamental a la protección de la vida privada (Pica y Vargas, 2021).

[6] En aplicación de esta reserva, las normas que regulen el tratamiento y protección de datos personales deberán siempre adoptar la forma de una ley, excluyéndose por tanto las formas infralegales de regulación.

d. Derecho a la libertad de expresión y derecho a la libertad de reunión y de asociación.

El derecho a la libertad de expresión se encuentra consagrado en el artículo 19 N°12 de la Constitución Política, asegurando a todas las personas *"La libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio (...)"*. A su turno, el artículo 19 N°13 de ese mismo cuerpo legal establece *"El derecho a reunirse pacíficamente sin permiso previo y sin armas. Las reuniones en las plazas, calles y demás lugares de uso público, se regirán por las disposiciones generales de policía"*.

Conforme señala Contreras et al. (2016), la libertad de expresión es uno de los derechos fundamentales que constituye un pilar del Estado democrático. Entre los fundamentos que reconoce de este derecho, señala que este permite el libre desarrollo de la personalidad y habilita la agencia moral de los individuos, promoviendo la protección de la autonomía de las personas. En dicho contexto, se ha entendido que el funcionamiento de sistemas de videovigilancia o de reconocimiento facial en el espacio público, puede generar afectaciones a los derechos mencionados por actuar como inhibidores del actuar libre de las personas. Los individuos, al saber la existencia de estos sistemas, dejarían de actuar normalmente, limitando, por ejemplo, los espacios políticos, de manifestación o protesta (WP29, 2015; GPA, 2020)[7].

[7] Sobre esta relación véase también Lovera, Domingo. (2018). Privacidad, espacios públicos y vigilancia. Anuario de Derecho Público UDP 2018, Facultad de Derecho Universidad Diego Portales. Santiago. Ediciones
UDP.

e. Derecho a la no discriminación.

La igualdad es uno de los principales valores del ordenamiento constitucional chileno y se encuentra en diversos preceptos de la Constitución Política (Contreras et al., 2016). En particular, se ha observa el artículo 19 N°2 de la Constitución, que asegura *"La igualdad ante la ley. En Chile no hay persona ni grupo privilegiados. En Chile no hay esclavos y el que pise su territorio queda libre. Hombres y mujeres son iguales ante la ley. Ni la ley ni autoridad alguna podrán establecer diferencias arbitrarias."* Bajo este esquema, la igualdad se ha entendido como una proscripción a las diferencias arbitrarias, lo que es obligatorio tanto para la ley como para las autoridades públicas en Chile.

Por su parte, cabe hacer presente que en nuestro país la Ley N°20.690 que Establece medidas contra la discriminación, indica que corresponde a cada órgano de la Administración del Estado, dentro del ámbito de su competencia, *"elaborar e implementar las políticas destinadas a garantizar a toda persona, sin discriminación arbitraria, el goce y ejercicio de sus derechos y libertades reconocidos por la Constitución Política de la República, las leyes y los tratados internacionales ratificados por Chile y que se encuentren vigentes"*. Dentro de la definición de discriminación arbitraria, se comprenden, entre otras, aquellas fundadas en motivos de raza, etnia, identidad y expresión de género, apariencia personal y sexo[8].

En el contexto de este trabajo, el derecho descrito resulta relevante pues se ha observado que la utilización de mecanismos de videovigilancia y de reconocimiento facial pueden conllevar eventos de discriminación arbitraria que afecten a personas o grupos demográficos particulares por, por ejemplo, tener estos sistemas errores o limitaciones de diseño o deficiencias en los datos utilizados que implican sesgos implícitos en su funcionamiento. En el ámbito del Estado, esta clase de situaciones puede generar discriminaciones ilegítimas en la entrega, por ejemplo, de productos, servicios o en el otorgamiento de derechos (Becker y Garrido, 2017). En el contexto específico de sistemas biométricos, se ha indicado que éstos pueden generar situaciones de discriminación en ciertas personas que, por su condición, no pueden efectuar un proceso de registro. En el caso del reconocimiento facial, también se ha señalado que estos sistemas pueden tener sesgos que conllevan riesgos para la adecuada identificación de mujeres, afrodescendientes, asiáticos o de minorías étnicas (WP29, 2012).

[8] Este derecho se relaciona fuertemente con el tratamiento de datos personales de carácter sensible, como datos sobre el origen étnico o datos biométricos en general, en el entendido que su uso indebido puede ser fuente de serias discriminaciones arbitrarias.

f. Derecho a la propia imagen.

El derecho a la propia imagen se ha entendido dentro del ámbito de los derechos de la personalidad que tienen por fin defender intereses humanos ligados a la esencia de la personalidad. Estos derechos son generales, absolutos, extrapatrimoniales, esenciales, indisponibles, e imprescriptibles (Alessandri et al., 2005). Este derecho se ha comprendido como una proyección física de la persona, un sello de singularidad distintiva dentro del ámbito de la vida en sociedad y que constituye un signo genuino de identificación de todo individuo, incluyendo incluso su nombre y su voz (Díez-Picazo, 2003). Este derecho estaría vinculado al derecho a la protección de la vida privada, al honor y a su valor comercial[9].

En el escenario bajo análisis, bien se podría llegar a interpretar que una grabación o captación y uso de imágenes del rostro de personas naturales, a través de un sistema de videovigilancia o de reconocimiento facial, sin la debida autorización, podría configurar en ciertos casos una vulneración al derecho a la propia imagen de los individuos filmados, al no haberse contando con la autorización del titular del derecho para captar y usar su rostro[10].

[9] Ver sentencia de Corte Suprema, Rol N°14988-2018. Tercera Sala Constitucional.

[10] Sobre este derecho se puede agregar que la evolución de la jurisprudencia de recursos de protección ha pasado desde la tesis de la renuncia tácita de privacidad en lugares públicos (SCA de Santiago, 1 de agosto de 1989, s/rol, c. 7°. Confirmada por SCS R. 14.598-1989) a la exigencia de consentimiento previo y expreso para la divulgación de la imagen (SCA de Santiago, R. 3322-97, c. 4°). La jurisprudencia exige que la persona sea identificable: requiere que "la figura utilizada sea reconocible, es decir, permita su identificación indubitada" (SCA de Santiago R. 469-2000, c. 4°). Por lo tanto, no se encuentran protegidas imágenes difuminadas, borrosas o aquellas que no permitan individualizar o identificar suficientemente al titular del derecho.

Ahora bien, al comprenderse -en la lista anterior- derechos que califican de fundamentales, cabe destacar que a estos se les aplica el régimen general del sistema de límites a los derechos fundamentales, el que exige que, para que una restricción sea constitucionalmente admisible, se cumpla con los siguientes presupuestos[11]:

i. La restricción debe estar prevista en la ley y el mandato legal debe ser determinado y específico. La intervención estatal respecto del derecho debe seguir los siguientes estándares que la doctrina ha sistematizado a partir de la jurisprudencia del Tribunal Constitucional (Cordero, 2009): **(i)** No basta con que sea una ley, la ley debe cumplir con estándares sustantivos (reserva material); **(ii)** La ley debe contemplar pautas objetivas —es decir, criterios objetivos— para el ejercicio de la potestad pública, incluyendo criterios de oportunidad; **(iii)** La potestad debe estar sujeta a control por un tercero imparcial; y **(vi)** Debe existir la posibilidad de ejercer los derechos procesales necesarios para tutelar al derecho respecto de la intervención estatal.

ii. La restricción debe perseguir una finalidad legítima, que puede estar fundada en la protección de un derecho fundamental (por ejemplo, la libertad de expresión) o un bien colectivo de rango constitucional (por ejemplo, la seguridad nacional o el orden público).

iii. La restricción debe ser proporcional al fin buscado y debe respetar el contenido esencial del derecho.

[11] Conforme señala Contreras (2021), los estándares interamericanos de derechos humanos son plenamente aplicables en Chile. En la jurisprudencia de la Corte Interamericana de Derechos Humanos, se han adoptado ciertos requisitos para justificar restricciones a un derecho establecido en la Convención Americana sobre Derechos Humanos (Pacto de San José). En Claude-Reyes et al. con Chile, la Corte adoptó tres condiciones (i) las restricciones deben estar establecidas previamente en la ley; (ii) deben cumplir un objetivo legítimo en virtud de la Convención; y (iii) deben ser necesarios para una sociedad democrática.

Habiéndonos referido al funcionamiento general de los mecanismos de video-vigilancia y de los sistemas de reconocimiento facial, así como al catálogo de potenciales derechos que, en mayor o menor medida, podrían verse afectados mediante su uso, resulta adecuado en este punto pasar a concentrarnos en dos temas esenciales para el contexto de este trabajo: las particularidades de la relación entre estas tecnologías y el derecho de protección de datos personales; y aquellos riesgos particulares que la videovigilancia y el reconocimiento facial genera en este derecho fundamental.

En primer lugar, advertimos que la tecnología de reconocimiento facial puede ser utilizada para un sinnúmero de propósitos particulares que van de la mano con el nivel de riesgo y afectación que genera en los derechos de las personas. Si bien la mayoría de estos propósitos tienen relación con la identificación de un individuo, existen distintas aplicaciones específicas que resulta ilustrativo observar para entender la multiplicidad de escenarios de utilización.

Entre estos casos de uso, podemos encontrar **(i)** autenticación o verificación de identidad (uno-a-uno) por parte del sector público (por ejemplo, para el control de pasaportes en aduanas) y autenticación o verificación de identidad (uno-a-uno) por parte del sector privado (por ejemplo, para controlar el acceso a ciertas instalaciones o recintos); **(ii)** identificación de individuos y marcado de imágenes en las redes sociales; **(iii)** servicios que ofrecen la identificación de personas mediante el emparejamiento o comparación de imágenes en bases de datos compiladas a partir de fuentes accesibles públicamente, como las redes sociales; **(iv)** vigilancia de espacios de acceso público (incluidos lugares de trabajo y tiendas) por parte del sector privado con fines de seguridad; **(v)** vigilancia de espacios de acceso público (incluidos los entornos educativos) por el sector público y las fuerzas de orden y seguridad con fines de prevención de la delincuencia o la protección de la salud pública[12]; **(vi)** utilización en espacios de acceso público con fines de marketing o publicidad personalizados; **(vii)** manejo y gestión de trabajadores (por ejemplo, para la comprobación de asistencia y seguimiento de la productividad); **(viii)** comprobación de asistencia y vigilancia de exámenes en contextos educativos; e **(ix)** investigación científica.

[12] Como veremos más adelante, este propósito de utilización es el que se ha visto mayormente en Chile en relación a la tecnología de reconocimiento facial.

Una vez descritas las distintas aplicaciones que puede presentar la tecnología de reconocimiento facial, resulta necesario que identifiquemos aquellas particularidades que presenta esta tecnología, y la de videovigilancia en general, para el derecho de protección de datos personales, lo cual resulta esencial a la hora de identificar con precisión los riesgos que ellas presentan, y aquellas medidas de resguardo que eventualmente se podrían aplicar.

Entre estas particularidades, podemos destacar las siguientes:

- En ambos casos existe una utilización de imágenes de personas naturales y sus rostros (GPA, 2020).

- En ambos casos las imágenes y rostros de las personas pueden ser recolectados sin necesidad de conocimiento, cooperación o contacto directo con el titular a quien hace referencia dicha imagen (GPA, 2020).

- Las características que son captadas mediante esta recolección de imágenes, como la imagen del rostro, son habitualmente visibles al público en general.

- La ausencia de contacto directo que permiten estas tecnologías y los propósitos a los que están asociados, generan dificultad en torno a la obtención de un consentimiento expreso de las personas para la utilización de sus datos.

- En el caso del reconocimiento facial, además se utilizan datos biométricos sobre rasgos faciales que también pueden ser recolectados sin necesidad de contacto, cooperación ni conocimiento de la persona afectada ni mediante el uso de la fuerza, lo cual lo distingue de la huella dactilar o la información genética.

- Estas captaciones pueden identificar personas naturales específicas directa o indirectamente (por ej. en combinación con otra información), lo que implica un tratamiento de datos personales de carácter sensible (que se definirán más adelante) y que requieren de una protección mayor (EDPS, 2021).

- Tanto el rostro, como la huella facial o datos biométricos en general, son únicos para los individuos y no pueden ser modificados o suprimidos por éste, como, por el contrario, podría ocurrir con un correo electrónico o número de teléfono (Becker y Garrido, 2017; GPA, 2020).

- La recolección de datos personales mediante el uso de estas tecnologías puede ser efectuada a escala masiva e indiscriminada, de un sinnúmero de sujetos en un limitado lapso de tiempo.

- La tecnología de reconocimiento facial en el estado actual puede operar mediante sistemas de video o cámaras que funcionan en tiempo real (live), y respecto de una gama de cámaras, ángulos y condiciones de iluminación.

Bajo esta gran cantidad de particularidades, observamos que la implementación de estas tecnologías puede generar un sinnúmero riesgos relevantes para el derecho de protección de datos personales y los titulares de datos, los cuales pueden acontecer por la gran variedad de variables que se pueden presentar en su utilización.

De esta forma, como elementos de riesgo podemos identificar, al menos, los siguientes:

i. Falta de transparencia en relación a la recolección de datos personales y sensibles, incluyendo datos biométricos.

ii. Falta de transparencia en relación al tratamiento de datos que se efectúa a partir de los datos recolectados, por ejemplo, en relación a su propósito y el tiempo de retención de los datos.

iii. Ausencia de avisos que informen debidamente sobre la existencia de mecanismo de videovigilancia o reconocimiento facial en determinada área o zona.

iv. Recolección a escala masiva e indiscriminada de datos personales sensibles y biométricos.

v. Falta de transparencia en relación con el intercambio o cesión de datos (por ejemplo, asociados a planillas biométricas) entre, por ejemplo, organismos públicos y privados, incluyendo fuerzas de orden y seguridad.

vi. Insuficientes medidas de seguridad en el tratamiento de los datos, incluyendo posibles vulneraciones a su integridad, disponibilidad o confidencialidad.

vii. Falta de control de los titulares sobre la recolección y el tratamiento de sus datos, incluida la falta de consentimiento para el tratamiento.

viii. Dificultades para los titulares a la hora de ejercer sus derechos en materia de protección de datos personales.

ix. Ausencia de debate público y acuerdo general sobre las tecnologías de reconocimiento facial y la videovigilancia.

x. Ausencia de una regulación específica que regule el uso de estas tecnologías, y/o ausencia de una normativa robusta en protección de datos personales.

xi. Ausencia de una autoridad de control con capacidad de fiscalizar y sancionar el uso indiscriminado de estas herramientas.

xii. Ausencia de normas específicas que regulen el uso de estas tecnologías por parte de las fuerzas de orden y seguridad, por ejemplo, en relación a la localización de la tecnología de reconocimiento facial o los criterios para incorporar individuos en listas de vigilancia.

Finalmente, para completar este cuadro general e inicial de riesgos al derecho de protección de datos personales, estimamos adecuado presentar también la categorización de riesgos que ha identificado la Working Party 29 sobre la tecnología de reconocimiento facial (WP29, 2012, p. 24-25). Esta categorización se refiere a los siguientes aspectos de esta tecnología:

i. Precisión. Asociado a la calidad de las imágenes y la dificultad que presentan para la correspondencia o categorización (índice de error).

ii. Impacto. Asociado a que la finalidad y circunstancias particulares de cada sistema de reconocimiento facial determinará el impacto específico en la protección de datos.

iii. Consentimiento y transparencia. Vinculado con el hecho de que las imágenes pueden capturarse y tratarse desde diversos puntos y ángulos, y sin el consentimiento del titular.

iv. Fin o fines ulteriores al tratamiento. Vinculado con el hecho de que las imágenes digitales capturadas pueden fácilmente compartirse o copiarse para su tratamiento en sistemas diferentes de aquellos para los que estaban destinadas originalmente.

v. Vinculación. Relativo a la creación y vinculación de perfiles.

vi. Seguimiento/elaboración de perfiles. Asociado al seguimiento de rutas, costumbres o localización de individuos, permitiendo la elaboración de perfiles.

vii. Tratamiento de datos sensibles. El tratamiento de datos biométricos puede utilizarse para determinar datos sensibles, en especial aquellos con señales visuales como raza, grupo ético u enfermedades.

viii. Revocabilidad. Vinculado con el hecho de que las principales características faciales de una persona son estables en el tiempo y los sistemas también pueden mejorar el reconocimiento recogiendo y asociando diferentes rostros conocidos de una persona.

ix. Suplantación – usurpación de identidad. Relativo al hecho de que existen sistemas de reconocimiento facial que son fáciles de suplantar.

III. MARCO NORMATIVO COMPARADO

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

A nivel de marco normativo comparado de protección de datos personales relacionado con el despliegue e implementación de mecanismos de videovigilancia y de reconocimiento facial podemos identificar varios instrumentos relevantes. Por la densidad normativa que presentan, y por ser jurisdicciones que habitualmente constituyen ejemplos para nuestro país, hemos revisado para esta sección el marco de la Unión Europea, del Reino Unido, de España e Italia.

Cabe mencionar que en estas jurisdicciones existen autoridades administrativas encargadas de ser garantes del derecho de protección de datos personales, las cuales han sido prolíficas en emitir directrices o recomendaciones que han resultado ser claves para avanzar en la delimitación y orientación en el uso de sistemas de videovigilancia y de reconocimiento facial, así como para abordar los desafíos particulares que presentan esas tecnologías frente al derecho de protección de datos personales. Por ejemplo, refiriéndose a las bases de legalidad habilitantes que están implicadas; la eliminación de imágenes luego de cierto periodo de tiempo; o la forma de almacenamiento de los datos tratados, entre un sinnúmero de otros aspectos.

Como veremos a continuación, en estas jurisdicciones está ya asentado el criterio de que la imagen de una persona es un dato personal que debe ser protegido, y que el uso de sistemas de videovigilancia y de reconocimiento facial pueden involucrar una afectación a los derechos fundamentales de respeto a la vida privada y de autodeterminación informativa. Adicional a esto, y como se observará en esta sección, dada la existencia del Reglamento General de Protección de Datos y otras normas particulares, se puede apreciar un entramado normativo y orgánico más avanzado que el que se contempla actualmente en nuestro país bajo la LPVP y que, por ejemplo, da cuenta de instituciones jurídicas que hoy en día no son aplicables en Chile, como la institución del interés legítimo como base habilitante del tratamiento de datos, o la regulación particular de los datos biométrico como una categoría especial de datos personales.

1. Unión Europea

A nivel de legislación vigente en la Unión Europea, podemos destacar dos instrumentos, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (el "Reglamento General de Protección de Datos" o "RGPD"); y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos (la "Directiva 2016/680")[13].

Por su parte, identificamos la existencia de un proyecto de reglamento que busca fijar normas en la Unión Europea en materia de inteligencia artificial y que, como veremos, presenta una importante vinculación con las tecnologías revisadas para este trabajo.

[13] Cabe destacar que estos instrumentos difieren entre sí debido a que el RGPD constituye un "reglamento" con fuerza normativa directa respecto de los Estados Miembros de la UE. Un reglamento no trata de armonizar los ordenamientos jurídicos de los países, sino que impone una norma única y aplicable de forma directa. Por su parte, la Directiva 2016/680 corresponde a una "directiva", lo cual es un instrumento que establece objetivos que todos los países de la UE deben cumplir a través de sus propias leyes nacionales. Para mayor información sobre esta distinción ver: https://europa.eu/european-union/law/legal-acts_es.

a) Reglamento General de Protección de Datos

En cuanto al RGPD[14] podemos señalar que desde su entrada en vigor en el año 2018 constituye la norma común aplicable en materia de datos personales en la Unión Europea. Se estructura en 99 artículos repartidos en 11 capítulos en los que se regulan cuestiones tales como los principios del tratamiento, bases de legalidad, medidas de seguridad de los datos, las evaluaciones de impacto relativa a la protección de datos, las transferencias internacionales de datos, las autoridades de control, el Comité Europeo de Protección de Datos, la responsabilidad por el incumplimiento, y el derecho de indemnización de los titulares.

En lo que respecta a los tratamientos de datos que acontecen en el contexto de sistemas videovigilancia y de sistemas de reconocimiento facial, podemos destacar especialmente las siguientes disposiciones del RGPD:

i. **Definiciones.** En primer lugar, resulta ilustrativo referirnos a las definiciones legales que establece este instrumento y que generan la base para hacer aplicable esta legislación al funcionamiento de los sistemas de videovigilancia y reconocimiento facial. En efecto, en su artículo 4, el RGPD define a los datos personales como *"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". Luego, define los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".* A partir de esto se observan que, bajo el RGPD, los datos biométricos son datos personales en cuanto identifiquen a una persona natural.

[14] El Reglamento General de Protección de Datos está disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR#d1e2051-1-1

ii. **Principios.** El RGPD establece una serie de principios de carácter transversal que deben ser aplicados por todos los responsables de datos, por lo que son de gran relevancia en el caso de tratamientos asociados a los sistemas de videovigilancia y de reconocimiento facial. Esta circunstancia ha sido señalada expresamente por el EDPB (2020) en sus documentos de orientación sobre estas tecnologías. Los principios del tratamiento están en el artículo 5 del RGPD y corresponden a los de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva.

iii. **Bases de legalidad.** El RGPD establece en su artículo 6 un conjunto de bases de legalidad en las cuales el tratamiento de datos personales se puede amparar, incluyendo el consentimiento del titular; si el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento; o si el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

iv. **Categorías especiales de datos[15].** Bajo el RGPD, los datos biométricos constituyen una categoría especial de datos. Su artículo 9 establece que el tratamiento de este tipo de datos para fines de identificar de manera única a una persona natural está, por regla general, prohibido salvo la concurrencia de ciertas excepciones, tales como la obtención del consentimiento explícito del titular[16]; o cuando el tratamiento sea necesario por razones de un interés público esencial[17].

[15] Las categorías especiales de datos o especialmente protegidos bajo el RGPD son equivalentes a la categoría de datos sensibles que establece la LPVP.

[16] Esto es aplicable salvo cuando el Derecho de la Unión o de los Estados miembros establezcan que la prohibición de tratamiento no puede ser levantada por el titular.

[17] En este caso, el tratamiento debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

v. **Evaluaciones de impacto de protección de datos.** El RGPD establece que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, genere un alto riesgo para los derechos de los titulares, el responsable deberá realizar, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales[18]. Sin perjurio de esto, el RGPD exige la realización de esta evaluación en ciertos casos particulares, como (i) en la evaluación sistemática y exhaustiva de aspectos personales de personas naturales que se base en un tratamiento automatizado; (ii) el tratamiento a gran escala de categorías especiales de datos (como los datos biométricos); y (iii) la observación sistemática a gran escala de una zona de acceso público. Según se advierte, estas causales de aplicación guardan gran similitud con ciertas implementaciones de sistemas de videovigilancia o de reconocimiento facial, lo cual genera un elemento de protección importante para los titulares que puedan verse expuestos a dichas tecnologías. Como veremos más adelante, esta figura ha sido considerada por las autoridades administrativas en la Unión Europea al referirse a estas tecnologías, siendo señalada como relevante a la hora de evaluar su implementación.

vi. **Derecho a no ser objeto de decisiones automatizadas.** Se establece que todo titular tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos en él o le afecte significativamente de modo similar. También se establecen ciertos casos en donde dicho derecho no aplicará[19].

vii. **Delegado de protección de datos.** Según establece el artículo 37 del RGPD, el responsable y el encargado (mandatario) del tratamiento deben designar a un delegado de protección de datos, entre otros casos, cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala. Esta hipótesis claramente hace subsumible el funcionamiento de sistemas de videovigilancia en el espacio público y de forma continua, y así lo ha indicado claramente el EDPB en sus documentos de orientación (2020).

[18] Conforme el artículo 35 numeral 7 del RGPD, las evaluaciones de impacto deben incluir, como mínimo: (i) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento; (ii) una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; (iii); una evaluación de los riesgos para los derechos y libertades de los titulares; y (iv) las medidas previstas para afrontar los riesgos.

[19] Por ejemplo, si la decisión automatizada es necesaria para ejecutar un contrato entre el titular y el responsable.

b) Directiva 2016/680

Respecto de la Directiva 2016/680[20], ésta tiene como principal finalidad garantizar la adecuada protección de los datos de las víctimas, testigos e investigados por la presunta comisión de delitos. Las disposiciones de la Directiva resultan aplicables a los procesos de registro de imágenes de video, en los que se pueden identificar a una persona, con el objetivo de prevenir, detectar o investigar delitos.

Para el cumplimiento de los mencionados fines, la Directiva 2016/680 se estructura en 65 artículos repartidos en 10 capítulos en los que se regulan cuestiones tales como los principios que rigen el tratamiento de estos datos, los derechos de los interesados, las obligaciones de los responsables y encargados del tratamiento de los datos, las medidas de seguridad en el tratamiento y la creación, por parte de cada Estado Miembro, de una autoridad independiente de control.

Dentro de las disposiciones de la Directiva 2016/680 identificamos las siguientes que, a nuestro juicio, pueden tener relación con los sistemas de videovigilancia y reconocimiento facial:

i. **Principios.** La Directiva 2016/680 recoge, en su artículo 4, un conjunto de principios aplicables al tratamiento de datos personales que determinan las obligaciones de los responsables y encargados de dicho tratamiento, y que han de ser recogidos por los Estados miembros en sus respectivos ordenamientos internos. Entre estos principios se encuentran los de licitud y lealtad; limitación de la finalidad; minimización; exactitud; limitación del plazo de conservación; seguridad y confidencialidad; responsabilidad; y protección de datos por defecto y desde el diseño.

[20] La Directiva 2016/680 se encuentra disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=FR#d1e1365-89-1

ii. **Categorías especiales de datos.** Al igual que en el RGPD, la Directiva 2016/680 reconoce a los datos biométricos dirigidos a identificar de manera unívoca a una persona física como una categoría especial de datos personales. En su artículo 10, establece que el tratamiento de esta clase de datos solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando (i) lo autorice el Derecho de la Unión o del Estado miembro; (ii) sea necesario para proteger los intereses vitales del interesado o de otra persona física; o (iii) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos. Se puede observar aquí una diferencia con la prohibición general que establece el RGPD y que indicamos anteriormente[21].

iii. **Derechos reconocidos a los titulares de datos.**
Derecho de acceso (art.14): el titular tiene derecho a obtener del responsable confirmación sobre si se están tratando sus datos; y en caso positivo, tiene derecho de acceso a dichos datos y a determinadas informaciones recogidas en el mismo precepto. Este derecho puede ser limitado por el Estado miembro de conformidad con el artículo 15.
Derecho de rectificación o supresión de datos personales y limitación de su tratamiento (art. 16): este derecho puede ser limitado por el Estado miembro, de conformidad con lo dispuesto en el artículo 16.4.
Derecho de información: Para facilitar el ejercicio de estos derechos, los artículos 12 y 13 establecen una serie de obligaciones de información del responsable del tratamiento.
Derechos en relación con decisiones individuales no únicamente automatizadas (art. 11): El interesado es titular de estos derechos en relación con los datos obrantes en los ficheros jurisdiccionales de procesos penales.

iv. **Autoridad de Control.** La normativa otorga gran relevancia al papel de la autoridad de control, a quien atribuye la misión de *"supervisar la aplicación de la presente Directiva 2016/680, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos personales y de facilitar la libre circulación de datos personales en la Unión"* (art. 41.1), concretando sus funciones en el artículo 46.

[21] Ver: Mathias Avocats (28 de febrero de 2020). Facial Recognition Regulation in the EU: a risk of legal fragmentation? https://www.avocats-mathias.com/actualites/facial-recognition.

c) Proyecto de reglamento sobre inteligencia artificial

Además de los dos instrumentos vigentes señalados, quisiéramos también destacar la Propuesta de regulación de la Comisión Europea para el Establecimiento de Normas Armonizadas en materia de Inteligencia Artificial[22] ("Ley de Inteligencia Artificial"), presentada el 21 de abril de 2021[23], y que podría constituir el primer marco normativo sobre sistemas de inteligencia artificial (IA) en el mundo. Esta propuesta, que tiene por objetivo asegurar los derechos fundamentales y promover la innovación en esta área, debe ahora ser revisada por el Parlamento Europeo y el Consejo para su debate.

En la propuesta se regulan diversas materias, incluyendo un ámbito de aplicación compuesto por proveedores y usuarios de sistemas de IA, así como proveedores y usuarios de sistemas de IA ubicados en terceros países y en donde el producto (output) de dichos sistemas sea utilizado en la UE[24].

La propuesta incluye una definición amplia de "sistema de IA", entendiendo por tal *"un software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"*. Se ha intentado que la definición sea tecnológicamente neutra y a prueba de futuro. En el Anexo I se incluye machine learning, deep learning, enfoques lógicos y basados en conocimiento, enfoques estadísticos, entre otros.

En términos normativos, la propuesta está basada desde una perspectiva de riesgos reconociendo tres clases de sistemas de IA: **sistemas de IA prohibidos por generar un riesgo inaceptable que viola los derechos fundamentales; sistemas de IA que generan un alto riesgo (high risk); y sistemas de IA que generan un riesgo bajo o mínimo.**

[22] Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1

[23] Este Proyecto forma parte de la estrategia europea sobre datos (European Strategy for data), disponible en https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[24] Las secciones de la Propuesta son: Título I Disposiciones Generales; Título II Prácticas prohibidas de Inteligencia Artificial; Título III Sistemas de IA de alto riesgo; Título IV Obligaciones de transparencia para ciertos sistemas de IA; Título V Medidas en apoyo de la innovación; Título VI Gobernanza; Título VII Base de datos europea para sistemas de IA de alto riesgo "stand-alone"; Título VIII Monitoreo post comercialización, entrega de información y vigilancia de mercado; Título IX Códigos de Conducta; Título X Confidencialidad y penas; Título XI Delegación de poder y procedimiento del Comité; y Título XII Provisiones finales.

i. Sistemas de IA prohibidos

En relación al primer grupo, diversas implementaciones de IA estarán prohibidas, incluyendo el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley (enforcement), salvo y en la medida que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes: (i) la búsqueda selectiva de posibles víctimas de un delito; (ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista; y (iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo[25], para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el derecho de dicho Estado miembro.

El uso de esta clase de sistemas en alguna de las hipótesis señaladas debe considerar y cumplir con una serie de elementos antes de su implementación, incluyendo la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente. Por último, cabe destacar que la propuesta agrega que el uso de sistemas de identificación biométrica en estos casos deberá tener en cuenta la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se producirá de no utilizarse el sistema. Agrega que también deberán considerarse las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular, la gravedad, probabilidad y magnitud de dichas consecuencias. Por su parte, señala que este uso deberá cumplir salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales.

[25] Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1). Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32002F0584

ii. Sistemas de IA de alto riesgo

En cuanto a los sistemas de IA que generan "alto riesgo", estos no se encuentran definidos, pero se establecen criterios para determinarlos. Quedarían comprendidos en esta clase los sistemas de IA empleados para la identificación biométrica remota "en tiempo real" y "posterior" de personas naturales; los empleados por las fuerzas policiales; los utilizados en procesos de migración, asilo y control fronterizo (ej. para control de la autenticidad de documentos de viaje); los utilizados en la administración de justicia; entre varios otros usos.

Se establecen reglas especiales para el uso e implementación de estos sistemas, incluyendo un sistema obligatorio de gestión de riesgos; reglas para el uso y manejo de datos para minimizar riesgos de discriminación; reglas para la documentación y manejo de archivos; adecuada supervisión humana; y reporte de incidentes.

[25] Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1). Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32002F0584

d) Supervisor Europeo de Protección de Datos y Comité Europeo de Protección de Datos

A nivel de órganos administrativos vinculados con la protección de datos personales en la Unión Europea destaca el Supervisor Europeo de Protección de Datos (*European Data Protection Supervisor* o EDPS)[26], el cual corresponde a una autoridad de control independiente, cuyo objetivo principal es garantizar que las instituciones y organismos de la Unión Europea respeten el derecho a la privacidad y la protección de datos. Por su parte, también podemos destacar el Comité Europeo de Protección de Datos (*European Data Protection Board* o EDPB)[27] que nombramos anteriormente, y que corresponde a un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en la Unión Europea y promueve la cooperación entre las autoridades de protección de datos. El EDPB está compuesto por representantes de las autoridades nacionales de protección de datos y el Supervisor Europeo de Protección de Datos.

Respecto a guías de orientación extendidas por estos organismos relativas a las tecnologías que estamos revisando, destaca el documento "*The EDPS video-surveillance guidelines*" que fue publicado el año 2010 por el EDPS. A este documento le siguió el informe de seguimiento "Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines" que publicó ese organismo el año 2012.

En lo sustantivo, el EDPS (2021) ha señalado que las cámaras de videovigilancia deben dirigirse a atender problemas de seguridad específicamente identificados, minimizando la recopilación de imágenes irrelevantes, lo cual lo vincula al principio de minimización de datos. Esto no solo reduciría las intrusiones a la privacidad, sino que también permitirá un uso más específico y eficiente de la videovigilancia. Sobre el periodo de retención, el EDPS ha indicado que, si bien la instalación de cámaras puede estar justificado bajo propósitos de seguridad, la eliminación automática y oportuna de las captaciones es esencial y que todas las instituciones de la Unión deben tener políticas claras sobre el uso de video vigilancia, incluyendo el potencial almacenamiento (EDPS, 2021)[28].

[26] Su sitio web es: https://edps.europa.eu/_en

[27] Su sitio web es: https://edpb.europa.eu/edpb_es

[28] El EDPS también se ha referido al tecnología de reconocimiento de emociones en: https://edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf

En cuanto al EDPB, podemos destacar el documento del año 2020 sobre "Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video. Versión 2.0". Este documento se refiere a un sinnúmero de aspectos relacionados con el tratamiento de datos mediante sistemas de videovigilancia, incluyendo los requisitos de licitud del tratamiento de datos; la divulgación de imágenes a terceros; el tratamiento de categorías especiales de datos; y obligaciones de transparencia e información. Sobre algunos aspectos particulares relativos a la licitud del tratamiento y al tratamiento de categorías especiales de datos, podemos destacar los siguientes planteamientos que realiza esta autoridad:

i. Conforme al RGPD, antes de utilizarse un sistema de videovigilancia se deben especificar de forma detallada y por escrito las **finalidades del tratamiento.** El EDPB (2020) señala que la videovigilancia basada en la mera finalidad de "seguridad" no es suficientemente específica para cumplir con el artículo 5, numeral 1, literal b) del RGPD, además de ser contrario al principio de que los datos se deben tratar de forma lícita, leal y transparente.

ii. Sobre las **bases de legalidad**, establece que cada una de las bases señaladas en el artículo 6, numeral 1, del RGPD[29], pueden proporcionar una base de legalidad para el tratamiento de datos de videovigilancia. Sin embargo, señala que, en la práctica, las bases que con "más probabilidad" se van a utilizar son la referida al interés legítimo, y aquella relativa al tratamiento que es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.

iii. En cuanto al **principio de minimización de datos**, establece que antes de instalar un sistema de videovigilancia, el responsable debe examinar si dicha medida es, en primer lugar, apta para lograr el objetivo deseado y, en segundo lugar, si es adecuada y necesaria para su fin. Solo debe optarse por la videovigilancia si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios menos intrusivos.

[29] Por ejemplo, el consentimiento del titular; o si el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

iv. En el caso de **categorías especiales de datos** que sean tratadas mediante un sistema de videovigilancia, el responsable debe identificar una excepción para el tratamiento de esa categoría de datos en virtud del artículo 9 del RGPD, así como una base de legalidad conforme estable el artículo 6 de ese reglamento[30].

v. Respecto del **uso de datos biométricos en el contexto de sistemas de reconocimiento facial**, el EDPB (2020) señala que dicho tratamiento conlleva elevados riesgos para los derechos de los titulares, siendo fundamental que el uso de tal tecnología respete los principios de licitud, necesidad, proporcionalidad y minimización de datos.

vi. En cuanto a los **derechos de los titulares**, se señala que todos los derechos establecidos en el RGPD aplican al tratamiento de datos personales con videovigilancia. En relación al derecho de acceso, podría ocurrir que en una grabación se capte un variado número de titulares, lo que generaría que su divulgación afectaría negativamente los derechos de titulares distintos al que ejerce el derecho. En dicho caso, el responsable no debe entregar las imágenes, sino que aplicar medidas técnicas para cumplir la solicitud, por ejemplo, editando las imágenes con enmascaramiento o codificación.

[30] Esto es indicado en un sentido similar por Carey, 2020.

2. Reino Unido

En Reino Unido se reconocen varios cuerpos normativos que pueden resultar atingentes a la videovigilancia y los sistemas de reconocimiento facial desde un punto de vista de datos personales. A continuación, hacemos un breve análisis de los más relevantes

a) Data Protection Act 2018

En primer lugar, resulta relevante mencionar la Data Protection Act de 2018[31] ("DPA 2018") que entró en vigor en mayo de ese mismo año. Esta norma está dividida en siete partes correspondientes a: Parte I: Preliminar; Parte 2: Tratamiento general; Parte 3: Tratamiento sobre cumplimiento de la ley (Law enforcement processing); Parte 4: Tratamiento de servicios de inteligencia; Parte 5: Comisionado de la Información (correspondiente a la autoridad administrativa, y al cual nos referiremos más adelante); Parte 6: Cumplimiento; y Parte 7: Anexo y disposiciones finales.

Bajo su normativa, si las imágenes que sean tratadas permiten la identificación de personas, entonces la DPA 2018 es aplicable, incluso en el caso de que se capten personas desconocidas a cuya identificación pueda llegarse mediante un cruce de datos. Este punto es particularmente relevante en relación al uso de tecnologías de reconocimiento automático de números de placas automovilísticas o de sistemas reconocimiento facial, al hacerse aplicables las reglas de protección de datos en la materia (Carey, 2015).

El **tratamiento de categorías especiales de datos en Reino Unido** requiere efectuarse conforme una base de legalidad del artículo 6 del RGPD, y una de las excepciones que establece el artículo 9 de ese reglamento. Además de esto, la DPA 2018 establece condiciones adicionales para el tratamiento de esta clase de datos, que se indican en su Anexo 1 (*Schedule 1*). Por su parte, existen condiciones específicas que solo gobiernan el tratamiento de datos por parte de autoridades competentes, incluyendo a la policía y otras autoridades dedicadas al cumplimiento de la ley (*law enforcement*) en la Parte 3 del DPA 2018; así como el MI5, MI6 y el GCHQ[32] en la Parte 4 de esa norma.

[31] Disponible en: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[32] Estos organismos de inteligencia son el Security Service (Servicio de Seguridad), el Secret Intelligence Service (Servicio de Inteligencia Secreto) y el Goverment Communications Headquarters (Cuartel General de Comunicaciones del Gobierno).

Para ser consistentes con las aplicaciones más habituales de videovigilancia y reconocimiento facial en Chile, nos concentraremos en la Parte 3 de la DPA 2018. Conforme su estructura, cabe señalar que el tratamiento de cualquier dato personal por parte de una autoridad competente para fines de enforcement está regulado por dicha sección, no solo los datos sobre ofensas criminales. En estas autoridades se comprenden las policías, los ministerios, el Comisionado de la Información, las cortes, etc. Por su parte, el concepto de "Law enfocement" se define de manera amplia como los fines de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública.

El tratamiento que realicen estas autoridades está sujeto, en general, a los mismos seis principios básicos de tratamiento que establece el artículo 5 del RGPD. Por su parte, el tratamiento de ciertos datos sensibles, como de datos que revelen el origen racial o étnico, o los datos biométricos, requiere cumplir con un estándar más alto por parte de las autoridades. En esos casos, el tratamiento puede ocurrir solo en dos casos:

i. Cuando el titular haya dado su consentimiento y el responsable tenga implementado un documento de política apropiado; o

ii. Cuando el tratamiento sea estrictamente necesario para el propósito de cumplimiento de la ley (*law enforcement*); cumple con una de las condiciones del Anexo 8 (*Schedule*); y el responsable tiene implementado un documento de política apropiado. Las condiciones del Anexo 8, que se asemejan a algunas de las condiciones del artículo 9 del RGPD, incluyen **(i)** fines judiciales y estatutarios; **(ii)** la protección de los intereses vitales de los individuos; **(iii)** datos personales que se encuentran en el dominio público; **(iv)** perseguir o defender acciones legales y la actuación de las cortes en sus atribuciones judiciales; **(v)** prevención del fraude; y **(vi)** archivo en el interés público, investigación científica o histórica, o fines estadísticos.

Los requisitos aplicables al "documento de política apropiado" se encuentran en la sección 42 de la DPA 2018.

b) Protection of Freedoms Act 2012 y el Surveillance Camera Code of Practice

La Protection of Freedoms Act de 2012[33] (la "PFA 2012") es la normativa que crea al Comisionado de Cámaras de Vigilancia (Surveillance Camera Commissioner - SCC) y que ordena la elaboración del Surveillance Camera Code of Practice. Para efectos de este trabajo, destacamos las Partes 1 y 2 de esta ley[34].

La Parte 1 de la PFA 2012 se refiere a la regulación de los datos biométricos. En su capítulo 1 se trata la destrucción, retención y uso de huellas digitales y otros; y en su capítulo 2 se regula la protección de información biométrica de niños en los colegios.

Luego, en la Parte 2 de la ley se regula la vigilancia. El Capítulo 1 se refiere a la regulación para sistemas CCTV y otras tecnologías de cámaras de vigilancia. Las disposiciones de esta norma se refieren al uso de sistemas de cámara de vigilancia en espacios públicos por parte de las autoridades en Inglaterra y Gales. Luego, la sección 29(1) es la que requiere al Secretario de Estado (Secretary of State) la preparación de un código de conducta (Surveillance Camera Code of Practice) que contenga orientación acerca de los sistemas de cámaras de vigilancia[35]. Conforme la sección 33, las autoridades relevantes, incluyendo las fuerzas de policía, están obligadas a tener en cuenta el código de conducta en el desarrollo de cualquier actividad que tenga relación con éste.

[33] Norma disponible en: https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

[34] Las demás secciones de la PFA 2012 son: Parte 3, relativa a la protección de la propiedad de las acciones desproporcionadas de enforcement; Parte 4, poderes antiterroristas; Parte 5, salvaguardas para grupos vulnerables y registros criminales; Parte 6, Acceso a la información y protección de datos; y Parte 7, Misceláneos.

[35] Este código debe incluir: (i) consideraciones sobre cómo usar circuitos cerrados de televisión (CCTV); (ii) tipos de sistemas o aparatos; (iii) estándares técnicos; (iv) ubicaciones para esos sistemas o aparatos; (v) publicación de información; (vi) estándares aplicables a personas usando o manteniendo dichos sistemas o aparatos; (vii) estándares aplicables a personas usando o procesando información obtenida por esos sistemas; (viii) acceso o divulgación a dicha información; y (ix) procedimientos para reclamos o consultas.

El Surveillance Camera Code of Practice entró en vigor en el año 2013 y, a la fecha de este trabajo, se encontraba en proceso de reforma luego de un periodo de consulta pública que concluyó en septiembre de 2021[36]. El proceso de reforma tuvo como origen el fallo de la Corte de Apelaciones de Inglaterra y Gales sobre tecnología de reconocimiento facial "R (Bridges) v-Chief Constable of South Wales Police & Others", que revisamos en más detalle más adelante. El Código vigente contiene los siguientes doce principios orientadores para el funcionamiento de sistemas de cámaras de vigilancia:

i. El uso de un sistema de cámaras de vigilancia debe ser siempre para un propósito específico que persiga un objetivo legítimo y sea necesario para satisfacer una necesidad urgente identificada.

ii. El uso de un sistema de cámaras de vigilancia debe tener en cuenta su efecto sobre las personas y su privacidad, con revisiones periódicas para garantizar que su uso sigue estando justificado.

iii. Debe existir la mayor transparencia posible en el uso de un sistema de cámaras de vigilancia, incluido un punto de contacto publicado para acceder a la información y las quejas.

iv. Debe haber una clara responsabilidad y rendición de cuentas por todas las actividades del sistema de cámaras de vigilancia, incluidas las imágenes y la información recopilada, almacenada y utilizada.

v. Deben existir reglas, políticas y procedimientos claros antes de que se utilice un sistema de cámaras de vigilancia, y estos deben comunicarse a todos los que deban cumplirlos.

vi. No se deben almacenar más imágenes e información que la estrictamente necesaria para el propósito declarado de un sistema de cámaras de vigilancia, y dichas imágenes e información deben eliminarse una vez que se hayan cumplido sus propósitos.

[36] Un borrador del código actualizado se puede encontrar en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_.pdf

vii. El acceso a las imágenes e información retenidas debe restringirse, y deben existir reglas claramente definidas sobre quién puede obtener acceso y con qué propósito se otorga dicho acceso; la divulgación de imágenes e información solo debe tener lugar cuando sea necesario para tal fin o para fines de aplicación de la ley.

viii. Los operadores de sistemas de cámaras de vigilancia deben considerar cualquier estándar operativo, técnico y de competencia aprobado que sea relevante para un sistema, su propósito y funcionamiento.

ix. Las imágenes y datos del sistema de cámaras de vigilancia deben estar sujetos a las medidas de seguridad adecuadas para protegerlos contra el acceso y uso no autorizados.

x. Debe haber mecanismos de revisión y auditoría efectivos para garantizar que los requisitos legales, las políticas y las normas se cumplan en la práctica, y deben publicarse informes periódicos.

xi. Cuando el uso de un sistema de cámaras de vigilancia persigue un objetivo legítimo y existe una necesidad imperiosa en su uso, debe utilizarse de la manera más eficaz para respaldar la seguridad pública y la aplicación de la ley con el objetivo de procesar imágenes e información de valor probatorio.

xii. Toda información utilizada de un sistema de cámaras de vigilancia que se coteje con una base de datos de referencia para fines de comparación debe ser precisa y mantenerse actualizada.

c) Oficina del Comisionado de la Información y Comisionado de Cámaras de Vigilancia

A nivel de **órganos administrativos relevantes en esta materia en el Reino Unido**, podemos identificar a la Oficina del Comisionado de la Información (*Information Comissioner's Office - ICO*), que tiene atribuciones y responsabilidades específicas bajo la DPA 2018[37]; así como al Comisionado de Cámaras de Vigilancia, y que corresponde al regulador en materia de cámaras de vigilancia utilizadas por la policía. Este tiene atribuciones bajo la sección 34 de la PFA 2012[38] que están destinadas a asegurar el cumplimiento del *Surveillance Camera Code of Practice*, así como de regular el uso de cámaras en conjunto con tecnología de reconocimiento facial.

Respecto a guías de orientación extendidas por estos organismos, destaca aquella denominada "*In the picture: A data protection code of practice for surveillance cameras and personal information. Version 1.2*" publicada por la ICO, y que contiene un conjunto de recomendaciones y buenas prácticas aplicadas a la videovigilancia. Bajo esta guía, la ICO establece que se deben atender a las siguientes reglas y estándares (ICO, 2017):

i. Antes de implementar un mecanismo de videovigilancia, el responsable del tratamiento debe efectuar una **evaluación de impacto en materia de protección de datos** (Carey, 2015). Fruto de la evaluación, se debe descartar el uso de cámaras si el fin es alcanzable por otros medios menos intrusivos. La ICO señala el siguiente ejemplo: si la cámara tenía por objeto prevenir los destrozos nocturnos a automóviles en un estacionamiento, debe considerarse si basta con mejorar la luminosidad del lugar para prevenir los daños.

ii. Luego de ello, debe **comunicar a la ICO cuál es la finalidad** para el registro de imágenes (por ejemplo, la prevención y persecución de delitos). La omisión de la comunicación tiene como consecuencia la ilegitimidad del tratamiento de datos (Carey, 2015).

iii. Las cámaras deben establecerse en **lugares** que minimicen la captación de imágenes, resguardando una "suficiente calidad" y evitando aquellos lugares en donde los individuos pudieren tener mayores expectativas de privacidad, como baños o camarines. Asimismo, el responsable tiene que informar de la grabación de imágenes. Los avisos o letreros no deben tener un texto excesivo, deben dejar claro que se está grabando y que el titular puede ejercer sus derechos ARCO (Carey, 2015).

[37] Su sitio web es https://ico.org.uk/.

[38] Su sitio web es https://www.gov.uk/government/organisations/surveillance-camera-commissioner

iv. El registro de imágenes debe estar **limitado en el tiempo** a la finalidad previamente declarada. Su almacenamiento debe asegurar la calidad e integridad del dato y garantizar la seguridad de la información. En este sentido, la ICO recomienda, en su caso, la encriptación de los datos. Cuando la encriptación no sea posible, entonces deben buscarse otras alternativas de seguridad.

v. El titular de la imagen tiene un **derecho de acceso a la grabación**. El responsable debe habilitar un procedimiento para hacerlo efectivo y debe capacitar al personal a cargo de estas solicitudes. En esta materia, debe ser especialmente diligente en difuminar o remover las imágenes de terceros (Carey, 2015).

vi. Respecto de **solicitudes de acceso a información pública** (bajo la Freedom of Information Act o FOIA), la ICO ha desarrollado los siguientes criterios: Si se trata de una solicitud del titular de la imagen, entonces se aplican las reglas de habeas data bajo la normativa de protección de datos personales. Si se trata de una solicitud de imágenes de terceros, entonces la divulgación solo puede efectuarse si no viola los principios de protección de datos personales. En particular: **(i)** la información puede ser reservada si se trata de una persona identificada o identificable; **(ii)** al decidir si corresponde la publicidad de la información, se debe evaluar cuál era la expectativa de privacidad del titular, qué revelará la información requerida, y el legítimo interés público sobre la información; y **(iii)** si es posible la divisibilidad de la información, anonimizando los datos personales de terceros, entonces se podría favorecer dicha medida frente a la reserva de la información.

vii. En relación al **periodo de almacenamiento** mínimo o máximo de las captaciones, la ICO expone que este debe reflejar los intereses de la organización al momento de la captura de la información. En aquellos casos en que la retención de la información no cumpla con el propósito con el cual se captó y retuvo, esta debe ser eliminada. Además, se dispone que no se debe conservar la información por más tiempo del estrictamente necesario para cumplir con los objetivos del almacenamiento.

Además de esta guía del año 2017, la ICO también ha publicado la guía "The use of live facial recognition technology by law enforcement in public places" del año 2019[39]. Entre su contenido más relevante, la guía requiere que el tratamiento bajo reconocimiento facial sea estrictamente necesario; que la medida implementada sea específica y limitada en el tiempo; que el responsable explique cómo la tecnología de reconocimiento facial será efectiva para el cumplimiento de la ley; y, por último, en el caso de listas de vigilancia (watchlists), éstas deben ser de un tamaño limitado, creadas bajo los principios de protección de datos, e incluir imágenes precisas y verificables.

Por último, de la ICO también advertimos la guía *"The use of live facial recognition technology in public places"* de junio de 2021. Respecto de esta, podemos destacar la identificación de una serie de problemáticas clave sobre protección de datos relacionadas con el uso de tecnología de reconocimiento facial en vivo. Entre estas, la guía enumera: **(i)** la gobernanza de los sistemas de reconocimiento facial, incluyendo por qué y cómo son utilizados; **(ii)** la recolección automática de datos biométricos a una velocidad y escala sin justificación clara; **(iii)** la falta de elección y control de parte de los individuos; **(iv)** la transparencia y los derechos de los titulares; (v) la efectividad y la precisión estadística de los sistemas; **(vi)** el potencial de sesgos y discriminación; **(vii)** la gobernanza de listas de vigilancia (watchlists) y procesos de escalada; **(viii)** el tratamiento de datos de niños y adultos vulnerables; y **(ix)** la potencialidad de impactos masivos y no anticipados para individuos y sus comunidades (ICO, 2021)[40].

En el caso del Comisionado de Cámaras de Vigilancia, este también ha publicado diversas guías de orientación, como por ejemplo "*Facing the Camera. Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*" publicada en noviembre de 2020[41]. Esta guía tomó en cuenta el fallo de la Corte de Apelaciones "*R (Bridges) v-Chief Constable of South Wales Police & Others*", y se refiere a diversos aspectos que podrían asistir a las fuerzas policiales de Inglaterra y Gales en la operación en espacios públicos de sistemas de videovigilancia junto con tecnología de reconocimiento facial. En términos de contenido, la guía se refiere a biometría, equidad y ética; derechos humanos y el marco legal; gobernanza, aprobaciones, listas de vigilancia y decisiones humanas; integridad y uso de material como evidencia; involucramiento del público y entrega de información; y certificación y accountability (SCC, 2020).

[39] Esta guía está disponible en: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

[40] Esta es una guía bastante completa que también hace referencia a aspectos particulares como la vigilancia y las listas de vigilancia; la realización de marketing directo; la realización de evaluaciones de impacto de protección de datos personales; obligaciones de transparencia que debe cumplir el responsable; entre otros aspectos.

[41] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

3. España

En materia constitucional, la videovigilancia es abordada en España fundamentalmente desde dos derechos: el derecho a la intimidad personal y familiar, y el derecho a la propia imagen. Respecto al primero, se entiende como un "ámbito propio y reservado" de las personas y que es necesario para garantizar una "calidad mínima de vida humana[42]". Como derecho, garantiza un ámbito reservado, excluido de la acción y el conocimiento de los demás. Respecto al segundo –el derecho a la propia imagen– se protege la facultad de *"disponer y decidir sobre el uso de la propia imagen, esto es, de los datos por los que una persona se identifica públicamente"*. En este punto, se requiere el consentimiento del titular de la imagen para su tratamiento por parte de terceros. Es un derecho autónomo del derecho a la intimidad (Gutiérrez, 2015, p. 323-324; Díez-Picazo, 2003, p. 262). Esto implica que, pese a que puede haber registros de imágenes que se efectúen en lugares abiertos al público, *"a la hora de valorar la reproducción y utilización de la imagen de las personas, lo decisivo es su consentimiento"* (Díez-Picazo, 2003, p. 262)[43].

Por su parte, cabe destacar que en España se ha entendido que la protección de las personas en relación con el tratamiento de sus datos personales puede derivarse del artículo 18.4 de la Constitución española, que establece que *"4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

A nivel de regulación legal sobre las materias de este trabajo, podemos observar en España la existencia de una regulación general compuesta por la Leyes Orgánicas 4/2015 y 4/1997; así como la de una regulación específica de protección de datos personales consistente en la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

[42] STCE 231/1988 de 2 de diciembre.

[43] Constitucionalmente, la videovigilancia se entiende como una injerencia en los derechos antes individualizados. Si bien la videovigilancia en espacios públicos no se estima una violación a la intimidad de las personas, antes existían dudas de su legitimidad legal por parte de las fuerzas y cuerpos de seguridad que hoy pueden considerarse superadas. En cualquier caso, al tratarse de una medida de control público sobre los particulares se encuentra sometida al "principio de interdicción de la arbitrariedad" y debe satisfacer el principio de proporcionalidad (Díez-Picazo, 2003, p. 257-258).

a) Ley Orgánica 4/2015 de protección de la seguridad ciudadana y Ley Orgánica 4/1997 sobre utilización de videocámaras por parte de las Fuerzas y Cuerpos de seguridad

En España existiría una autorización legal explícita de uso de videocámaras. El art. 22 de la Ley Orgánica 4/2015[44] dispone que la autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.

Por su parte, la Ley Orgánica 4/1997[45] tiene por objeto regular la utilización -por las Fuerzas y Cuerpos de Seguridad- de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

En su artículo 2 establece que la captación, reproducción y tratamiento de imágenes y sonidos, en los términos previstos en la ley, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Luego señala que “sin perjuicio de las disposiciones específicas de la ley”, el tratamiento automatizado se regirá por la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Advirtiendo que dicha ley está derogada, asumimos que la redirección procede en relación de la Ley Orgánica 3/2018.

Finalmente, destacamos que la Ley Orgánica 4/1997 regula una serie de materias que son relevantes para le videovigilancia a nivel de autoridades de fuerza y seguridad, incluyendo: autorización para instalaciones fijas; autorizaciones de videocámaras móviles; principios de utilización de las videocámaras; conservación de grabaciones; derechos de los interesados; infracciones y sanciones; y recursos.

[44] Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-3442

[45] Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1997-17574

b) Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales ("LOPDGDD")

Conforme la legislación española, la recolección y uso de la imagen de las personas es un tratamiento datos personales que se encuentra regulado por la LOPDGDD[46]. En efecto, el artículo 22 de esta ley se refiere expresamente a los tratamientos con fines de videovigilancia, estableciendo -en términos generales- los siguientes requisitos y condiciones:

i. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

ii. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada anteriormente. No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

iii. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

[46] Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&tn=2&p=20210527

iv. El deber de información del artículo 12 del RGPD se entenderá cumplido mediante la colocación de un dispositivo informativo en un lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 de ese reglamento. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

v. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el RGPD y la LOPDGDD.

c) Agencia Española de Protección de Datos

A nivel de órganos administrativos relevantes en esta materia, podemos identificar la Agencia Española de Protección de Datos (AEPD), que corresponde a la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de la ciudadanía en España[47].

Por su parte, también cabe destacar la existencia del Consejo de Transparencia y Buen Gobierno[48], que es la autoridad encargada de supervisar el cumplimiento de la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno.

Respecto a guías de orientación o similares extendidas por estos organismos, destaca la "Guía sobre el uso de videocámaras para seguridad y otras finalidades" que la AEPD publicó el año 2018[49]. Sobre la seguridad pública y las cámaras de videovigilancia, la AEPD establece que ellas deben responder a la finalidad consistente en la seguridad pública. Luego, al tratar la proporcionalidad, hace mención expresa al principio de minimización de datos, así, indica que este apunta a que "los datos objeto de tratamiento sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados" (AEPD, 2018, p. 8). Cabe observar que, respecto al plazo de almacenamiento de captaciones de videovigilancia, la AEPD señala que el plazo será de un mes (AEPD, 2018).

Por otro lado destacamos el documento "Nota Técnica: 14 equívocos con relación a la identificación y autenticación biométrica" por su valor pedagógico. Conforme señala la AEPD, este documento tiene por objeto hacerse cargo de un conjunto de concepciones equivocadas que han surgido a partir de la popularización del uso de datos biométricos para fines de identificación y autenticación. En este contexto, el documento contiene las siguientes aclaraciones (AEPD, 2020):

[47] Su sitio web es: https://www.aepd.es/es

[48] Su sitio web es: https://www.consejodetransparencia.es/.

[49] Respecto de entidades privadas, cabe señalar que la AEPD publicó recientemente un informe sobre el uso de sistemas de reconocimiento facial por parte de empresas de seguridad privada (N/REF: 010308/2019). En este, establece como una de sus bases que la existencia de un interés legítimo no habilita a cualquier tipo de tratamiento de datos. La Agencia dispone que el reconocimiento facial se engloba dentro de los datos biométricos y que, el tratamiento de estos requiere que esté amparado en una norma de derecho europeo o nacional (esta última debe tener rango de ley). Este informe se encuentre disponible en: https://www.aepd.es/es/documento/2019-0031.pdf.

i. **El uso de datos biométricos es más intrusivo que otros sistemas de identificación/autenticación.** A partir de los datos biométricos se pueden derivar datos del sujeto como su raza o género, su estado emocional, enfermedades, discapacidades, características genéticas y consumo de sustancias.

ii. **La identificación/autenticación biométrica no siempre es precisa.** A diferencia de los procesos basados en contraseñas o certificados, la identificación/autenticación biométrica se basa en probabilidades. Existe una determinada tasa de falsos positivos y falsos negativos. Estas tasas son mayores cuanto menos preciso sea el equipo de captura de datos y dependen de las condiciones de recolección.

iii. **La identificación/autenticación biométrica no siempre es adecuada para todas las personas.** Algunas personas no pueden utilizar determinados tipos de biometría porque sus características físicas no son reconocidas por el sistema.

iv. **El proceso de identificación/autenticación biométrica se puede burlar.** Existen procedimientos y técnicas que permiten burlar sistemas de autenticación biométrica y asumir la identidad de otra persona.

v. **La información biométrica está expuesta.** La mayoría de las características biométricas de una persona están expuestas y se pueden capturar a distancia, ya que no se oculta habitualmente el rostro, las huellas, la forma de moverse, la huella térmica, etc.

4. Italia

En Italia no se aprecia la existencia de una legislación especial que regule la implementación de dispositivos de videovigilancia ni de reconocimiento facial. En este contexto, se advierte como normativa relevante la normativa general de protección de datos personales correspondiente al Código de Privacidad[50], que armoniza la regulación con el RGPD en virtud del Decreto Legislativo 101/2018 y que modificó una serie de disposiciones del Decreto Legislativo 196/2003.

A nivel de órganos administrativos, se identifica a la Autoridad de Protección de Datos Italiana (*Garante per la protezione dei dati personali - GPDP*), que es una autoridad administrativa establecida originalmente por la Ley N°675 de 31 de diciembre de 1996 sobre protección de las personas y otros sujetos en relación con el procesamiento de datos personales, cuya función es ser la autoridad de control en materia de datos personales en Italia.

En este orden de cosas, resulta relevante la posición que ha tomado la GPDP sobre este tema, donde podemos destacar fundamentalmente dos instrumentos. En primer lugar, una guía sobre videovigilancia publicada en diciembre del año 2020 en formato de "preguntas frecuentes" (FAQ)[51] y que está disponible en el sitio web de la autoridad. Esta guía hace referencias directas a la normativa que establece el RGPD. En segundo lugar, destacamos la "Decisión sobre Videovigilancia" del año 2010[52] (Video Surveillance Decision) en la que se consignan los principales estándares aplicables en la materia. Esto, sin perjuicio de las leyes especiales que tienen normas particulares sobre videovigilancia.

En relación a la guía de preguntas frecuentes, destacamos los siguientes criterios señalados por la autoridad italiana:

[50] Disponible en: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.8

[51] Disponible en: https://www.garanteprivacy.it/temi/videosorveglianza

[52] Este documento se refiere a ciertos principios generales; al deber de información del responsable; a los requisitos especiales para ciertos tipos de vigilancia; a medidas de seguridad, al plazo de almacenamiento de las imágenes; y a los derechos de los titulares de datos. Está disponible en: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1734653

i. **Sobre las normas aplicables al instalar un sistema de videovigilancia.** La GPDP indica que, para esto, se requiere dar cumplimiento a la normativa sobre protección de datos, así como también a las demás disposiciones aplicables de la ley como, por ejemplo, las normas de derecho civil y penal sobre injerencia ilícita en la vida privada, o sobre el control remoto de los trabajadores. Agrega que esta actividad debe llevarse a cabo siguiendo el principio de minimización de datos en lo que respecta a la elección de métodos de disparo, localización y gestión de las diversas fases de procesamiento. Los datos tratados deben ser pertinentes y no excesivos con respecto a las finalidades perseguidas.

ii. **Sobre la información a las personas que pasan por el área cubierta por el sistema.** La autoridad señala que las personas siempre deben ser informadas de que están a punto de acceder a un área de videovigilancia, incluso durante eventos y espectáculos públicos e independiente de si el responsable es una entidad pública o privada. La información puede entregarse mediante un modelo simplificado que debe contener, entre otra información, indicaciones sobre el responsable del tratamiento y la finalidad perseguida. La GPDP pone a disposición un modelo para uso de los responsables[53].

iii. **Sobre los tiempos de retención de las imágenes grabadas**. En este punto se señala que las imágenes no podrán conservarse más tiempo del necesario para los fines para los que se adquieran. Esto es a menos que las disposiciones legales específicas no previeran expresamente ciertos tiempos de retención de datos (por ejemplo, la normativa aplicable a los municipios establece que el almacenamiento de imágenes recopiladas mediante el uso de sistemas de videovigilancia se limita a siete días después de la detección, sujeto a necesidades especiales de almacenamiento adicional). En algunos casos puede ser necesario ampliar los tiempos de almacenamiento, por ejemplo, en el caso de que dicha prórroga sea necesaria para dar seguimiento a una solicitud de la autoridad judicial o de la policía judicial en relación con una actividad de investigación en curso.

[53] Disponible en: https://www.garanteprivacy.it/documents/10160/0/CARTELLO+VIDEOSORVEGLIANZA+-+Modello+semplificato.docx/5409e-fd5-08a1-7be5-d0c2-672356606af0?version=4.0

iv. **Sistemas de videovigilancia que requieren una evaluación de impacto**. Esta evaluación debe realizarse cuando el sistema implica, en particular, el uso de nuevas tecnologías, teniendo en cuenta la naturaleza, el objeto, el contexto y los fines del tratamiento y que puede presentar un alto riesgo para las personas. Esto puede incluir sistemas integrados que conecta cámaras entre diferentes entidades o sistemas inteligentes capaces de analizar y procesar imágenes.

v. **Utilización de sistemas de videovigilancia para tratar categorías especiales de datos.** Si la captación se efectúa para obtener categorías especiales de datos (como los datos biométricos), dicho tratamiento solo estará permitido bajo las causales de excepción que contempla el artículo 9 del RGPD (por ejemplo, cuando el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado[54]). El tratamiento de categorías especiales de datos requiere una supervisión reforzada y continua de determinadas obligaciones, como un alto nivel de seguridad y una evaluación de impacto de protección de datos, cuando sea necesario.

[54] Artículo 9 letra g) del RGPD.

IV. JURISPRUDENCIA COMPARADA

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

A continuación presentamos algunas decisiones que se han tomado en casos resueltos en sede judicial o administrativa comparada y que estimamos relevantes respecto de sistemas de videovigilancia y reconocimiento facial.

Para poder hacer un seguimiento de la aplicación normativa, hemos considerado las mismas jurisdicciones revisadas en la sección de marco normativo comparado.

1. Unión Europea

Fallo del Tribunal de Justicia de la Unión Europea (CJEU) sobre videovigilancia en edificios residenciales. C-708/18, TK v Asociaţia de Proprietari bloc M5A-ScaraA[55].

Este caso tuvo origen en una petición de decisión prejudicial planteada por el Tribunal de Distrito de Bucarest, Rumania, conforme el artículo 267 del Tratado de Funcionamiento de la Unión Europea[56]. En particular, el caso se refirió a la instalación de cámaras de videovigilancia en las áreas comunes de un edificio residencial, y si tal actividad era, por una parte, necesario; y por otra, si era proporcional en relación a la base de legalidad del interés legítimo[57]. En términos generales, el CJEU examinó cómo el interés legítimo de los operadores de cámaras de videovigilancia se debe equilibrar en relación con los derechos fundamentales de los titulares de datos.

El 11 de diciembre de 2019, el CJEU decidió el caso indicando que el marco jurídico de la Unión Europea[58] no se opone a disposiciones nacionales que autorizan la instalación de un sistema de videovigilancia en las zonas comunes de un edificio residencial sin el consentimiento de los interesados, con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y protección de personas y bienes, si el tratamiento de datos personales mediante el sistema reúne los requisitos del artículo 7 letra f) de la Directiva 95/46/CE[59], lo que le corresponde verificar al Tribunal de Distrito de Bucarest. En términos generales, la Corte llegó a esta conclusión en virtud de los siguientes planteamientos:

[55] Disponible en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=221465&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3006261
[56] Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12016E267
[57] La solicitud se formula en el contexto de un litigio entre TK y la Asociaţia de Proprietari bloc M5A-ScaraA, correspondiente a una comunidad de propietarios; en donde TK demandó a la comunidad para que desactivara el sistema de videovigilancia del edificio y retirara las cámaras instaladas en las zonas comunes del mismo.
[58] Específicamente los artículos 6 y 7 de la Directiva 95/46/CE (la norma anterior al RGPD) y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.
[59] Este artículo establece que "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."

- La aplicación de la **base de legalidad del interés legítimo** exige que se proceda a una ponderación de los derechos e intereses en conflicto, que dependerá de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado.

- La grabación en video de **imágenes de personas que se almacenan en un dispositivo de grabación** continuada constituye un tratamiento automatizado de datos personales.

- **Todo tratamiento de datos personales** debe responder a alguno de los principios relativos a la legitimación del tratamiento de datos (bases de legalidad).

- **El artículo 7, letra f), de la Directiva 95/46** fija tres requisitos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo; segundo, que el tratamiento de datos personales sea necesario para la satisfacción de ese interés legítimo; y, tercero, que no prevalezcan sobre el interés legítimo perseguido los derechos y libertades fundamentales del interesado en la protección de los datos.

- **En relación al primer requisito:** La Corte indicó que este requisito estaría satisfecho en cuanto el responsable estaría buscando la protección de la propiedad, salud y vida de los residentes del edificio. Agregó que había un historial de robo y vandalismo en el edifico que no había sido disuadido por la instalación previa de un sistema de control de entrada. También señaló que, si bien los intereses legítimos perseguidos por el tratamiento deben estar presentes y ser efectivos, eso no significaba que fuera un requisito que la seguridad de la propiedad y las personas estuviera comprometida.

- **En relación al segundo requisito:** El CJEU indicó que se debe comprobar que tales intereses no pueden alcanzarse razonablemente de manera eficaz por otros medios menos atentatorios respecto de los derechos y libertades fundamentales de los interesados, en particular respecto de los derechos al respeto de la vida privada y de protección de datos personales. El principio de minimización de datos también es parte de esta evaluación, y conforme a este, el responsable de datos debe examinar si es necesario operar el sistema de videovigilancia de manera constante (o si podía hacerlo solo por la noche o fuera del horario laboral), y si se pueden bloquear u obscurecer imágenes de áreas donde la vigilancia es innecesaria. Esto es planteado como elementos que deben ser considerados por el responsable, no necesariamente aplicarlos.

- **En relación al tercer requisito:** La Corte señaló que este requisito necesita de una evaluación de los derechos e intereses en juego, lo que depende de las circunstancias individuales de cada caso. La Corte agregó que la ponderación específica del hecho debe tener en cuenta factores tales como la naturaleza de los datos, especialmente si son de naturaleza sensible, la naturaleza y los métodos de tratamiento involucrados, y el número de personas que tienen acceso a los datos y los métodos para hacerlo, junto con las expectativas razonables del interesado, así como la legitimidad indiscutible del interés de los propietarios de los departamentos en proteger la propiedad, salud y vida de los residentes.

2. Reino Unido

Fallo de la Corte de Apelaciones de Inglaterra y Gales sobre tecnología de reconocimiento facial. R (Bridges) v-Chief Constable of South Wales Police & Others[60].

El caso se refiere a la legalidad del uso de tecnología de reconocimiento facial en vivo o en tiempo real por la policía de South Wales con el fin de escanear individuos mediante el uso de cámaras de videovigilancia (CCTV) en lugares públicos, y registrando automáticamente sus rostros. La relevancia de este caso radica en que correspondió al primer caso exitoso en contra de la tecnología de reconocimiento facial en Reino Unido.

En septiembre del año 2019, Edward Bridges interpuso una acción de revisión judicial (judicial review proceeding) luego de que la policía de South Wales implementara un proyecto de vigilancia utilizando la tecnología descrita. Esta acción fue apoyada por la ONG defensora de la privacidad y los derechos civiles "Liberty". La tecnología, llamada "AFR Locate", fue utilizada en ciertos eventos y en distintos lugares públicos susceptibles a la ocurrencia de actos delictuales; escaneando a los miembros del público mediante el uso de cámaras de videovigilancia y capturando automáticamente hasta cincuenta imágenes digitales de rostros por segundo.

La tecnología comparaba las imágenes capturadas con imágenes digitales del rostro de personas de una lista de vigilancia de la policía, que incluía individuos buscados por la justicia o personas desaparecidas. Cuando las imágenes no coincidían, la imagen capturada era automáticamente eliminada. Cuando sí coincidían, la tecnología producía una alerta dirigida al oficial de policía a cargo. De 50 utilizaciones efectuadas entre 2017 y 2018, se estimó que se capturaron imágenes y datos biométricos de, al menos, 500.000 personas sin su consentimiento.

Edward Bridges basó su acción judicial en que el uso de la tecnología era ilegal, y que contravenía tanto el artículo 8 del Convenio Europeo de Derechos Humanos, como la DPA 2018. Indicó también que la policía no cumplió sus obligaciones de igualdad de trato bajo la Public Sector Equaility Duty (Equality Act 2010).

[60] Disponible en: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

El fallo de primera instancia del tribunal administrativo (High Court of Justice Queen's Bench Division - Administrative Court for Wales), de fecha 4 de septiembre de 2019, estableció que, si bien la tecnología de reconocimiento facial comprometía los derechos a la privacidad y a la protección de datos de las personas escaneadas, el marco legal proporcionaba suficientes resguardos para el uso de la tecnología. Se estableció que el uso de esta tecnología para obtener datos biométricos del público era efectuado dentro de las competencias de la policía destinadas a prevenir y detectar el crimen.

Posteriormente, la Corte de Apelaciones de Inglaterra y Gales al revisar el caso indicó que la tecnología de reconocimiento facial en vivo era una tecnología nueva, que involucraba la recolección de imágenes y el procesamiento automatizado de información digital de un gran número de personas del público, en circunstancias que la mayoría de ellos no son de interés de la policía. Luego estableció que, en el contexto de la DPA 2018, los datos recolectados son datos sensibles y que son distintos de, por ejemplo, las fotografías ordinarias. Luego de su análisis, la Corte acogió la apelación de Edward Bridges, anulando el fallo de primera instancia y dictaminando, resumidamente que:

- **El uso de la tecnología de reconocimiento facial infringió el artículo 8 del Convenio Europeo de Derechos Humanos** que establece el respeto a la vida privada y familiar, en base a que, de forma automática y sin consentimiento, se recolectaba y procesaban los datos biométricos de individuos, lo que comprometía los derechos de una persona sobre su imagen. La Corte señaló que, aunque el ordenamiento jurídico de Reino Unido contiene tanto legislación primaria (leyes) tales como la DPA 2018, como legislación secundaria (normas reglamentarias o administrativas) como el Surveillance Camera Code of Practice o políticas dictadas por la policía de South Wales, en ellas no existen definiciones suficientemente claras sobre "dónde" puede ser utilizada la tecnología de reconocimiento facial, ni "quien" puede ser incorporado en una lista de vigilancia (watchlist) por parte de la policía. Estas ausencias otorgan un nivel de discrecionalidad muy alto a los oficiales de policía que impiden dar cumplimiento al estándar exigido por el inciso segundo del artículo 8 del Convenio Europeo de Derechos Humanos.

- **La Evaluación de Impacto a la Privacidad efectuada por la policía no cumplió con la DPA 2018**, ya que falló en evaluar adecuadamente los riesgos que la tecnología de reconocimiento facial implicaba para los derechos y libertades de los individuos.

- La policía de South Wales **no cumplió sus obligaciones de igualdad de trato bajo la Public Sector Equality Duty (Equality Act 2010)**, con anterioridad o durante el uso de la tecnología de reconocimiento facial. A juicio de la Corte, la policía no investigó con suficiencia si la tecnología presentaba un riesgo de discriminación indirecta.

3. España

Jurisprudencia de la AEPD – Procedimiento PS/00120/2021[61]. Resolución de terminación de procedimiento por pago voluntario de empresa Mercadona S.A

El 5 de mayo de 2021 la AEPD inició un procedimiento sancionatorio contra la empresa Mercadona S.A. a causa de la utilización de un sistema piloto de reconocimiento facial por varios meses para la detección de personas con sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o alguno de sus trabajadores. El sistema de reconocimiento facial, implementado en 40 establecimientos, capturaba automáticamente los datos biométricos de cualquier persona en las tiendas y los contrastaba con una base de datos de muestras.

En su análisis, la AEPD estableció que el reconocimiento facial de personas que acceden a los centros de Mercadona constituye un tratamiento de datos de categoría especial regulados en el art. 9 del RGPD y el art. 9 de la LOPDGDD. En ese sentido, estableció que el tratamiento de datos basados en el reconocimiento facial con fines de identificación implementado por la empresa se encuentra prohibido por lo dispuesto en el artículo 9 número 1 del RGPD, al no constar ninguna causa que permita levantar la prohibición entre las excepciones expuestas en el número 2 del RGPD, por lo que no procede ampararse en las causales de licitud del artículo 6.1 del mismo reglamento. Esta prohibición no puede obviarse mediante la aplicación de medidas de seguridad proactiva, ya que la prohibición de tratamiento señalada en el artículo 9 número 1 del RGPD determina que sean irrelevantes.

[61] Disponible en: https://www.aepd.es/es/documento/ps-00120-2021.pdf

En virtud de esto, la AEPD estableció que Mercadona habría infringido diversas disposiciones del RGPD, correspondientes a las siguientes:

- Artículo 6 del RGPD sobre bases de licitud del tratamiento de datos personales;
- Artículo 5.1 letra c) del RGPD sobre el principio de minimización de datos personales;
- Artículo 9 del RGPD sobre el tratamiento de categorías especiales de datos personales;
- Artículo 12 del RGPD sobre transparencia de la información, comunicaciones y modalidades de ejercicio de los derechos del interesado;
- Artículo 13 del RGPD sobre la información que deberá facilitarse cuando los datos personales se obtengan del interesado;
- Artículo 25 sobre la protección de datos desde el diseño y por defecto; y el
- Artículo 35 relativo a la evaluación de impacto relativa a la protección de datos personales.

Conforme este procedimiento Mercadona pagó 2.520.000 € haciendo uso de reducción del 20% por pago voluntario. El monto original de la sanción era de 3,15 millones de euros.

Jurisprudencia de la AEPD – Otros criterios generales

En su jurisprudencia, la AEPD ha fijado una serie de estándares en la resolución de casos asociados a la protección de la imagen de las personas, lo cual se relaciona directamente con el ámbito de la videovigilancia y el reconocimiento facial.

En un caso contra un hospital público, la AEPD determinó que: **(i)** *"la imagen de una persona constituye un dato personal"* ya que es información que concierne a personas y suministra información sobre éstas, como el lugar y la actividad que realizan[62]; **(ii)** al constituir un dato personal, su tratamiento se encuentra regulado por la ley de protección de datos; **(iii)** el hospital carece del consentimiento expreso del titular y de autorización legal, puesto que no se ha demostrado que haya sido realizado bajo la Ley Orgánica 4/1997 (esto es, bajo la competencia de las Fuerzas y Cuerpos de Seguridad[63]) ; y **(iv)** que la *"legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados"*, y que las ocho cámaras que registraban imágenes en la vía pública constituía un tratamiento desproporcionado[64], conforme a la Instrucción 1/2006[65].

Por su parte, la AEPD ha señalado que, en casos de cámaras de videovigilancia en espacios comunes de copropiedad inmobiliaria o de libre acceso para los vecinos, invitados y trabajadores de una copropiedad privada, el responsable requiere contar con la "autorización de la comunidad de propietarios" como título habilitante para el tratamiento de los datos[66].

[62] AEPD, Resol. R/00869/2015, FJ. VI.

[63] AEPD, Resol. R/00869/2015, FJ. V.

[64] AEPD, Resol. R/00869/2015, FJ. V-VI.

[65] Cabe destacar que la AEPD ha señalado que, con la aplicación del RGPD desde el 25 de mayo de 2018, la mayor parte de la Instrucción 1/2016 ha quedado desplazada por lo establecido en la norma europea (AEPD, 2018).

[66] AEPD, Resol. R/00389/2015, FJ. III.

En relación a la legitimidad del tratamiento, la AEPD ha validado el interés legítimo como título habilitante[67].

En directa aplicación de la entonces vigente Directiva 95/46 de la Unión Europea (la antigua norma comunitaria de protección de datos personales[68]), se puede invocar el interés legítimo para la cesión o comunicación de imágenes con el objeto de prevenir posibles ilícitos, en el marco de un convenio entre entidades financieras de crédito y las Fuerzas y Cuerpos de Seguridad. Sin embargo, para que tal título y tal finalidad justifiquen el intercambio de información, el convenio celebrado entre estas partes debe satisfacer garantías suficientes para proteger los datos involucrados. Entre estas garantías se encuentra el deber de confidencialidad, perfiles de acceso a los datos, medidas de seguridad de nivel medio, informe de auditoría de las entidades adheridas al Convenio y la devolución de los datos[69].

Esta decisión cita una sentencia del Tribunal de Justicia de la Unión Europea que ordenó a España a aplicar directamente –esto es, sin intermediación o necesidad de norma doméstica expresa que lo habilitare– la Directiva 95/46 de la Unión Europea con el objeto de legitimar los tratamientos de datos que se efectúen en base al principio de "interés legítimo", sin consentimiento del titular de datos[70]. Cabe señalar, no obstante, que la sentencia no versa sobre datos personales que hubieren sido recopilados a través de dispositivos de videovigilancia. En nuestro país, no es aplicable el "interés legítimo" en tanto título legitimador para el tratamiento de datos

[67] AEPD, Informe 0156/2014.

[68] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta Directiva fue derogada por el RGPD..

[69] AEPD, Informe 0156/2014.

[70] Sentencia del Tribunal de Justicia Europeo (3ª Sala), ECLI/EU/2011/777, de 24 de noviembre de 2011. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=ES.

Resolución 107/2020, de 1 de junio de 2020, del Consejo de Transparencia y Buen Gobierno[71].

Este caso se enmarca respecto de las captaciones efectuadas en el momento de una manifestación social. Así, se solicitaron las filmaciones íntegras en formato video de las vistas aéreas de una concentración celebrada el día 6 de diciembre de 2019 en un sector de Madrid.

La autoridad en española de transparencia accedió parcialmente a la petición del reclamante, instando al Ministerio del Interior a remitir: "Todas y cada una de las filmaciones íntegras en formato vídeo de las vistas aéreas de la concentración celebrada desde Atocha a Nuevos Ministerios de Madrid el día 6 de diciembre de 2019 a las 18:00 bajo el lema Marcha por el clima Emergencia climática. A excepción de aquellas imágenes de la citada manifestación en las que se pudiera identificar a los manifestantes, circunstancia que deberá justificarse y probarse debidamente".

A juicio de la autoridad, la imagen de las personas es un dato de carácter personal que permite su identificación. Respecto a la ponderación entre el derecho de acceso a la información y el derecho a la protección de datos personales, el Consejo español señala que *"Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso"*. Esto fue aprobado en conjunto con la Agencia Española de Protección de datos (AEPD).

[71] Disponible en:
https://www.consejodetransparencia.es/ct_Home/dam/jcr:c0948302-3a67-4387-bd7f-7ddddb1ffa20/R-0107-2020.pdf

4. Italia

Dictamen sobre el sistema Sari Real Time – 25 de marzo de 2021. Registro de medidas n° 127. [9575877][72]

Mediante dictamen del 25 de marzo del 2021, el GPDP de Italia declaró que el uso del sistema de reconocimiento facial "Sari Real Time" no cumplía con la normativa aplicable de protección de datos personales de ese país. A juicio de la autoridad, el sistema, además de carecer de una base de legalidad que permita el tratamiento automatizado de datos biométricos para el reconocimiento facial con fines de seguridad, crearía una forma de vigilancia indiscriminada o masiva.

En cuanto al sistema propiamente tal, este sería utilizado por parte del Ministerio del Interior y no estaría aun activo. Funcionaría mediante una serie de cámaras instaladas en un área geográfica específica, analizando rostros de individuos en tiempo real, y comparándolos con una base de datos predefinida (lista de vigilancia), la cual puede contener hasta 10.000 rostros. Si existe correspondencia entre un rostro de la lista de vigilancia y un rostro grabado por las cámaras, el sistema genera una alerta que llama la atención de los operadores. El sistema también permite grabar las imágenes tomadas por las cámaras, realizando una función de videovigilancia.

En términos sustantivos, la autoridad de protección de datos determinó los siguientes puntos para fundamentar su decisión:

[72] Dictamen disponible en: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

- El uso de tecnología de reconocimiento facial para la prevención y represión de delitos es un asunto extremadamente delicado, que conlleva intromisiones en el derecho a la privacidad y la dignidad de las personas, junto con riesgos en otros derechos humanos y libertades fundamentales.

- El sistema Sari llevaría a cabo un tratamiento automatizado a gran escala que puede afectar a las personas presentes en manifestaciones políticas y sociales, que no son objeto de atención por parte de la policía.

- Aun cuando las imágenes capturadas se borrarían de inmediato, la identificación de una persona se lograría mediante el tratamiento de los datos biométricos de todos los presentes en el espacio monitoreado, con el fin de generar modelos comparables con los sujetos incluidos en la lista de vigilancia.

- Por su fuerte injerencia en la vida privada de las personas es que la legislación sobre privacidad establece estrictas precauciones para el tratamiento de datos biométricos y categorías particulares de datos, lo cual debe encontrar una justificación sobre una base normativa adecuada. Base de legalidad que no se encontró en la documentación aportada por el Ministerio del Interior. Esto es consistente con el artículo 8 del Convenio Europeo de Derechos Humanos y los requisitos para justificar una injerencia en el derecho de respeto a la vida privada.

  Un base de legitimidad adecuada debe tener en cuenta todos los derechos y libertades involucrados y definir las situaciones en las que es posible el uso de tales sistemas, sin dejar una amplia discrecionalidad a quienes los utilizan. Esto debe incluir aspectos fundamentales de la tecnología, como los criterios de identificación de los sujetos que se pueden incluir en la lista de vigilancia, las consecuencias en el caso de falsos positivos o la adecuación del sistema hacia personas pertenecientes a minorías étnicas.

V. MARCO NORMATIVO EN CHILE

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

V. Marco Normativo En Chile

En Chile no existen cuerpos normativos que tengan por objeto regular el uso –a nivel general- de sistemas de videovigilancia o de reconocimiento facial por parte del sector público (Cordero, 2009). En virtud de esto, a nivel de protección de datos personales resulta aplicable lo dispuesto en la LPVP, norma del año 1999 que constituye el marco normativo que regula el tratamiento de datos personales en nuestro país, y que aplica tanto para personas naturales y jurídicas públicas y privadas. Esta norma genera derechos únicamente para las personas naturales en cuanto solo los individuos pueden considerarse como titulares de datos personales.

Además de la LPVP, es preciso destacar la Resolución Exenta N°304, de 30 noviembre de 2020, que aprobó el texto actualizado y refundido de las recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado, y que vino a actualizar las recomendaciones del año 2011 en esta materia[73] (en adelante, las "Recomendaciones del CPLT"). Estas recomendaciones tienen por objeto entregar criterios que orienten la aplicación de la LPVP y que permitan concretizar el derecho fundamental a la protección de datos personales, todo ello con el fin de incrementar y mejorar el nivel de cumplimiento de las obligaciones que la Constitución Política y la ley imponen.

1. La videovigilancia y el uso de la tecnología de reconocimiento facial dentro del ámbito de aplicación de la LPVP

El ámbito de la LPVP en virtud del cual se hace aplicable su regulación atiende a una actividad específica definida por el legislador, a saber, el tratamiento de datos personales. Para evaluar la pertinencia o aplicación de esta norma al contexto de las tecnologías revisadas debemos, en primer lugar, detenernos en la relación existente entre la imagen/huella facial de la persona y el concepto de dato personal; así como lo que se entiende por la actividad de tratamiento de datos.

[73] Publicadas en el Diario Oficial el 7 de diciembre de 2020 y disponibles en: https://www.bcn.cl/leychile/navegar?idNorma=1152996.

a) La imagen y la huella facial de las personas naturales como dato personal

En primer lugar, resulta relevante señalar que la LPVP define, en el literal f) de su artículo 2, a los **datos personales** como todos aquellos relativos a *"cualquier información concerniente a personas naturales, identificadas o identificables"*. En este marco, las Recomendaciones del CPLT profundizan este concepto indicando que los elementos básicos de la definición de datos personales son **(i)** que debe tratarse de información relativa a una persona natural; **(ii)** que debe tratarse de información que permita identificar al titular;[74] y **(iii)** el titular solo puede ser una persona natural.

Luego, la LPVP define una categoría de esta clase de datos en el literal g) del mismo artículo, estableciendo, de forma no taxativa, a los **datos sensibles** como 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, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual"*. Esta es una definición legal de carácter abierto que, conforme señalan las Recomendaciones del CPLT, reconoce categorías tales como datos que se refieren a las características físicas de una persona, como los biométricos; datos que se refieren a las características morales de una persona, como sus creencias o convicciones religiosas; y datos que se refieren a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, la información sobre desplazamiento geográfico o la geolocalización.

A partir de estos conceptos, podemos concluir que la imagen del rostro de una persona y la huella facial obtenida a partir ella[75] -ambos elementos susceptibles de obtención por sistemas de videovigilancia y de reconocimiento facial, respectivamente- pueden calificar en Chile de datos personales de carácter sensible conforme define la LPVP, al corresponder a información que se refiere a las características físicas de una persona natural. Más adelante profundizaremos en los tipos de datos relevantes.

[74] Conforme las Recomendaciones del CPLT, se entiende para estos efectos por identificable, toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante uno o más elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social, siempre y cuando el esfuerzo de determinación no resulte excesivo o desproporcionado.

[75] Mediante el uso de tecnología de reconocimiento facial se traspasa una imagen digital del rostro de una persona a un conjunto de datos que constituyen su huella facial o datos biométricos.

b) La videovigilancia y la tecnología de reconocimiento facial como tratamiento de datos personales

La LPVP define el tratamiento de datos propiamente tal, lo que hace de forma sumamente amplia y abarcando, básicamente, cualquier clase de actividad relacionada con el uso o manejo de datos personales. Su definición se encuentra en el literal o) del artículo 2° de la LPVP, y es definido como cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan *"recolectar, almacenar, grabar, organizar, (...)", o "utilizarlos en cualquier otra forma".*

Ahora bien, teniendo presente la extensión de los conceptos referendos y conforme la forma de funcionamiento de los sistemas de videovigilancia y de reconocimiento facial, en que en la gran mayoría de sus operaciones captan, graban y utilizan -al menos- imágenes de rostros de personas y sus huellas faciales, es posible advertir que su funcionamiento implicará necesariamente y en dicho respecto, un tratamiento de datos personales de carácter sensible regido bajo la LPVP al comprender la recolección, cruce y manejo de información concerniente a personas naturales identificadas o identificables que se refieren a sus características físicas. En tal circunstancia, los titulares de estos datos serán aquellas personas naturales a las cuales se refieran las imágenes o huellas tratadas, ya sea en el contexto del sistema de videovigilancia o en el de reconocimiento facial.

En este escenario, resulta adecuado reforzar la idea de que la amplitud del vocablo "tratamiento" en la LPVP implica que, aun cuando las acciones que involucren la imagen del rostro de personas y/o sus huellas faciales sean menores o, dicho de otro modo, los sistemas de videovigilancia o reconocimiento facial sean imperfectos o con funcionalidades limitadas, igualmente existirá un tratamiento de datos personales en cada nivel de operación que se relacione con tales antecedentes. Esto implica que nos encontremos ante un tratamiento de datos personales regido por la LPVP, por ejemplo, con la sola captación de rostros a través de cámaras de videovigilancia (aun cuando su procesamiento sea temporal o momentáneo); en el almacenamiento de dichos rostros en un disco local y sin acceso por parte de terceros; o en el match realizado entre los datos captados mediante cámaras con una base de datos que contenga datos biométricos o huellas faciales y que fueron almacenados con anterioridad.

En las circunstancias descritas, se desprende entonces que una entidad pública o privada que opere un sistema de videovigilancia o de reconocimiento facial en Chile, estará obligado a cumplir la LPVP, en cuanto su actividad involucrará un tratamiento de datos personales. En este contexto, la puesta en marcha de esta clase de sistemas requerirá dar estricto cumplimiento a lo que al efecto dispone la LPVP, so pena de realizar un tratamiento de datos personales indebido por infracción a la normativa vigente y sujeto, bajo lo dispuesto en el artículo 23 de la LPVP, a la indemnización de los perjuicios que se hayan generado a los titulares de datos.

Por último, cabe señalar que pueden existir ciertas circunstancias en las cuales el uso de un sistema de videovigilancia no necesariamente caiga bajo la regulación de la LPVP. Esto ocurrirá en aquellos casos donde el tratamiento de datos no permita la identificación de personas naturales, directa o indirectamente y como podría acontecer, por ejemplo, en el caso de disparos a gran altitud, cuando las cámaras instaladas estén sin funcionamiento, o cuando la persona grabada tenga el rostro cubierto. No obstante, esto es un análisis que cada responsable debe hacer caso a caso, conforme las características propias de los sistemas que utilice y, sobre todo, conforme su correspondencia con la definición legal de dato personal, dato sensible y tratamiento de datos personales.

2.
Tipos de datos personales tratados a través de sistemas de videovigilancia y de reconocimiento facial

Como dijimos, los sistemas de videovigilancia implican la captura de imágenes que pueden incluir imágenes de personas naturales y sus rostros. Por su parte, los sistemas de reconocimiento facial implican, en general, la recolección, cruce y uso de imágenes del rostro de personas naturales, sus puntos de referencia, su huella facial y sus datos asociados. De esta forma, y siguiendo las categorías de datos que contempla la LPVP, así como la que contempla el proyecto de ley que busca modificar la Ley N°19.628 sobre Protección de la Vida Privada, correspondiente a los Boletines refundidos N°11144-07 y N°11092-07 ("Proyecto de Ley")[76], podemos clasificar los tipos de datos personales que son tratados bajo estas tecnologías de la siguiente manera:

- **Datos personales.** Estos datos pueden ser tratados en relación con aquellos otros datos que se recolecten mediante el uso de cámaras de videovigilancia o de sistemas de reconocimiento facial, y que pueden ser recolectados antes, durante o después de su funcionamiento. En este grupo podemos encontrar nombres, apellidos, direcciones, correos electrónicos, teléfonos y otros. Por ejemplo, el tratamiento de estos datos ocurría cuando el sistema de reconocimiento facial se encuentre asociado a un mecanismo de ingreso, en donde exista un perfil previo que asocie los datos biométricos con aquellos otros antecedentes del trabajador como, por ejemplo, su cargo, nombre, departamento en el que trabaja, turno de trabajo, etc.

- **Datos personales de carácter sensibles.** Estos datos son tratados tanto en un contexto de cámaras de videovigilancia como de sistemas de reconocimiento facial y corresponderían, fundamentalmente, a las imágenes de rostros de personas naturales. Según indicamos, bajo lo dispuesto en la LPVP estas imágenes califican como datos personales de carácter sensible al consistir en información concerniente a personas naturales que se refieren a sus características físicas (Becker y Garrido, 2017: 68-72).

  En este grupo también se puede incluir otra información relevante como información sobre coincidencias con imágenes de personas almacenadas en una lista de vigilancia; información sobre el origen étnico; información sobre las emociones y bienestar; o incluso, integrando toda esta información de forma progresiva durante un lapso de tiempo, datos sobre los hábitos personales de quienes se ven expuestos a estos mecanismos. Todos estos casos califican igualmente de datos de carácter sensible por corresponder claramente a datos que se refieren a hechos o circunstancias de la vida privada o intimidad de los titulares.

[76] Para este trabajo, se utilizó la versión del Proyecto de Ley actualizada hasta el mes de septiembre de 2021.

- **Datos biométricos.** Estos datos son tratados dentro del contexto de los sistemas de reconocimiento facial y corresponden a la huella facial o rasgos faciales que son extraídos de las imágenes digitales que son procesadas por esta tecnología. Estos datos son esenciales en el contexto de los sistemas de reconocimiento facial y su relevancia radica en que permiten la identificación única de los individuos.

  Cabe destacar que esta clase de datos no está reconocida expresamente en la LPVP, por lo que, al referirse a las características físicas de una persona, caerían actualmente bajo la categoría general de datos personales de carácter sensibles (Becker y Garrido, 2017). Por otro lado, estos sí están reconocidos en el Proyecto de Ley, que los define hasta ahora 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, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz"*. Como veremos más adelante, esta definición es similar a la que establece el RGPD de la Unión Europea para datos biométricos[77].

  En términos generales, el dato biométrico surge a través de un proceso de registro o codificación de aspectos materiales (ej. el iris, la oreja o el rostro) o inmateriales (ej. el patrón de la voz[78]). El simple tratamiento de imágenes de una persona no conlleva necesariamente el tratamiento de datos biométricos, sino cuando se han tratado con medios técnicos específicos conforme señala la definición[79] (EDPB, 2020).

- **Datos de geolocalización o sobre el desplazamiento geográfico.** Estos están asociados a la ubicación de los dispositivos utilizados y pueden ser tratados tanto en un contexto de cámaras de videovigilancia como de sistemas de reconocimiento facial.

  Al igual que con los datos biométricos, esta clase de datos no está reconocida de forma expresa en la LPVP, por lo que actualmente caerían en la categoría general de datos personales de carácter sensible, por ser datos que se refieren a hechos o circunstancias de la vida privada o intimidad de los titulares. Este criterio ha sido adoptado en la Sección octava de las Recomendaciones del CPLT.

  Por su parte, estos datos no están definidos en el Proyecto de Ley, sin perjuicio de contener condiciones particulares para su tratamiento.

[77] Se ha indicado que los datos biométricos cambian la relación entre el cuerpo y la identidad "ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior" (WP29, 2012).
[78] En esta línea, Becker y Garrido (2017) clasifican los datos biométricos en tres grupos: (i) datos estáticos, que se extraen de las características físicas del individuo; (ii) datos dinámicos, que se vinculan con patrones de conducta asociados a una persona; y (iii) datos mixtos, que combinan los datos estáticos y los dinámicos.
[79] Véase el considerando número 51 del RGPD.

3.
Obligaciones para el tratamiento de datos personales en el contexto de videovigilancia y de tecnología de reconocimiento facial

El sujeto obligado bajo la LPVP corresponde al responsable del banco de datos, el cual es definido en el literal n) del artículo 2 de la LPVP como "la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal". De esta forma, un organismo público, como una municipalidad o un Ministerio, que utilice esta clase de tecnologías en el ejercicio de sus funciones tendrá, de acuerdo con la LPVP, la calidad de responsable del banco de datos para efectos del tratamiento de datos personales que se lleve a efecto, estando sujeto a las obligaciones dispuestas en esa norma[80].

Al haber observado que bajo la utilización de sistemas de videovigilancia o de reconocimiento facial es posible encontrarse frente a un tratamiento de datos personales, resulta ahora relevante referirse a aquellas obligaciones que implica dicha actividad en Chile en virtud de lo que dispone la LPVP, y que deben ser cumplidas por las entidades públicas que realicen el tratamiento como responsables. En este catálogo de obligaciones, encontramos principalmente las relativas a la obtención de una base de legalidad; la observancia del principio de finalidad en el tratamiento; la observancia de la obligaciones de seguridad y confidencialidad en el tratamiento de datos; el respeto al ejercicio de los derechos ARCO por parte de los titulares sobre sus datos personales; la observancia de las obligaciones de eliminación, modificación y bloqueo de datos que tiene el responsable; la suscripción de mandatos para el tratamiento de datos por terceros que traten datos en nombre del responsable; y, la inscripción de las bases de datos en el Registro a cargo del Servicio de Registro Civil e Identificación. Estas las pasamos a revisar en mayor detalle a continuación.

[80] En el caso de las municipalidades, el Consejo para la Transparencia ha establecido, a través de las recomendaciones esgrimidas mediante el Oficio N°2309, de 6 de marzo de 2017, la calidad de responsables del banco de datos de dichas entidades cuando utilicen sistemas de videovigilancia para fines de seguridad comunal, aun cuando dicho tratamiento sea encargado a un tercero mandatario.

a) Base de legalidad para el tratamiento de datos personales por parte del sector público

La regla general en esta materia se encuentra en el artículo 4 de la LPVP, que reconoce como bases de legalidad en nuestro ordenamiento únicamente a la ley y al consentimiento del titular. Respecto de los organismos públicos, el artículo 20 establece que el tratamiento de datos que éstos realicen *"sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular"*.

Ahora bien, en atención a que los sistemas de videovigilancia y de reconocimiento facial implican el tratamiento de datos sensibles (imágenes del rostro de las personas y su huella facial), especial atención deberá prestarse también al artículo 10 de la LPVP, que dispone una prohibición general al tratamiento de esta clase de datos al establecer que *"No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares"*. El legislador ha consagrado un régimen especial de protección para los datos personales sensibles en el entendido que su tratamiento es particularmente propenso a lesionar derechos fundamentales de los titulares.

Por otro lado, cabe recordar que, mediante el uso de tecnología de reconocimiento facial, la huella facial de una persona obtenida a partir de su imagen digital es utilizada para compararla con otros datos biométricos previamente almacenados en una base de datos (WP29, 2012). En virtud de esto, hay que tener presente que la base de legalidad para el tratamiento de datos se requiere no solo respecto de los datos que son extraídos en el contexto del uso del sistema de reconocimiento facial (por ejemplo, mediante cámaras instaladas en el espacio público), sino que también respecto de los demás datos biométricos que ya estén almacenados, y con los cuales se realiza el proceso de comparación o correspondencia biométrica. En el caso de fines de vigilancia, estos datos biométricos con los cuales las imágenes capturadas se comparan habitualmente corresponden a listas de vigilancia (watchlists) compiladas por las fuerzas de orden y seguridad.

Bajo este entramado normativo, y conforme la posición que en la materia ha ido desarrollando el Consejo en el contexto de la consagración constitucional del derecho de protección de datos personales (por ejemplo, en las Recomendaciones del CPLT), las entidades públicas solo pueden hacer tratamiento de datos de carácter sensible, como los biométricos, en alguno de los siguientes casos[81]:

i. Cuando el tratamiento de datos sensibles esté expresamente contenido en una norma de rango legal;

ii. Cuando el tratamiento de datos sensibles, no estando autorizado expresamente, resulte imprescindible (criterio de necesidad) para el debido cumplimiento de una función pública establecida por ley y forme parte esencial de las materias de su competencia[82]; o

iii. Cuando se ha obtenido el consentimiento del titular de datos. En cuanto a los requisitos del consentimiento, éste deberá ser otorgado de forma expresa, por escrito, y habiéndose informado debidamente al titular del propósito del almacenamiento de datos y su posible comunicación al público. Este consentimiento debe ser otorgado de manera libre, o sea, no condicionando la capacidad del titular de negarse a otorgarlo. Por su parte, es importante que se le permita al titular ejercer efectivamente su derecho a revocar su consentimiento, sin efectos retroactivos.

[81] Esta interpretación es consistente con la jurisprudencia de la Contraloría General de la República (véase dictamen N°25.682 de 2019), así como la jurisprudencia de la Corte Suprema en la materia (véase sentencia en causa Rol N°85.215-2020 de 4 de enero de 2021 relativa al Sistema de Apoyo a Fiscales "SAF"). A mayor abundamiento, cabe destacar que la historia de la ley del artículo 20 de la LPVP muestra que los legisladores tuvieron una idea de "competencia" asociada a la idea de "necesariedad". La historia de la ley está disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/.

[82] Cabe destacar que el Consejo para la Transparencia ha calificado circunstancias donde no se advierte la existencia de una base de legalidad basada en una autorización legal respecto de un organismo público. Véase Oficio N°127, de 30 de abril de 2021, del Consejo para la Transparencia, por el que se evacua pronunciamiento a requerimiento de una asociación gremial en relación al tratamiento de datos efectuado por la Subsecretaria de Telecomunicaciones del Ministerio de Transporte y Telecomunicaciones. Este oficio está disponible en: https://www.portaltransparencia.cl/PortalPdT/documents/10179/62801/N%C2%B0000127+Alfie+Ulloa+Urrutia.+Presidente+Ejecutivo+-+Asociaci%C3%B3n+Chilena+de+Telefon%C3%ADa+M%C3%B3vil+A.G..pdf/efa6f497-a456-45a3-9e70-bc7e18656edc

b) Principio de finalidad

Este principio está establecido en el artículo 9 de la LPVP, que señala *"Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público"*. En el contexto de las entidades públicas, la finalidad está determinada en función de las materias propias de su competencia y por la función legal específica que está ejecutando y que justifica el tratamiento de datos personales.

En el contexto de los sistemas de videovigilancia y de reconocimiento facial este principio debe ser íntegramente cumplido por los responsables del banco de datos, teniendo presente que el tratamiento -en la mayoría de estos casos- se basa en datos recolectados directamente desde el titular y no desde una fuente accesible al público.

Por su parte, cabe señalar que la LPVP define a la fuente accesible al público en su artículo 2 literal i) como *"los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes"*. De esta forma, de su tenor literal se descarta que la recolección directa de datos desde los titulares mediante cámaras instaladas en el espacio público signifique la obtención de datos mediante una fuente accesible al público. A mayor abundamiento, el tratamiento de datos obtenidos mediante una fuente accesible al público, sin el consentimiento del titular, está condicionado a los escenarios de tratamiento descritos en el artículo 4 de la LPVP[83] que, por lo demás, no son aplicables al tratamiento de datos sensibles que prescribe el artículo 10 de esa misma ley. Por último, esto también es consistente con la posición del EDPB (2020, p. 17), que establece que los responsables que traten datos de categorías especiales en el contexto de videovigilancia, no se pueden amparar en la base de legalidad del art. 9, numero 2, letra e) del RGPD, que permite el tratamiento de datos personales que el interesado ha hecho manifiestamente públicos. Dicha autoridad señala que *"el mero hecho de entrar en el alcance de la cámara no implica que el interesado pretenda hacer públicas categorías especiales de datos relacionadas con su persona"*.

En el caso de operar mediante la base de legalidad consentimiento, la finalidad de dicho tratamiento deberá estar alineada con los propósitos que fueron informados al momento de la obtención de la autorización (por ejemplo, para efectos de verificar la identidad de un individuo y permitir su acceso a cierta instalación u oficinas). De esta forma, cabe reiterar que la autorización que se presente a los titulares debe ser explícita y detallada respecto a las finalidades y propósitos del tratamiento y su alcance, en cuanto el artículo 4 de la LPVP requiere que el titular sea "debidamente informado" de dichos aspectos. Por el contrario, una autorización que esté redactada en términos generales y abstractos no cumpliría los requisitos establecidos por el legislador para configurar la base de legalidad en comento.

[83] Por ejemplo, que los datos a tratar sean de carácter económico, financiero, bancario o comercial.

c) Obligaciones de seguridad y confidencialidad del responsable de datos

La **obligación de seguridad** que tiene el responsable del banco de datos se encuentra establecida en el artículo 11 de la LPVP, que señala *"el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños"*. Esto se ha entendido, de forma reciente, como el deber de adoptar medidas, tanto organizativas como técnicas, que garanticen la integridad, confidencialidad y disponibilidad de todos los datos tratados, con miras a evitar la alteración, perdida y acceso no autorizado a los mismos. En el contexto particular que estamos analizando, estas medidas deberían abordar conductas que puedan resultar en una reconstrucción no autorizada de rasgos biométricos a partir de una plantilla de referencia; su vinculación con otras bases de datos; su uso ulterior sin consentimiento de los titulares de datos para fines no compatibles con los originales; o la posibilidad de que algunos datos biométricos puedan utilizarse para revelar información sobre la raza o salud de las personas (WP29, 2012). Para la determinación de las medidas, especial atención se deberá prestar a los riesgos asociados al tratamiento, así como al estado de la técnica y los costos de implementación de las medidas.

Por su parte, la **obligación de confidencialidad** de los responsables se encuentra en el artículo 7 de la LPVP que consagra esta obligación señalando que *"las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo"*.

En el contexto de los datos biométricos tratados al alero de los sistemas de reconocimiento facial, estas obligaciones resultan de suma importancia, en el entendido que la huella facial o los datos biométricos en general, no pueden ser modificados o suprimidos por los titulares de datos. En este escenario, una vulneración a la seguridad se ve enfrentada al hecho de no poder mitigar los efectos perjudiciales de la misma, y por tanto, generar una grave afectación a los titulares de datos.

d) Respeto al ejercicio de los derechos ARCO de los titulares

Conforme establece el Título II de la LPVP, los titulares de datos cuentan con un conjunto de derechos que, en el contexto del tratamiento de datos efectuado mediante sistemas de videovigilancia y de reconocimiento facial, son plenamente aplicables y deben ser respetados por los responsables de datos. Estos derechos son[84].

i. **Derecho de información y acceso:** el derecho a exigir al responsable del tratamiento información sobre los datos relativos a su persona que el responsable esté tratando; su procedencia; su destinatario; los propósitos del almacenamiento; y la individualización de las personas a los cuales los datos son transmitidos regularmente.

   Conforme señala la doctrina, este derecho corresponde también al derecho de acceso del titular a aquellos datos que son tratados y que conciernen a su persona (Cerda, 2012). Cuestión que también ha sido establecida por la jurisprudencia de la Corte Suprema y del Consejo para la Transparencia, precisamente en casos relativos al acceso a grabaciones efectuadas por cámaras de videovigilancia que contenían datos personales[85].

   A mayor abundamiento, el Consejo para la Transparencia ha reconocido[86] que el ejercicio de este derecho puede efectuarse a través del derecho de acceso a la información pública consagrado en la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, sobre Acceso a la Información Pública (la "Ley de Transparencia") cuando se soliciten datos personales que obren en poder de un sujeto obligado por dicha ley, en cuyo caso se aplicará el procedimiento establecido en ella, incluyendo la posibilidad de recurrir de amparo ante el Consejo. No obstante, en lo relativo a la gratuidad del acceso, se observará lo dispuesto en la LPVP.Por último, a nivel comparado destaca el hecho que la Working Party 29 también se ha referido expresamente al derecho de acceder a datos biométricos, indicando que los titulares tienen derecho a acceder a posibles perfiles basados en dichos datos (WP29, 2012)[87].

[84] El artículo 3 de la LPVP también reconoce el derecho de oposición, que consistente en el derecho del titular a oponerse a la utilización de datos con fines de publicidad, investigación de mercado o encuestas de opinión.

[85] Ver, por ejemplo, sentencias de Corte Suprema en Roles N°18.458-2016 y N°18.481-2016, ambas de 1 de junio de 2016; Oficio N°2309, de 6 de marzo de 2017, del Consejo para la Transparencia que formula recomendaciones a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N°19.628; y amparos C759-10, C148-21 y C4687-20 del Consejo para la Transparencia.

[86] Sección 5.1 de las Recomendaciones del CPLT.

[87] Agrega en este punto que, si el responsable del tratamiento tiene que verificar la identidad de los interesados para conceder acceso a los mismos, es esencial que este se ofrezca sin que medie tratamiento de datos personales adicionales (WP29, 2012, p. 15).

ii. **Derecho de modificación:** el derecho a exigir la modificación de los datos cuando ellos sean erróneos, inexactos, equívocos o incompletos.

iii. **Derecho de eliminación o cancelación:** el derecho a exigir la eliminación de los datos cuando su almacenamiento carezca de fundamento legal; los datos hayan caducado; los haya proporcionado voluntariamente; o ellos se utilicen para comunicaciones de carácter comercial, y el titular no desee seguir figurando en el registro de datos.

iv. **Derecho de bloqueo:** el derecho a exigir la suspensión temporal del tratamiento cuando su exactitud no pueda ser establecida o su vigencia sea dudosa, en los escenarios en que no corresponda la eliminación.

De acuerdo con el artículo 13 de la LPVP, el ejercicio de estos derechos no puede ser limitado por medio de ningún acto o convención. Si el responsable no se pronuncia sobre la solicitud del titular que ejerce alguno de estos derechos dentro de dos días hábiles, o la deniega por una causa distinta de la seguridad de la Nación o el interés nacional, el titular tendrá acción para solicitar amparo a estos derechos ante el juez de letras en lo civil del domicilio del responsable, lo que también se conoce como acción habeas data.

En Chile hay una percepción favorable a este tipo de derechos, ya que son importantes para la autodeterminación de la información personal. No obstante, son las personas más educadas, con una situación socioeconómica más alta o que tienen conocimiento de leyes afines, como la Ley de Transparencia, las que perciben su importancia.

e) Obligaciones de eliminación, modificación y bloqueo de datos personales que tiene el responsable

Conforme señala el artículo 6 de la LPVP, los responsables de datos tienen las siguientes obligaciones: (i) eliminar o cancelar los datos personales cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado; (ii) modificar los datos personales cuando sean erróneos, inexactos, equívocos o incompletos; y (iii) bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa, y respecto de los cuales no corresponda la cancelación.

Estas obligaciones operan de oficio, sin necesidad de requerimiento del titular de datos, por tanto, resulta esencial que los responsables establezcan políticas y procedimientos efectivos para su cumplimiento, con periodos y condiciones de retención acordes a la LPVP. En cuanto a la obligación de eliminación de datos, destacamos las acciones que ha realizado el Consejo en esta materia en relación a las grabaciones efectuadas por sistemas de videovigilancia operadas por municipalidades. Sobre este punto nos referiremos en mayor profundidad más adelante.

Por su parte, cabe destacar que la obligación de modificación es relevante en el contexto del tratamiento de datos biométricos realizado por los sistemas de reconocimiento facial, por cuanto la precisión de los datos es esencial en la recolección y en el establecimiento del vínculo entre la persona y los datos biométricos. Según señala la Working Party 29, la exactitud en el registro también es importante para prevenir la usurpación de identidad (WP29, 2012).

f) Mandato para el tratamiento de datos personales

La LPVP establece condiciones para que un responsable del banco de datos pueda encargar a un tercero el tratamiento de datos en su nombre. Este tercero se conoce como "mandatario" o "encargado", y corresponde a aquel que trata los datos por cuenta y nombre del responsable del tratamiento. La regulación de esta institución se encuentra en el artículo 8 de la LPVP, que establece que el mandato entre responsable y mandatario debe ser otorgado por escrito, *"dejando especial constancia de las condiciones de la utilización de los datos"*.

Si bien la obligación de la LPVP es general, dentro de las condiciones que se establezcan para el mandatario se deben incluir todas aquellas que sean necesarias para que el tratamiento de datos se efectúe respetando, en todo momento, los derechos de los titulares. En este sentido, se ha estimado que estos acuerdos deberían, al menos, indicar **(i)** que el tratamiento se efectúa a cuenta y riesgo del organismo responsable del tratamiento; **(ii)** los tipos de datos personales a ser tratados y las condiciones de utilización (por ejemplo, datos sensibles relativos a imágenes de rostros de titulares de datos); **(iii)** las medidas de seguridad que se deben adoptar; **(iv)** las exigencias de confidencialidad de las personas que trabajen en el tratamiento; y **(v)** el plazo en que el mandatario conservará los datos y las condiciones para su devolución o eliminación segura e irrevocable[88].

En el contexto de este trabajo, la figura del mandato es muy importante en el entendido que la operación de algunos o varios aspectos de los sistemas de videovigilancia o de reconocimiento facial, muchas veces es delegada a terceros contratistas, como precisamente ocurrió en el caso de los globos de vigilancia empleados por las municipalidades de Las Condes y Lo Barnechea. Este caso se describe más adelante en la sección de jurisprudencia.

g) Inscripción de bases de datos en el Registro a cargo del Servicio de Registro Civil e Identificación

Esta obligación, aplicable solo para los organismos públicos, requiere la inscripción de los bancos de datos personales que se encuentren a su cargo. Este es un registro público que debe contener cierta información asociada, como el fundamento jurídico de la existencia del banco de datos, y su finalidad. De la amplitud de su configuración, resulta plenamente aplicable a aquellas bases de datos que contengan datos personales relativos al funcionamiento y operación de sistemas de videovigilancia o de reconocimiento facial.

[88] Como recomendaciones para robustecer el tratamiento de datos biométricos por mandato, podemos destacar el Oficio N°48, del Consejo para la Transparencia, de 24 de febrero de 2021, dirigido al Servicio de Registro Civil e Identificación en el contexto de la licitación del nuevo sistema de identificación llevado por ese servicio. En dicho oficio, se encontraban -entre otras- recomendaciones relativas a (i) la especificación de condiciones para que el mandatario realice la delegación del mandato de tratamiento; (ii) la especificación de condiciones relativas a la localización del tratamiento por parte del mandatario; y (iii) procedimientos para el adecuado cumplimiento de los derechos ARCO.

4.
Debilidades de la Ley 19.628 sobre Protección de la Vida Privada para responder frente a los riesgos que presenta la videovigilancia y la tecnología de reconocimiento facial

Desde hace un tiempo a esta parte, la doctrina y la ciudadanía en general están contestes en que la LPVP es un instrumento normativo obsoleto[89], que no se hace cargo del desarrollo tecnológico actual y que, por tanto, no confiere una protección suficiente a los titulares de datos. De esta forma, es posible advertir una serie de debilidades que le impiden hacerse cargo, de manera óptima, de los riesgos que conllevan la videovigilancia y la tecnología de reconocimiento facial en relación al derecho fundamental de protección de datos personales. A nivel general, entre dichas debilidades observamos:

i. Principios del tratamiento de datos regulados de forma inorgánica y deficiente;

ii. Un procedimiento insuficiente de tutela de derechos ARCO (acceso, rectificación, cancelación y oposición);

iii. Un catálogo limitado de bases de legalidad habilitantes basado únicamente en la ley o en el consentimiento del titular de datos;

iv. Una regulación limitada y confusa de la base de legalidad aplicable a los organismos públicos;

v. Ausencia de obligaciones robustas de transparencia y publicidad relativas a políticas de privacidad o tratamiento de datos;

[89] Véase Contreras, 2021.

vi. Ausencia de regulación sobre categorías de datos relevantes, como los datos biométricos o de geolocalización;

vii. Una regulación confusa respecto al tratamiento de datos almacenados u obtenidos desde fuentes accesibles al público[90];

viii. Una regulación limitada de la figura del mandatario o encargado del tratamiento de datos a nombre de un responsable[91];

ix. Un estatuto sancionatorio deficiente y sin multas que signifiquen incentivos al cumplimiento de la norma; y

x. Ausencia de una autoridad de control independiente y con facultades de fiscalización y supervisión de los responsables de datos personales, debiendo los titulares afectados recurrir ante los tribunales de justicia en caso de advertir un tratamiento indebido.

Las debilidades descritas de la LPVP y, particularmente, la referida a la ausencia de una autoridad supervisora autónoma, ha generado que no exista un mayor control respecto de la implementación en Chile de tecnologías de videovigilancia y reconocimiento facial, por ejemplo, en contextos de seguridad de espacios públicos.

[90] La LPVP establece en su artículo 4 ciertas excepciones al consentimiento de los titulares para efectuar el tratamiento de datos cuando los datos provienen de esta clase de fuentes, las cuales están redactadas de forma abierta y poco clara. Este hecho, sumado a la falta de jurisprudencia existente en la materia y la ausencia de una autoridad administrativa de protección de datos que contribuya en la interpretación de la norma, genera una situación de desprotección para los titulares frente a entidades privadas que realicen uso de datos obtenidos de esta clase de fuentes. Esta circunstancia genera condiciones que facilitan un uso inapropiado o abusivo de la tecnología de reconocimiento facial.

[91] Muchas veces quienes ofrecen servicios de identificación o vigilancia actúan en calidad de "mandatarios" o "encargados" del tratamiento, no obstante, la regulación en Chile de esta figura es limitada requiriéndose únicamente un mandato por escrito y el establecimiento de las condiciones para el tratamiento de datos, lo cual genera insuficientes resguardos para los titulares de datos.

5.
Proyecto de ley de protección de datos personales

Desde el año 2017 se discute en el Congreso Nacional un proyecto de ley que busca modificar la Ley N°19.628 sobre Protección de la Vida Privada, correspondiente a los Boletines refundidos N°11144-07 y N°11092-07[92]. Este proyecto se encuentra todavía en su primer trámite constitucional en el Senado, y no es posible advertir una fecha en la que pueda transformarse en ley. En términos sustantivos, el Proyecto de Ley busca modificar la LPVP, creando una autoridad de control administrativa y mejorando el estándar de protección de datos personales acercándolo al dispuesto por el Reglamento General de Protección de Datos de la Unión Europea. Entre las modificaciones que se contemplan, se pueden destacar:

i. **Principios.** Establecimiento expreso de los principios aplicables al tratamiento de datos personales, como el de licitud, finalidad, proporcionalidad, información, seguridad y confidencialidad.

ii. **Derechos ARCOP.** Reforzamiento de los derechos ARCO y reconocimiento del nuevo derecho de portabilidad de datos.

iii. **Bases de legalidad.** La incorporación de nuevas bases de legalidad distintas al consentimiento y la ley, como la ejecución de un contrato en que haya sido parte el titular, o el interés legítimo del responsable.

iv. **Nuevas instituciones.** Se regulan instituciones hasta ahora no comprendidas en nuestra legislación, como la cesión de datos entre dos responsables, y la transferencia internacional de datos personales.

v. **Autoridad de control.** La creación de un organismo público encargado de velar por el cumplimiento de la ley con facultades de interpretar, fiscalizar y sancionar infracciones legales.

[92] El Proyecto de Ley corresponde a un texto que todavía no constituye ley de la República y está sujeto a discusión legislativa. En dicho contexto, sus disposiciones pueden ser modificadas en el transcurso del proceso legislativo restante. El texto del Proyecto de Ley utilizado para esta sección corresponde a aquel aprobado por la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado en primer trámite constitucional. El Proyecto de Ley está disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07

vi. **Multas.** La modificación de las multas por incumplimiento de la ley, estableciendo que las infracciones podrán ser sancionadas con multa de hasta 10.000 Unidades Tributarias Mensuales.

vii. **Nuevas obligaciones.** El establecimiento de nuevas obligaciones para el responsable de datos, entre las cuales podemos destacar **(i)** una **obligación de confidencialidad** más robusta que la que establece la actual LPVP en su artículo 7; **(ii)** una **obligación de implementar medidas de seguridad,** que consideren el estado actual de la técnica, los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados; **(iii) obligaciones de transparencia e información.** El responsable estará obligado a mantener cierta información permanentemente a disposición del público, como la política de tratamiento de datos que haya adoptado y la individualización del responsable y su representante legal. Entre otras informaciones relevantes; y **(iv) una obligación de notificar brechas de seguridad**, tanto a los titulares de datos afectados como a la nueva autoridad. Esta notificación deberá efectuarse por los medios más expeditos posibles y sin dilaciones indebidas. La notificación a la autoridad deberá ocurrir siempre que exista una vulneración, y la notificación a los titulares, cuando se refieran a datos personales sensibles, datos relativos a niños y niñas menores de catorce años, o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

[93] Alrededor de 530 millones de pesos a octubre de 2021.7

En el entendido que el funcionamiento de los sistemas de videovigilancia y de reconocimiento facial implican el tratamiento de datos personales de variadas categorías, bien puede sostenerse que todas las modificaciones y mejoras descritas del Proyecto de Ley tendrán -en mayor o menor medida- un impacto muy positivo en términos de los derechos de protección de datos personales de los titulares que pudieran llegar a verse afectados por tales tecnologías.

Sin perjuicio de esto, quisiéramos destacar las disposiciones que contiene el Proyecto de Ley en relación a las bases de legalidad aplicables para el tratamiento de datos sensibles y biométricos, que, como vimos, son aquellos preferentemente tratados en el contexto de la videovigilancia y el reconocimiento facial. En primer lugar, resulta necesario señalar que la base de licitud general para el tratamiento de datos por los organismos públicos se encuentra en el artículo 20 del proyecto, indicando que "es lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en la ley, y a las disposiciones previstas en este Título. En esas condiciones, los órganos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales". Sin perjuicio de esta norma, el artículo 21 del proyecto hace aplicable a los organismos públicos las disposiciones particulares sobre datos sensibles y biométricos, las que establecen:

> **Datos sensibles.** El Proyecto de Ley los define como aquellos que revelen el origen étnico o racial, la afiliación política, sindical o gremial, 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. Además de otras bases de legalidad específicas, estos datos podrán tratarse **(i)** con el consentimiento expreso del titular; y **(ii)** cuando lo autorice o mandate expresamente la ley[94].

[94] Las otras bases de legalidad que permitirán el tratamiento de datos sensibles son (i) Cuando el tratamiento se refiere a datos personales sensibles que el titular ha hecho manifiestamente públicos y su tratamiento esté relacionado con los fines para los cuales fueron publicados; (ii) Cuando el tratamiento se basa en un interés legítimo realizado por una persona jurídica de derecho público o de derecho privado que no persiga fines de lucro y se cumplan las siguientes condiciones: i.- Su finalidad sea política, filosófica, religiosa, cultural, sindical o gremial; ii.- El tratamiento que realice se refiera exclusivamente a sus miembros o afiliados; iii.- El tratamiento de datos tenga por objeto cumplir las finalidades específicas de la institución; iv.- La persona jurídica otorgue las garantías necesarias para evitar filtraciones, sustracciones o un uso o tratamiento no autorizado de los datos, y v.- Los datos personales no se comuniquen o cedan a terceros; (iii) Cuando el tratamiento de los datos personales del titular resulte indispensable para salvaguardar la vida, salud 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; (iv) 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; y (v) Cuando el tratamiento de datos sea necesario para el ejercicio de derechos y el cumplimiento de obligaciones del responsable o del titular de datos, en el ámbito laboral o de seguridad social, y se realice en el marco de la ley.

Datos biométricos. Como ya señalamos, el Proyecto de Ley los define como los 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, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz. Sin perjuicio de otras bases de legalidad aplicables, estos datos pueden ser tratados **(i)** cuando se haya obtenido el consentimiento del titular y sujeto a ciertos deberes especiales de información[95]; y **(ii)** cuando la ley así lo permita e indique expresamente la finalidad que deberá tener dicho tratamiento.

Según se observa de estas bases de legalidad, se puede advertir que el campo de acción que tendrán los órganos públicos para poder sustentar la implementación de mecanismos de videovigilancia y reconocimiento facial será más restringido que el que se configura actualmente a partir de la LPVP. En este contexto, de ser aprobado el Proyecto de Ley en este estado, va a ser necesario que los organismos públicos reevalúen todas aquellas implementaciones de estas tecnologías que estén operando, de forma de verificar si todavía cuentan con una base de legalidad que fundamente los tratamientos respectivos. Particular atención se deberá prestar a aquellos tratamientos que se basen en atribuciones genéricas de los organismos públicos y que no estén autorizados de forma expresa en la ley.

[95] Se requiere informar (i) la identificación del sistema biométrico usado; (ii) la finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados; (iii) el período durante el cual los datos biométricos serán utilizados; y (iv) la forma en el que el titular puede ejercer sus derechos

6.
Acciones relevantes del Consejo para la Transparencia asociadas a mecanismos de videovigilancia y sistemas de reconocimiento facial

En el rol del Consejo para la Transparencia[96] respecto a la protección de datos personales podemos diferenciar dos ámbitos claramente definidos. Por una parte, como órgano encargado del cumplimiento de las normas sobre transparencia y derecho de acceso a la información pública, en virtud de las cuales ha tenido que interpretar profusamente la causal de reserva establecida en el artículo 21 número 2 de la Ley de Transparencia. Y, por otra parte, como órgano que, en virtud de lo dispuesto en la letra m) del artículo 33 de la Ley de Transparencia, tiene la función legal de velar por el adecuado cumplimiento de la Ley N°19.628, por parte de los órganos de la Administración del Estado.

En este segundo rol, el Consejo para la Transparencia ha efectuado diversas acciones para instar a los servicios públicos, tales como los organismos de la administración central ("OAC"), municipalidades u organismos autónomos, a dar cumplimiento a la LPVP y ser rigurosos en el cuidado de los datos personales de los ciudadanos. De esta manera, por medio de oficios, ha solicitado a los servicios públicos información respecto de prácticas, iniciativas o gestiones que tienen relación con mecanismos de videovigilancia o reconocimiento facial, y que podrían poner en riesgo el derecho a la protección de datos de las personas; así como ha formulado diversas recomendaciones sobre el establecimiento de estándares adecuados de protección de datos personales cuando se utilizan esos mecanismos. En términos estadísticos, observamos los siguientes datos sobre estos oficios:

[96] El Consejo para la Transparencia corresponde a una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, creada por la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado.

- Entre 2015 y 2021 se han despachado 34 oficios cuyas materias refieren a temáticas de videovigilancia (53%) o reconocimiento facial (41%), el cual un 80% de ellos se concentran entre 2017 y 2020. Además, también existen oficios respecto al tratamiento de datos personales que contienen ambos mecanismos (6%).

- Por otra parte, un 65% de los oficios enviados a instituciones públicas tuvieron como objetivo pronunciarse sobre iniciativas que podían contravenir la LPVP, tales como la implementación de globos aerostáticos de vigilancia o sistemas de reconocimiento facial. En cuanto a las solicitudes de información relativas a mecanismos de videovigilancia, un 67% son dirigidas a municipios y un 33% a OAC. En cambio, en el reconocimiento facial es al revés, un 62% de las solicitudes son dirigidas a OAC, mientras que un 31% son dirigidos a municipalidades. Se podría deducir, en principio, que los OAC implementan más mecanismos de reconocimiento facial y los municipios sistemas de videovigilancia, no obstante que puede ocurrir que existan proyectos de estas características que sean posteriores o que han sido todavía conocidos públicamente, que pudieran alterar esta situación.

- Un 26% de los oficios tienen por objeto formular recomendaciones para implementar estándares de protección de datos. Dichos oficios se alinean con las solicitudes de iniciativas que ponen en riesgo la protección de datos, pues la mayoría de las recomendaciones en reconocimiento facial son dirigidas a las OAC (100%), mientras que la mayoría de las recomendaciones en videovigilancia son para los municipios (68%).

- El 9% de los oficios restantes tienen como objetivo dar respuesta a algún requerimiento realizado por otra institución pública o dar aviso de inspecciones para indagar un correcto desempeño en la materia.

En este escenario, y sin perjuicio que más adelante se detallan los amparos al derecho de acceso a la información que ha resuelto el Consejo en relación con esta materia, es pertinente destacar las siguientes acciones vinculadas con recomendaciones, requerimientos y solicitudes de información que ha realizado el Consejo y que han tenido como foco el tratamiento de datos personales que, instituciones públicas en Chile, han realizado en el contexto de la utilización de mecanismos de videovigilancia y sistemas de reconocimiento facial[97]:

[97] Estas acciones particulares se enmarcan dentro del marco general que dispone las Recomendaciones del CPLT que, como dijimos, fueron actualizadas a fines del año 2020 y contienen una regulación exhaustiva que busca orientar y perfeccionar el estándar de cumplimiento de la LPVP por parte de los órganos de la Administración del Estado.

a) Recomendaciones del Consejo para la Transparencia sobre la instalación de dispositivos de videovigilancia por parte de las municipalidades

Estas recomendaciones se dictaron mediante el Oficio N°2309, de 6 de marzo de 2017, del Consejo para la Transparencia, se dirigieron a todas las municipalidades del país, y estuvieron en vigencia hasta la dictación del Oficio N°[****] que lo reemplazó. Su objetivo fue regular el uso de dispositivos de videovigilancia con fines de seguridad comunal de forma de tutelar y garantizar el derecho a la propia imagen y la plena protección de los datos personales de los individuos. Estas recomendaciones se elaboraron fundamentalmente en torno a la sentencia de la Excelentísima Corte Suprema Rol N°18.458-2016, del 1 de junio de 2016; y la jurisprudencia del Consejo, en particular, la decisión C2493-15, de 26 de enero de 2016. El Oficio N°2309 dividió su contenido en dos partes. En primer lugar, se refirió a ciertos aspectos generales sobre videovigilancia y protección de datos. Luego, en la segunda parte se contenían las recomendaciones propiamente tal.

b) ctualización sobre el contenido y alcance del Oficio N°2309 en lo que respecta a la finalidad de la grabación, la retención de los registros, y su acceso por parte de los titulares de datos

En noviembre de 2021, el Consejo para la Transparencia remitió el Oficio N°[***], de [****] del 2021, a todas las municipalidades del país, y el cual tuvo por objeto actualizar las recomendaciones realizadas respecto a la instalación y uso de dispositivos de videovigilancia por parte de las municipalidades, efectuando precisiones sobre la finalidad de la grabación, la retención de los registros, y su acceso por parte de los titulares de datos. Con fines de orden, este Oficio dejó sin efecto el Oficio N°2309, sin perjuicio de mantener gran parte de su regulación original.

En cuanto a los aspectos generales, destacamos los siguientes planteamientos del Oficio:

i. La imagen de las personas constituye un dato personal sensible protegido por ley.

ii. La grabación y captación de imágenes son tratamientos de datos personales sensibles. Dicho tratamiento, para efectos de su legitimidad, sólo puede efectuarse cuando el responsable del banco de datos cuente con una base habilitante.

iii. Los municipios tienen competencias legales relacionadas con fines de seguridad comunal.

iv. El municipio es el responsable del banco de datos en el tratamiento de las imágenes, aun cuando dicho tratamiento sea encargado a un tercero.

Por su parte, las recomendaciones realizadas fueron:

i. La grabación y captación de imágenes deberá efectuarse para el cumplimiento de sus funciones legales, dentro de su ámbito de competencias.

ii. Las imágenes sólo podrán ser captadas en lugares públicos. Excepcionalmente podrán ser captadas en lugares privados abiertos cuando se trate de la persecución por un hecho constitutivo de delito flagrante.

iii. El municipio es el responsable del banco de datos en relación a los datos personales que sean tratados mediante el uso del sistema de videovigilancia.

iv. Se deben implementar medidas para garantizar la seguridad de las imágenes que sean captadas, de forma de proteger los datos personales tratados en dicho contexto.

v. Las grabaciones deben ser eliminadas dentro de los 30 días desde que estas hayan sido grabadas o captadas, salvo la verificación de un circunstancia de excepción que justifique un almacenamiento prolongado. Por su parte, las municipalidades deben ser transparentes en cuanto a los plazos y condiciones de retención y eliminación de las grabaciones.

vi. Un funcionario municipal deberá certificar que las imágenes hayan sido grabadas en los lugares permitidos.

vii. La municipalidad debe garantizar el ejercicio de los derechos de las personas para acceder a las captaciones donde conste su imagen. La entrega de copia de las captaciones se efectuará al titular de datos (o su apoderado) sin contener datos personales de terceros.

viii. La municipalidad deberá inscribir el banco de imágenes en el Servicio de Registro Civil e Identificación.

ix. El municipio deberá informar al Consejo para la Transparencia sobre las medidas adoptadas.

Si bien en estas recomendaciones no se establecieron directrices específicas para la tecnología de reconocimiento facial, se puede advertir que este contempla criterios generales de uso de dispositivos de grabación audiovisual que igualmente pueden impactar en el despliegue de tal tecnología por parte de las municipalidades.

c) Observaciones sobre el uso de sistema piloto de reconocimiento facial para control de ingreso de público a casinos de juego

Este oficio[98] tuvo como objeto pronunciarse sobre la implementación, por parte del Grupo Dreams, de un programa piloto de reconocimiento facial para el ingreso de público a los casinos de juego que opera. Entre las observaciones que hizo el Consejo a este programa piloto, podemos destacar las siguientes:

i. Los sistemas de reconocimiento facial implican el tratamiento de datos personales y de datos personales de carácter sensibles y, por tanto, se requiere dar estricto cumplimiento a lo que al efecto dispone la Constitución Política y la LPVP.

ii. En virtud de lo anterior, se destacan una serie de obligaciones incluyendo la obtención de una base de legalidad; la estricta observancia del principio de finalidad en el tratamiento de datos personales; la observancia de las obligaciones de seguridad y confidencialidad en el tratamiento de datos; el respeto al ejercicio de los derechos ARCO; la observancia de las obligaciones de eliminación, modificación y bloqueo de datos que tiene el responsable; y la suscripción de mandatos robustos.

iii. Desde un punto de vista de la legislación vigente sobre protección de datos personales, la implementación de un sistema piloto de reconocimiento facial puede ser válidamente efectuada únicamente en la medida que los responsables del banco de datos resguarden debidamente los datos personales tratados mediante el cumplimiento permanente de la Constitución y la LPVP.

iv. Por último, cabe hacer presente que, el alto riesgo que supone para los titulares de datos el uso indiscriminado o indebido de un sistema de reconocimiento facial, impone a los responsables de datos un alto estándar de cumplimiento de la normativa, de forma que en todo momento se otorgue resguardo y respeto a los derechos fundamentales de las personas, incluyendo no solo el referido a la protección de datos personales, sino que los demás que puedan verse implicados, como el de protección a la vida privada y la no discriminación arbitraria.

[98] Oficio N°290, de 8 de octubre de 2021, del Consejo para la Transparencia.

d) Requerimientos sobre la conservación y acceso a los registros de dispositivos de videograbación y cámaras fotográficas portátiles utilizadas en el contexto de operativos policiales

Este oficio[99], dirigido al General Director de Carabineros de Chile, tuvo por objeto que dicha institución adoptara medidas en relación a la captación de imágenes por medio de dispositivos de videograbación y cámaras fotográficas portátiles, de forma de asegurar un adecuado ejercicio del derecho de acceso a la información pública. Entre estas medidas, se cuentan:

i. Asegurar y respetar el legítimo ejercicio del derecho de acceso a la información, respecto de cualquier documento o soporte informático, en el que se contengan los registros captados por funcionarios policiales.

ii. Asegurar y respetar los derechos de los titulares de las imágenes captadas, así como el ejercicio de los derechos contemplados en la LPVP.

iii. Conservar, de manera indefinida, las imágenes obtenidas por dispositivos de videograbación o cámaras fotográficas portátiles.

iv. Registrar previamente la utilización de dispositivos de videograbación o cámaras fotográficas portátiles.

v. Adoptar medidas de seguridad de la información, con ocasión del tratamiento de las imágenes, incluyendo medidas relativas a perfiles de acceso y encriptación.

[99] Oficio N°1828, de 29 de noviembre de 2019, del Consejo para la Transparencia.

e) Requerimientos de información sobre proyectos realizados por entidades públicas y privadas que utilizaban tecnología de reconocimiento facial en espacios abiertos al público

Desde hace varios años en Chile, entidades públicas y privadas han buscado implementar tecnología de reconocimiento facial en espacios abiertos al público con el objetivo fundamental de combatir la criminalidad. Entre estos proyectos destacan los llevados a cabo por la municipalidad de Las Condes en dicha comuna[100]; por la municipalidad de Lo Barnechea en dicha comuna[101]; por la intendencia de la Región Metropolitana[102]; por el centro comercial Mall Plaza Los Dominicos[103]; y por el Metro Regional de Valparaíso S.A. (Merval)[104]. Todos proyectos respecto de los cuales el Consejo hizo requerimientos de información y antecedentes relevantes sobre la tecnología aplicada, y la forma en que las instituciones estaban dando cumplimiento al marco normativo vigente.

Si bien el objeto principal de estos requerimientos fue la obtención de información, de dichos oficios también es posible desprender criterios relevantes del Consejo en relación a esta tecnología:

i. El uso de tecnología de reconocimiento facial puede generar vulneraciones al derecho de protección de datos personales y al derecho de respeto a la vida privada, independiente de que el responsable del banco de datos sea una entidad pública o privada. Estos generalmente implican una operación altamente intrusiva que puede no ser proporcional en relación a los fines que persiguen.

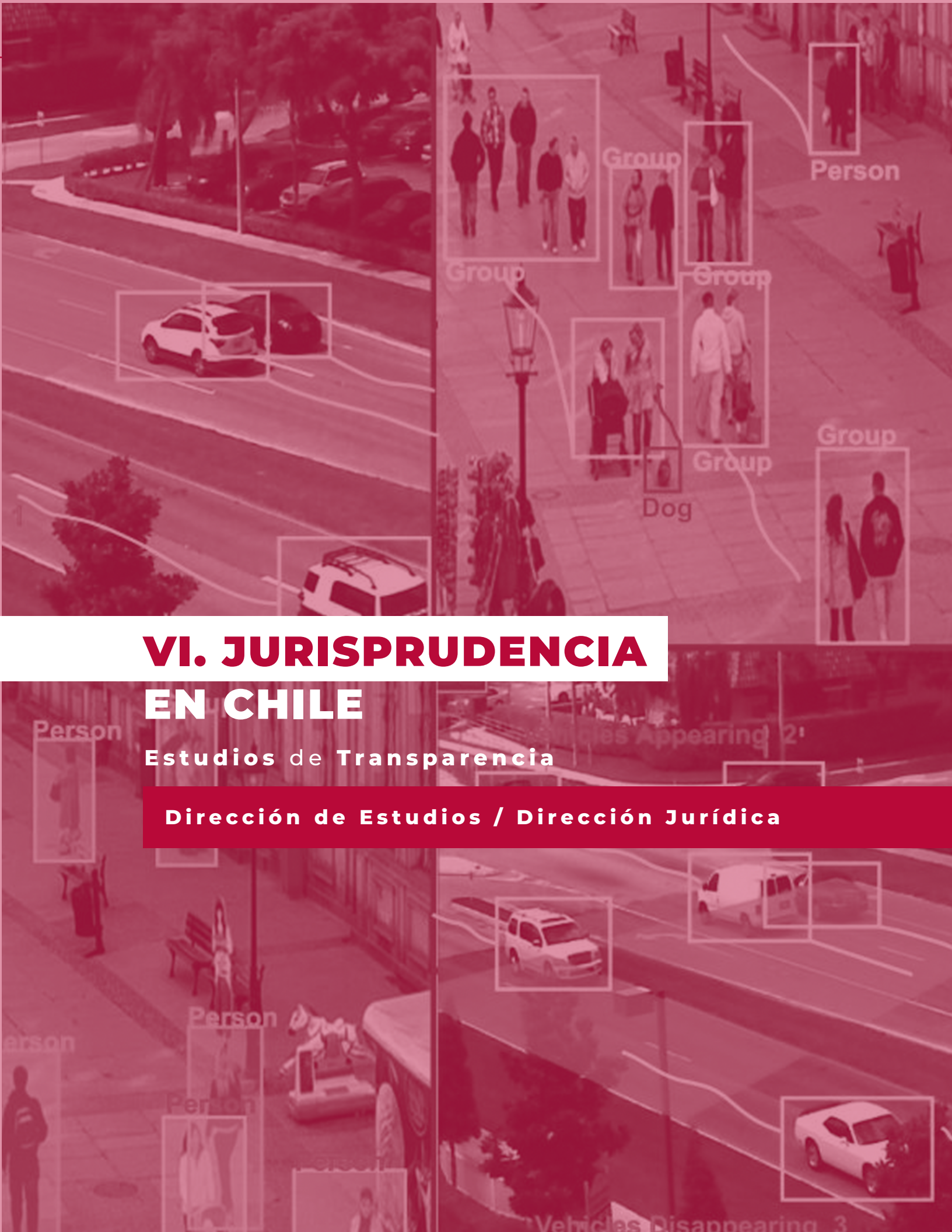
ii. Los sistemas de reconocimiento facial tienen la potencialidad de generar falsos positivos.

iii. El uso de tecnología de reconocimiento facial implica la captación de imágenes de rostros de personas naturales que corresponde a datos personales sensibles de carácter biométrico y, por tanto, su tratamiento en Chile requiere dar cumplimiento a la LPVP.

iv. En términos de base de legalidad, el tratamiento de estos datos personales requiere necesariamente contar de una autorización legal o del consentimiento expreso del titular afectado.

v. Para abordar adecuadamente esta clase de tecnología, en Chile se requiere modificar y robustecer la LPVP.

[100] Oficio N°1936, de 18 de diciembre de 2019, del Consejo para la Transparencia, y Oficio N°714, de 18 de mayo de 2020, del Consejo para la Transparencia.
[101] Oficio N°4765, de 11 de octubre de 2018, del Consejo para la Transparencia.
[102] Oficio N°1935, de 18 de diciembre de 2019, del Consejo para la Transparencia.
[103] Oficio N°5091, de 29 de noviembre de 2018, del Consejo para la Transparencia; Oficio N°5092, de 29 de noviembre de 2018, del Consejo para la Transparencia; y Oficio N°5093, de 29 de noviembre de 2018.
[104] Oficio N°4209, de 31 de agosto de 2018, del Consejo para la Transparencia.



VI. JURISPRUDENCIA EN CHILE

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

1. Criterios de amparos relevantes del CPLT

En términos de amparos al derecho de acceso a la información pública resueltos por el Consejo para la Transparencia relacionados con los mecanismos analizados bajo este trabajo cabe señalar que, si bien los amparos y sus considerandos son aplicables a cada caso en concreto conforme sus propias particularidades, de la revisión de alguno de ellos se pueden observar ciertos criterios relevantes que, a partir de su razonamiento, pueden llegar a influir en la futura decisión de casos similares.

En este sentido, observamos -en términos generales- dos grupos de decisiones, un primer grupo sobre grabaciones de cámaras de videovigilancia en general, y otro relativo específicamente a grabaciones de cámaras que portaban funcionarios de Carabineros en ejercicio de sus funciones.

Además de las diferencias obvias entre estos dos grupos, se observa que el sustento que da origen a estos casos difiere entre sí. En el caso de solicitudes relativas a cámaras de videovigilancia en general, observamos solicitudes en donde los requirentes solicitan las captaciones porque ellos aparecen en las mismas y son necesarias para satisfacer un fin o derecho ulterior, como ejercer una acción judicial a causa de un accidente. En este caso, el derecho de acceso a la información resulta un medio útil para acceder a dichas captaciones en el entendido que fueron realizadas por un sujeto obligado por la Ley de Transparencia. Lo interesante, a nivel de datos personales, es que el Consejo reconoce en este punto la utilidad del derecho de acceso a la información como una forma válida de ejercer o garantizar el derecho de acceso a los datos personales que establece la LPVP, lo cual ha manifestado tanto en su jurisprudencia administrativa como en las Recomendaciones del CPLT. Como ya vimos, la LPVP tiene serias deficiencias, encontrándose, entre ellas, precisamente el procedimiento de tutela de derechos ARCO, por ello, el mecanismo de acceso a la información dispuesto en la Ley de Transparencia se presenta como una forma más expedita de obtener acceso a información personal respecto de la cual el requirente es titular, y que se encuentra en poder de un órgano público.

Ello reforzado además por la circunstancia de existir una autoridad de control a quien recurrir en caso de denegación del acceso, a saber, el Consejo para la Transparencia.

Por su parte, en el caso de las solicitudes de grabaciones realizadas por cámaras portadas por funcionarios de Carabineros, observamos que estas tienen un fuerte componente de rendición de cuentas y de control del ejercicio de la función pública. Desde un punto de vista de datos personales, la controversia en estos casos se ha concentrado en la necesidad de que las captaciones que sean entregadas no contengan datos personales de terceros.

Al margen de estas distinciones cabe precisar que, en ambos casos, el Consejo ha ido tendiendo a la entrega de registros obtenidos mediante sistemas de videovigilancia y operados por entidades públicas, pero bajo un estricto apego al derecho de protección de datos de los terceros que pueden aparecer o ser identificados a partir de esas imágenes. Para ello, el Consejo tiende a utilizar el principio de divisibilidad que reconoce la Ley de Transparencia en el literal e) de su artículo 11, y que establece que “si un acto administrativo contiene información que puede ser conocida e información que debe denegarse en virtud de causa legal, se dará acceso a la primera y no a la segunda”.

Bajo este escenario, a continuación, presentamos algunos de los criterios desarrollados en estos dos grupos de amparos, por parte del Consejo.

a) En relación a grabaciones de cámaras de videovigilancia en general el Consejo ha sostenido[105]:

- Que el núcleo del derecho de acceso a la información es servir de derecho llave para el ejercicio de otros derechos fundamentales, como puede ser, constituir prueba suficiente para evaluar la pertinencia de iniciar una acción ante los órganos que ejercen jurisdicción.

- Que los titulares de datos personales pueden ejercer el derecho de acceso a la información pública consagrado en el artículo 10 de la Ley de Transparencia para requerir, a las autoridades sujetas a dicha ley, acceso a aquellas captaciones que se hayan generado mediante la utilización de sistemas de cámaras de vigilancia y donde ellos figuren.

- Que la entrega de estas captaciones debe hacerse dando estricto cumplimiento a la Instrucción General N°10, punto 4.3. del Consejo, que dispone que *"cuando la información requerida contenga datos de carácter personal y el peticionario indique ser su titular, sólo se procederá a la entrega presencial y quien la efectúe deberá verificar que la información sea retirada por quien efectivamente tenga dicha calidad o por su apoderado conforme a lo dispuesto en el artículo 22 de la Ley N° 19.880"*.

  Con respecto a este último criterio, cabe señalar que, con ocasión de la pandemia y en línea con lo dispuesto en las Recomendaciones del CPLT, con el objeto de facilitar la entrega de la información, el Consejo ha indicado que ella también podrá efectuarse por medios electrónicos, para lo cual deberá utilizarse un mecanismo de autenticación idóneo y seguro, como Clave Única o similares, que garanticen la confidencialidad, disponibilidad e integridad de la información transmitida, cumpliendo además con el deber de información y el principio de seguridad que establece la Ley N°19.628.

[105] Amparos C148-21 y C4687-20 del Consejo para la Transparencia.

b) En relación a grabaciones de cámaras portadas por funcionarios de Carabineros el Consejo ha señalado[106]

- Que las imágenes captadas a través de dispositivos de video grabación por parte de Carabineros de Chile en cumplimiento de funciones destinadas a la mantención y resguardo del orden público constituyen, en principio, información pública.

- Dentro de los registros se incluyen imágenes de personas naturales, por lo que es información que contiene datos personales.

- La información requerida puede ser entregada difuminando los rostros de las personas y otros elementos que permitan su individualización, contenidos en las grabaciones solicitadas, resguardando de esta forma la protección de los datos personales y aplicando el principio de divisibilidad que orienta el procedimiento de acceso a la información que obra en poder de los órganos de la Administración del Estado.

- En dicho contexto, corresponde la entrega de los registros requeridos, ya que se trata de información que obra en poder de Carabineros, registrada en cumplimiento de funciones públicas.

- Sin perjuicio de lo anterior, en aplicación del principio de divisibilidad, Carabineros debe, en forma previa a la entrega de los registros, proteger los datos personales que pudieren estar contenidos en la información cuya entrega se ordena.

Los criterios anteriormente descritos, correspondientes a los criterios vigentes, difieren del que anteriormente había adoptado el Consejo en torno a rechazar solicitudes de acceso a grabaciones efectuadas por cámaras de vigilancia[107] atendido, fundamentalmente, a que ellas contenían datos personales y sensibles cuya divulgación podría afectar los derechos fundamentales a la intimidad, privacidad y propia imagen. Esto, en aplicación de la hipótesis de reserva prevista en el artículo 21 N°2 de la Ley de Transparencia[108].

Por último, destacamos un grupo de casos en donde se ha ejercido el derecho de acceso a la información, en relación a captaciones realizadas por sistemas de videovigilancia, que han sido rechazados por el Consejo por haberse determinado que la información solicitada no obraba en poder del organismo al cual le fue requerida o no existía. No disponiendo el Consejo de antecedentes suficientes que permitieran desvirtuar lo expresado por el organismo requerido[109].

[106] Amparos C8436-19, C163-21, C2742-21, C2745-21, C975-21, C8066-20, C8051-20, C2311-21, C1753-21 y C8279-20 del Consejo para la Transparencia. Este criterio ha sido seguido por la Corte de Apelaciones de Santiago al conocer recurso de legalidad en causa Rol N°231-2021.

[107] Por ejemplo, en amparos del Consejo para la Transparencia C6644-19, C1295-19, C5026-18, C67-18, C2493-15, C1505-17, C3006-17, C4217-17 y C385-18.

[108] Esta hipótesis de reserva señala que se podrá denegar total o parcialmente el acceso a la información "Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico"

[109] Por ejemplo, amparos C3432-21, C2766-21 y C1008-21.

2. Jurisprudencia de los tribunales de justicia

Caso globos de vigilancia.

Este caso corresponde a dos acciones de protección interpuestas ante la Corte de Apelaciones de Santiago, que luego fueron conocidas en apelación por la Corte Suprema. Dado que las sentencias en ambos procedimientos son, en lo sustantivo, similares, procedemos a tratarlas simultáneamente a continuación.

a) Sentencias de Corte de Apelaciones de Santiago. Roles N°81.627-2015 y N°82.289-2015, ambas del 4 de marzo de 2016.

El 4 de marzo de 2016, la Corte de Apelaciones de Santiago acogió los recursos de protección presentados por vecinos de las comunas de Las Condes y Lo Barnechea, en contra de las municipalidades de dichas comunas, con motivo de la implementación de un sistema de videovigilancia instalado en globos aerostáticos, ordenando el cese de las actividades de captación, almacenamiento y procesamiento de imágenes que se realizaba a través de dichos aparatos. Los recurrentes estimaron conculcados los derechos fundamentales contemplados en los numerales 4, 5, y 24 del artículo 19 de la Constitución Política.

La Corte acogió el recurso al verificar que las bases administrativas y técnicas establecidas por los municipios no contemplaban ningún tipo de resguardo para evitar que la visión de las cámaras cubra vistas áreas en que los vecinos ejecutan actividades propias de su vida privada e intimidad. También desestimó la legalidad del actuar de las municipalidades, indicando que no se pueden amparar únicamente en el cumplimiento de trámites administrativos ante la Dirección General de Aeronáutica Civil (DGAC) y la respectiva autorización de ese organismo para efectos de grabar imágenes con las cámaras de los globos de vigilancia.

Por su parte, la Corte estableció que, aunque la Ley N°18.695, Orgánica Constitucional de Municipalidades, otorgue facultades a los municipios, esto no implica que puedan ejercerlas de cualquier modo, debiendo respetar los derechos esenciales que emanan de la naturaleza humana conforme establece el artículo 5 inciso segundo de la Constitución Política. La Corte sostuvo que la Constitución, en su artículo 7, en conjunto con los artículos 1 y 20 de la LPVP, requieren que el tratamiento de datos se realice de la forma que prescriba la ley, respetando los derechos fundamentales.

Finalmente, es relevante indicar que la Corte puso también énfasis en el hecho de que la captación de las imágenes no era realizada por funcionarios públicos que formen parte de las plantas del municipio, sino por trabajadores contratados por la empresa que prestaba el servicio de vigilancia, los cuales no tendrían autorización para ello.

b) Sentencias de Corte Suprema. Roles N°18.458-2016 y N°18.481-2016, ambas del 1 de junio de 2016.

Con fecha 1 de junio de 2016, la Corte Suprema acogió los recursos de apelación presentados por las municipalidades en contra de las sentencias de Corte de Apelaciones que habían ordenado cesar las actividades de los globos de vigilancia, revocando dichas sentencias. En su lugar, decidió que los globos pueden seguir operando bajo el siguiente régimen de autorización:

i. Las cámaras sólo pueden grabar lugares públicos, y ocasionalmente espacios privados abiertos, cuando se trate del seguimiento de un hecho que pueda constituir un delito.

ii. Un inspector municipal deberá certificar, una vez al mes, que las cámaras no hayan captado imágenes de naturaleza privada.

iii. Las grabaciones deberán destruirse luego de 30 días, salvo si en ellas se ha captado un ilícito penal u otra falta, en cuyo caso la municipalidad adoptará las medidas para su pronta entrega a los órganos competentes.

iv. Se deberá permitir el acceso a las grabaciones a todo ciudadano que lo requiera, para lo cual deberá presentar una solicitud al municipio, debiendo indicar el día en que presumiblemente fue grabado. Se les ordena a los municipios recurridos establecer un procedimiento que permita a los ciudadanos el efectivo ejercicio de este derecho.

Dentro de análisis de la Corte para arribar a esta decisión se observa que, en primer lugar, rechazó el criterio que tuvo la Corte de Apelaciones respecto a que existiría una ilegalidad en que los globos de videovigilancia hayan sido operados por trabajadores de una empresa privada, indicando que no puede inferirse que la contratación de servicios de televigilancia, mediante el procedimiento de la Ley N°19.886, signifique una delegación de potestades por parte de las municipalidades. Luego, establece que esta clase de cámaras ha sido reconocida por el legislador como un instrumento eficaz para la seguridad ciudadana, y es por eso que el ordenamiento las ha admitido en una variedad de recintos, no pudiendo pretenderse una mayor expectativa de privacidad en el espacio público. Por último, la Corte reconoce que los globos de vigilancia pueden afectar el derecho a la intimidad o a la propia imagen si se utilizan para observar espacios privados.

Bajo estas sentencias la Corte Suprema admite que la competencia para utilizar sistemas de videovigilancia por las municipalidades estaría fundada en las atribuciones de "apoyo" y "fomento a medidas de prevención en materias de seguridad ciudadana" (art. 4 letra j) de la Ley N°18.695, Orgánica Constitucional de Municipalidades). A nivel de datos personales, no se observa un desarrollo particular del artículo 20 de la LPVP por parte del máximo tribunal, sin perjuicio de implícitamente establecer que las competencias mencionadas con las que gozan las municipalidades serían suficientes para justificar un tratamiento de datos personales recolectados por cámaras de vigilancia con fines de seguridad comunal, sin necesidad de obtener el consentimiento del titular. No obstante, también estaría dando cuenta de que dichas competencias requieren de cierto control adicional en su ejercicio, el que estaría dado por el régimen de autorización que la Corte establece y que hoy no estaría consagrado en la ley[110].

Por otro lado, si bien estos no son casos específicos de reconocimiento facial, constituyen antecedentes jurisprudenciales relevantes en Chile en torno al uso de cámaras de videovigilancia de alta tecnología que pueden sentar la base para futuros pronunciamientos en la materia. No obstante, esto, cabe también tener presente que el artículo 3 del Código Civil establece el efecto relativo de las sentencias al indicar que las sentencias judiciales no tienen fuerza obligatoria sino respecto de las causas en que actualmente se pronunciaren; todo lo cual deja abierta la posibilidad de que en un futuro pueda existir un cambio de criterio en este tema por parte de los tribunales de justicia.

[110] Cabe destacar que el fallo ha sido comentado ampliamente por la doctrina en Chile. Véase Ramírez, Tomás. (2016). Nuevas tecnologías al servicio de la seguridad pública y su impacto en la privacidad: criterios de ponderación. Revista Chilena de Derecho y Tecnología, Vol. 5, N° 1, pp. 57-86; Lovera, Domingo. (2017). Privacidad: La vigilancia en espacios públicos. En Vial, Tomás (Ed.), Informe Anual sobre Derechos Humanos en Chile 2017 (pp. 383-417). Ediciones Diego Portales; Mohor, Elías (24 de mayo de 2017). Globos y drones de vigilancia: seguridad y privacidad ¿qué derecho debe prevalecer? Hipervínculos. https://www.hipervinculos.cl/globos-y-drones-de-vigilancia-seguridad-y-privacidad-que-derecho-debe-prevalecer/

Caso drones.
a) Sentencias de Corte de Apelaciones de Santiago. Rol N°34.360-2017 de 21 de agosto de 2017.

El 21 de agosto de 2017, la Corte de Apelaciones de Santiago rechazó un recurso de protección interpuesto en contra de la Municipalidad de Las Condes debido a la implementación de un sistema de vigilancia a través de drones con cámaras aéreas de alta tecnología. La sentencia descartó las ilegalidades y arbitrariedades alegadas y la afectación de derechos fundamentales.

Uno de los puntos discutidos consistió en que este sistema de vigilancia infringía el artículo 20 de la LPVP ya que, a juicio de los recurrentes, la Municipalidad de Las Condes no contaba con competencia para efectuar el tratamiento de datos sensibles que recababa, en particular la imagen de las personas. Sin embargo, la Corte ratificó la competencia del municipio, señalando que sobre la materia debe tenerse en consideración lo señalado por el Consejo para la Transparencia en su Oficio N°2309, de 6 de marzo de 2017, donde se indica que los municipios tienen competencias legales para operar dispositivos de video vigilancia con fines de seguridad comunal, estando dicha finalidad establecida en el Manual de Procedimientos "RPAS" elaborado por la Municipalidad. Bajo esta consideración, la Corte estableció que *"puede concluirse que la actividad desarrollada por el Municipio se ajusta a la competencia de este órgano comunal en relación a la implementación de medidas en el ámbito de la seguridad pública, y con ello el tratamiento de datos que realiza, no aparece contrario a la ley"* (considerado Decimosexto).

La segunda alegación de los recurrentes se sustentaba en un incumplimiento a la norma técnica DAN 151 de la Dirección General de Aeronáutica Civil (DGAC), lo cual también fue descartado por la Corte.

Por último, y luego de descartar ilegalidad o arbitrariedad en el actuar de la municipalidad, la Corte se refirió a los derechos fundamentales aducidos por los recurrentes. En relación al derecho a la vida privada, la Corte sostuvo que "*la implementación de una televigilancia no resulta atentatoria a la vida privada de los actores si ellos llegan a circular por los espacios públicos donde sobrevuelan los drones en atención a la forma como ha sido implementada la medida por el Municipio, pues ha existido una regulación de la actividad que permite conocer en forma previa, los lugares donde se realiza la actividad, el horario, las personas encargadas de ello, las situaciones en que se procederá a la grabación, la duración en su mantención, y la forma que tienen los ciudadanos de acceder a ellas; se trata además de vistas panorámicas de dichos lugares, que dejan a salvaguarda el anonimato de los transeúntes, a menos, claro está de situaciones delictivas o de emergencia en que el anonimato puede decrecer en pro de otros fines legítimos de seguridad*".

b) Sentencias de Corte Suprema. Rol N°38.527-2017 de 11 de diciembre de 2017.

El 11 de diciembre de 2017 la Corte Suprema confirmó la sentencia de la Corte de Apelaciones de Santiago que rechazó el recurso de protección interpuesto en contra de la Municipalidad de Las Condes. El fallo de la Corte solo confirmó la sentencia, sin efectuar ningún tipo de declaración o fundamentación.

Al igual que con el caso de globos de vigilancia, este fallo también ha sido criticado por la doctrina nacional[111].

[111] Véase Contreras, Pablo (2021).

VII. NIVEL DE CUMPLIMIENTO INSTITUCIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

Como se ha mencionado, en Chile, la LPVP regula que el tratamiento de datos personales, realizado por organismos públicos y privados, debe estar sujeto a ciertas disposiciones contenidas en la misma ley[112]. En el caso específico de los servicios u organismos de la administración del Estado, se dispone expresamente en la ley que éstos pueden tratar datos personales, siempre y cuando lo hagan acorde a las finalidades permitidas y respetando el pleno ejercicio de los derechos fundamentales de los titulares de los datos. Como obligación adicional, es deber de los servicios públicos proporcionar al Servicio de Registro Civil e Identificación antecedentes sobre los bancos o bases de datos personales en su poder, para efectos de su inscripción.

Es común que los servicios públicos traten datos personales para identificar a sus usuarios y cumplir con la finalidad o finalidades asociadas a sus funciones legales, dentro del ámbito de su competencia, incluidos datos provenientes de tecnologías como la videovigilancia y el reconocimiento facial[113]. En términos generales, uno de los requisitos para el tratamiento de datos personales es contar con una base de legalidad que habilite dicho tratamiento. Como ya señalamos, las bases de legalidad que podrían justificar la implementación de sistemas de videovigilancia o reconocimiento facial son **(i)** cuando el tratamiento esté expresamente contenido en una norma de rango legal; **(ii)** cuando el tratamiento, no estando autorizado expresamente, resulte imprescindible (criterio de necesidad) para el debido cumplimiento de una función pública establecida por ley y forme parte esencial de las materias de su competencia; o **(iii)** cuando se ha obtenido el consentimiento del titular de datos en los términos del artículo 4 de la LPVP.

En base al estudio sobre Protección de Datos Personales realizado por el Consejo para la Transparencia en 2019, un 73% de las instituciones de la administración del Estado contaba con una base de datos con información personal. Entre dichas instituciones se encuentran las municipalidades, ministerios, subsecretarías, servicios, organismos autónomos, hospitales y universidades públicas. La información tratada va a depender de la competencia institucional: si es un hospital debiese tratar datos asociados a la salud. Si es una universidad, debiese tratar información asociada a resultados académicos. Además, la mayoría de las instituciones también tratan datos asociados a la identificación de las personas como nombres, apellidos, dirección, teléfono, etc.

[112] Véase https://www.bcn.cl/leychile/navegar?idNorma=141599.

[113] Véase https://www.bcn.cl/leychile/navegar?idNorma=141599.

Como se señaló anteriormente, cada institución o servicio es responsable de informar al Servicio de Registro Civil e Identificación las bases de datos con información personal que se encuentran en su poder, constatando el fundamento jurídico de su existencia, su finalidad, los tipos de datos almacenados y la descripción del universo de personas que comprende. También deben comunicar cualquier cambio de los elementos en las bases de datos dentro de los quince días en que éstos se produzcan[114].

De las bases de datos con información personal en poder de servicios públicos, solo un 35% están inscritas en el Servicio de Registro Civil e Identificación, siendo las municipalidades las entidades públicas que menos informan las bases que tratan[115]. Lo anterior, puede facilitar un posible uso discrecional de los datos personales, reflejando además una carencia de cultura institucional respecto a la protección de datos personales, puesto que un 12% de los servicios no sabe cómo proceder para informar al Registro Civil las bases con información personal que poseen.

Advirtiendo el sinnúmero de debilidades existentes en la LPVP, es importante monitorear la incorporación de conductas proactivas del cuidado de datos personales. La incorporación de políticas de privacidad, estándares de ciberseguridad, protocolos de intercambio de información con otras entidades y la designación de un funcionario a cargo de la correcta administración de las bases de datos es fundamental para generar confianza en la ciudadanía respecto al uso de los datos personales que realizan los servicios públicos. A modo de ejemplo, sólo un 24% de las instituciones ha designado a un encargado de protección de datos, los que generalmente corresponden a encargados de transparencia, encargados de tecnologías de información y directores o encargados de control. Por otra parte, las municipalidades son las instituciones que más tratarían datos personales, pues satisfacen las necesidades sociales, económicas y culturales de su comuna. Otorgan beneficios sociales como los subsidios, emiten patentes comerciales, registran información de tránsito y se ocupan de la seguridad comunal, entre muchas otras actividades. Sin embargo, y aunque no es exclusivo de ellas, son las instituciones que menos cuentan con una política de privacidad de datos personales.

[114] Un ejemplo de ello es la Comisaría Virtual. En dicha base, registrada en el Registro Civil, se identifica el organismo público: Carabineros de Chile. El fundamento jurídico: "Artículo 101 de la Constitución Política de la República. Art. 1° y 3° Ley N°18.961, Orgánica de Carabineros de Chile. Ley N°18.415, Orgánica Constitucional de Estados de Excepción, que, en general, establece los efectos de la declaración de estado de excepción constitucional y de catástrofe. Decreto N°269, de 12 de junio de 2020, que prorroga declaración de estado de excepción constitucional de catástrofe, por calamidad pública, en el territorio de Chile, por el lapso que indica". La descripción del universo: "Cualquier persona que resida o transite por el país y que pretenda realizar una constancia u obtener un permiso o salvoconducto". La finalidad: "(i) Mantener el registro de las personas naturales que han iniciado de forma electrónica diversos trámites de constancias ante Carabineros de Chile. (ii) Mantener el registro de las personales naturales o jurídicas que han solicitado un permiso temporal de desplazamiento o salvoconducto". Y la identificación del tipo de información almacenada: Domicilio; Estado Civil; Nombre y Apellidos; Edad; Nacionalidad; RUN; Correo Electrónico y Teléfono.

[115] Estudio de Protección de Datos Personales, CPLT, 2019.

En 2019 solo un 28% de los servicios públicos contaba con una política de privacidad de los cuales un poco más de la mitad de ellos la publicaba en su sitio web. El déficit institucional para adoptar políticas de privacidad puede generar incertidumbre en los usuarios y desinformación sobre el tratamiento futuro de sus datos personales. Aun así, las pocas instituciones públicas que cuentan con una política de privacidad generalmente cumplen con ciertos estándares de tratamiento de datos personales, tales como establecer medidas de seguridad; identificar a la institución responsable del tratamiento de datos; declarar las condiciones y garantías sobre el tratamiento de datos y emitir una declaración expresa sobre los derechos de los titulares de los datos personales, entre otros.

El déficit de protocolos robustos de privacidad de datos personales en las instituciones públicas coincide con la falta de estándares de ciberseguridad aplicables a las bases de datos personales, puesto que sólo un 34% de las instituciones públicas cuenta con ellos. Muchos servicios públicos poseen datos sensibles, esto es datos personales que se refieren a las características físicas, morales o hechos o circunstancias de su vida privada o íntima. La información de salud o datos recabados de tecnologías de información, como la videovigilancia y el reconocimiento facial, se pueden considerar datos sensibles. Si dichos datos no se resguardan con un debido procedimiento, son un blanco fácil para los ciberataques y sus consecuencias como una posible extorsión. Inclusive, del poco porcentaje de servicios que incorporan políticas de ciberseguridad, algunas de ellas ni siquiera cuentan con alguna certificación externa que garantice la seguridad de la información. Una gran parte de las agencias de protección de datos recomiendan a las instituciones públicas que tratan datos personales “adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado”[116]. Entre estas medidas se encuentran: designar un responsable de la seguridad de la información; educar el comportamiento de los funcionarios; poseer un registro de incidencias; controlar el acceso a información personal; control de identificación y autenticación para acceder a ficheros con información personal y sensible; gestión de soportes; copias de respaldo de datos; auditorías y traslado de información[117].

[116] Guía de Seguridad de los Datos. Agencia Española de Protección de Datos, 2008, página 4.

[117] Ibid.

La mayoría de las políticas públicas requieren de información intersectorial para poder focalizarlas. Por ejemplo, la Subvención Escolar Preferencial para mejorar la equidad y calidad educativa en establecimientos educacionales requiere de la caracterización de los estudiantes para definirlos como prioritarios y preferentes y así entregar los recursos correspondientes a los sostenedores. Para ello, el Ministerio de Educación necesita informarse de la situación socioeconómica de los estudiantes y ejecutar su política y probablemente recurriría a las bases de datos con información personal del Registro Social de Hogares del Ministerio de Desarrollo Social y Familia. Un 10% de los servicios públicos intercambia información personal a través de convenios según la razón expuesta: los servicios de planificación como los ministerios y subsecretarías necesitan de un abanico de información personal para poder sectorializar y focalizar sus políticas públicas. La verificación de datos personales de beneficiarios de algún programa o política pública abarca un 63% del público objetivo de los convenios y la información intercambiada se centra en antecedentes financieros.

Existen acciones de amparo ante el Consejo para la Transparencia por denegación de acceso a información cuyas materias se refieren a la protección de datos personales, aunque los amparos asociados a videovigilancia y reconocimiento facial representan un porcentaje menor comparadas con otras temáticas[118]. Desde 2019 se contabilizan 336 casos de amparos y reclamos (casos) por denegación de acceso a la información referidos a temáticas de protección de datos personales. El año con más casos fue el 2020 debido, quizás, a la pandemia del Coronavirus, la cual aceleró el uso de tecnologías de información.

Tabla 1: Casos relacionados a la Protección de Datos Personales

Año ingreso	Amparo	Reclamo	Total
2019	101	0	101
2020	213	12	225
2021	5	5	10
Total	**319**	**17**	**336**

[118] 23.873 casos entre los años 2019-2021.

De los 336 casos, 234 fueron acogidos de forma parcial o total y, además, 29 casos se refieren a temáticas de videovigilancia -de los cuales fueron acogidos total o parcialmente 13- y 7 casos a reconocimiento facial -de los cuales fueron acogidos totalmente 4-. Uno de los temas que concita mayor preocupación en materia de uso de tecnologías es la seguridad. No es de extrañar que la mayor parte de los casos que refieren a temas de televigilancia y reconocimiento facial, están asociados a instituciones de orden y seguridad.

Tabla 2: Casos relacionados a mecanismos de videovigilancia y reconocimiento facial

Tipo	Amparo	Reclamo	Total
Videovigilancia	28	1	29
Reconocimiento Facial	6	1	7
Total	34	2	36

Los servicios públicos pueden reclamar respecto de la decisión del Consejo para la Transparencia frente a un amparo mediante la interposición de un reclamo de ilegalidad ante la Corte de Apelaciones del domicilio del reclamante; así como pueden presentar un recurso de queja ante la Corte Suprema en caso de que estimen que los jueces de la Corte de Apelaciones, resolviendo dicho reclamo de ilegalidad, han cometido falta o abuso grave al dictar su sentencia. Desde el 2020 a agosto de 2021, se han interpuesto un total de 54 recursos en las cortes (considerando Cortes de Apelaciones y Corte Suprema) en casos vinculados al derecho de protección de datos personales, en el cual 44 corresponden a reclamos de ilegalidad[119] y del cual fueron acogidos tres; uno correspondiente a una acción de protección[120], que fue rechazada por improcedente; y nueve recursos de queja[121], de los cuales tres fueron rechazados por improcedentes y cinco están pendientes de sentencia. En conclusión, los tribunales superiores de justicia ratifican en la mayoría de los casos las decisiones del Consejo, lo que refrenda que, hasta ahora, ha sabido ponderar adecuadamente el derecho de acceso a la información pública y la protección de datos personales.

Tabla 3: Casos relacionados a mecanismos de videovigilancia y reconocimiento facial

Recursos interpuestos por casos PDP	Tipo recurso			
Año interposición recurso	Ilegalidad	Queja	Protección	Total
2020	36	1	0	37
2021	8	8	1	17
Total	44	9	1	54

[119] Reclamo de ilegalidad: Mecanismo de reclamación dirigido en contra de las decisiones dictadas por el Consejo para la Transparencia, los cuales deben ser resueltos por la Corte de Apelaciones del domicilio del reclamante.

[120] Acción de protección: Acción judicial que se presenta ante la Corte de Apelaciones, en contra de actos u omisiones ilegales o arbitrarias cometidas por personas o autoridades, y que representen una amenaza, privación o perturbación al ejercicio de ciertos derechos fundamentales, que están señalados en el Art. 20 de la Constitución.

[121] Recurso de queja: En este caso, es un recurso que se presenta en la Corte Suprema en contra de los jueces de la Corte de Apelaciones que resolvieron un reclamo de ilegalidad, culpándolos de una falta o abuso grave en la dictación de una resolución.

Contrariamente a las debilidades halladas en el tratamiento de la información personal de los usuarios de servicios públicos, la mayoría de los organismos protegen los datos personales de sus funcionarios, destacando a los organismos de la administración central y a las municipalidades. Un gran porcentaje de la información personal que tratan los órganos públicos pertenecen a sus funcionarios (30%), referida a la identificación y caracterización, como nombres, apellidos, domicilio, información académica, datos bancarios, remuneraciones e información previsional entre otros. Además, más que contar con una designación formal de un encargado, los servicios han optado por la incorporación de soluciones tecnológicas para gestionar el cuidado de los datos personales de sus funcionarios. Establecer una red cerrada con acceso restringido, autenticación, implementación de una bóveda de datos o encriptación de datos son algunas de las iniciativas que contribuyen a dotar una mayor seguridad a la información de los funcionarios públicos.

Finalmente, en cuanto al ejercicio efectivo de los derechos ARCO por parte de las y los usuarios de servicios públicos, a un 15% de estos últimos se les ha solicitado alguna vez modificar, eliminar o bloquear los datos por parte de su titular; un 2% ha sido demandado en tribunales por negarse a entregar datos personales a su titular; y un 1% ha sido demandado por vulnerar la protección a la vida privada. Según estas cifras, pareciese ser que las instituciones en Chile cumplen con el mandato del titular de los datos al hacer exigible sus derechos ARCO.

En conclusión, existen algunos déficits en la incorporación de estándares que protejan la información personal de usuarios de servicios públicos, lo cual se evidencia por, por ejemplo, un porcentaje menor de servicios que incorporan una política de privacidad; un pequeño porcentaje que publica su política de privacidad en un lugar visible en el sitio electrónico institucional; falencias en la inclusión de estándares de seguridad y certificación por parte de una empresa externa; y en el incumplimiento de ciertos servicios de registrar sus bases de datos personales en el Registro Civil. Por otra parte, se evidencian avances reflejados en el comportamiento de las instituciones respecto a la protección de datos personales de sus funcionarios.

De esta forma es necesario mejorar pues, como hemos visto, en el marco de la LPVP en contextos de videovigilancia y reconocimiento facial es necesario que las instituciones cuenten con lo más altos estándares, buenas prácticas y cumplimiento normativo. Si no existe una política de privacidad de datos publicada en el sitio web de un servicio público, difícilmente los usuarios tendrán conocimiento de cómo fueron tratados sus datos personales. Lo mismo ocurre si intercambian información personal con otras entidades públicas o privadas sin un fundamento legal ni una finalidad amparada por la ley, o si existen ciberataques que pueden romper fácilmente las barreras de seguridad institucionales y obtener información personal con un fin malicioso como, por ejemplo, la suplantación de identidad. Es necesario entonces, generar una mayor cultura institucional respecto a la protección de datos personales y también fomentar en la ciudadanía el conocimiento de las herramientas legales disponibles para exigir el derecho a la protección de sus datos personales en el marco de esta ley.

VIII. RECOMENDACIONES

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

Según hemos podido observar en este trabajo, los sistemas de videovigilancia y los de reconocimiento facial tienen la potencialidad de afectar -con diversas intensidades- una serie de derechos de las personas, encontrándose entre ellos, el derecho fundamental a la protección de datos personales que está consagrado expresamente en nuestra Constitución. En dicho contexto, cabe destacar que estos sistemas han ido evolucionando a gran velocidad en el último tiempo, mejorando sistemas tradicionales de video mediante la incorporación de programas computacionales que los transforman en sistemas inteligentes, y que incluso se asocian, a bajo costo, a sistemas de reconocimiento facial e inteligencia artificial que pueden ser utilizados en diversos ámbitos de la vida cotidiana. Esto da cuenta de tecnologías con cualidades que cada vez son más intrusivas y que, por lo mismo, requieren de medidas apropiadas que aseguren que su implementación, tanto por el sector público como el privado, siempre se efectúe respetando los derechos fundamentales de las personas.

En particular sobre los sistemas de reconocimiento facial, se debe enfatizar su potencial para afectar gravemente los derechos de las personas cuando son utilizados de forma indiscriminada y sin atención a estándares adecuados de protección a los derechos fundamentales. En este trabajo, se han esgrimido un sinnúmero de riesgos específicos asociados a esta tecnología, los que se refieren a aspectos tales como la transparencia, información, finalidades, seguridad, ejercicio de derechos, fiscalización, precisión, tipos de datos involucrados, entre varios otros. En este sentido, resulta esencial que en Chile se tomen -desde ya- mejores y mayores medidas de resguardo y protección para la implementación de esta tecnología, sobre todo, teniendo presente que, como vimos, su operación por parte de diversas autoridades públicas ya ha estado ocurriendo.

La urgencia que presenta este desafío, en lo que respecta a la afectación de los derechos de las personas, ha sido recalcada y enfatizada al más alto nivel internacional y haciendo eco de la gravedad de la misma. En este sentido, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos y ex Presidenta de la República, Michelle Bachelet, hizo un llamado en septiembre de este año a que los países tomen acciones urgentes en relación a los sistemas de inteligencia artificial por el riesgo que presentan a los derechos humanos, incluyendo ciertos sistemas biométricos. En su reporte[122], la Alta Comisionada recomendó explícitamente a los países establecer una moratoria en el uso de sistemas remotos de reconocimiento biométrico en espacios públicos, al menos, hasta que las autoridades responsables puedan demostrar cumplimiento de los estandartes de privacidad y protección de datos, la ausencia de problemas de precisión e impactos discriminatorios, entre otras medidas[123] (OHCHR, 2021).

[122] El reporte de la Alta Comisionada se puede encontrar en: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

[123] Aquellas de párrafo 53 (j) (i–v) del documento A/HRC/44/24 de la Alta Comisionada en relación al impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de asambleas, incluyendo protestas pacíficas. Disponible en: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx

A lo anterior se suma la resolución no vinculante del Parlamento Europeo[124], del 6 de octubre de 2021, en la que igualmente se pide que se imponga una moratoria al despliegue de sistemas de reconocimiento facial para fines coercitivos o de aplicación de la ley (law enforcement) con funciones de identificación, a menos que se utilicen estrictamente para fines de identificación de víctimas de delitos, hasta que las normas técnicas puedan considerarse plenamente acordes con los derechos fundamentales, los resultados obtenidos no estén sesgados y no sean discriminatorios, el marco jurídico prevea salvaguardias estrictas contra el uso indebido y un control y supervisión democráticos estrictos, y existan pruebas empíricas de la necesidad y proporcionalidad del despliegue de estas tecnologías[125].

En virtud de lo anterior, y sin el objeto de ser exhaustivos, a continuación se presentan varias recomendaciones generales y particulares que, a nuestro juicio, constituyen acciones que, en conjunto con otras, podrían mejorar sustancialmente el nivel de protección de los derechos fundamentales de las personas frente a la implementación de sistemas de videovigilancia y de reconocimiento facial, tanto por entidades públicas como privadas en Chile, y sobre todo, el nivel de protección del derecho a la protección de datos personales que consagra expresamente nuestra Constitución desde el año 2018.

Por último, cabe señalar que en estas recomendaciones se incluyen sugerencias generales de política pública en este tema, así como de medidas particulares para la adecuada implementación de esta clase de tecnología por responsables del banco de datos.

[124] Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

[125] La resolución también pide la prohibición permanente del uso de análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz, y otras señales biométricas y de comportamiento.

1. Recomendaciones generales

a) Evaluar la conveniencia de implementar una moratoria en la implementación de tecnología de reconocimiento facial para fines de seguridad o vigilancia por parte de entidades públicas y privadas

Siguiendo el planteamiento efectuado por diversas autoridades internacionales alrededor del mundo respecto de los severos riesgos que presenta la tecnología de reconocimiento facial para un gran número de derechos fundamentales de las personas, en conjunto con el deficitario marco regulatorio vigente en Chile sobre protección de datos personales y, particularmente, la ausencia de una autoridad administrativa y autónoma que fiscalice y sancione el debido cumplimiento de los estándares de datos personales, sugerimos evaluar desde ya la conveniencia de implementar una moratoria o suspensión temporal en la implementación de tecnología de reconocimiento facial para fines de seguridad o vigilancia en espacios públicos y mediante tecnología remota y en vivo (live), al menos hasta que los aspectos indicados se vean subsanados debidamente o el responsable otorgue garantías suficientes.

b) Actualizar la LPVP mejorando los estándares de protección de datos personales en Chile

Como ya señalamos, la LPVP presenta un sinnúmero de debilidades que impactan en el nivel de protección que se otorga a los titulares cuyos datos son tratados en el contexto de sistemas de videovigilancia y de reconocimiento facial. En dicho sentido, resulta esencial una modificación normativa, ya sea a través del Proyecto de Ley u otro instrumento que establezca los mejores estándares en la materia y que se ajuste al desarrollo tecnológico actual. A modo de ejemplo, resulta esencial que se consagren expresamente y de forma orgánica los principios que informan el tratamiento de datos personales, como el principio de minimización de datos, y que en cada operación de tratamiento se requiera una evaluación exhaustiva de la necesariedad y proporcionalidad del mismo en vista a los objetivos que se persiguen y los riesgos asociados. Esto, sobre todo teniendo presente que los datos que son tratados mediante estos sistemas corresponden a datos de carácter sensible y datos biométricos.

c) Contar con una autoridad o agencia administrativa independiente de protección de datos personales

Como sabemos, no existe en Chile una autoridad o agencia administrativa de protección de datos personales que vele y que pueda sancionar y fiscalizar el correcto tratamiento de datos personales en el sector público y privado. Actualmente, el Consejo para la Transparencia solo cuenta con facultades para "velar" por el adecuado cumplimiento de la LPVP, por parte de los órganos de la Administración del Estado. En este contexto, resulta esencial que se avance en este tema en Chile, pues de otra forma no se generarán los incentivos suficientes para que todos los responsables que implementen sistemas de videovigilancia y de reconocimiento facial den cumplimiento a la normativa de protección de datos personales.

d) Avanzar en orientación y guía sobre los riesgos que conllevan los mecanismos de videovigilancia y la tecnología de reconocimiento facial, así como la forma adecuada de implementarlos

Muchas entidades públicas y privadas están implementado y evaluando proyectos que involucran esta clase de tecnologías sin tener conciencia acabada sobre los riesgos que se pueden generar en los derechos fundamentales de las personas. A su turno, tampoco se advierte que exista una preocupación generalizada en la ciudadanía sobre la implementación de esta tecnología en el espacio público (o abierto al público) y la posible afectación en sus derechos. Esta situación hace necesario que se avance en mayor orientación y guía respecto de los riesgos que conllevan los mecanismos de videovigilancia y de reconocimiento facial, tanto para los responsables de banco de datos, como para los mismos titulares que pudieran verse afectados, especialmente en grupos socioeconómicos más desfavorecidos como C3, D, E. Mayor conciencia a nivel ciudadano puede generar mejores condiciones para que se avance decididamente por parte de las autoridades en otras medidas relevantes como, por ejemplo, la de impulsar una normativa que modifique definitivamente la actual LPVP.

e) Evaluar la necesidad de contar con una entidad pública encargada específicamente del uso de videovigilancia por parte del Estado con el objeto de generar confianza pública en este mecanismo

El impacto que, en los derechos de las personas, puede generar la videovigilancia y su uso combinado con tecnologías de reconocimiento facial, o inteligencia artificial en general, puede ser sustantivo si no se toman medidas adecuadas para su correcta implementación. Las distintas particularidades que presentan estas tecnologías en el espacio público, así como su uso por parte de las autoridades con fines de seguridad requiere de medidas particulares de control y de legitimidad que, es posible, vayan incluso más allá de lo que pueda establecer una normativa general de protección de datos personales. En dicho escenario, resulta al menos conveniente, evaluar la necesidad de contar con una entidad pública encargada específicamente del uso de esta tecnología por parte del Estado, y como tiene actualmente Reino Unido mediante el Comisionado de Cámaras de Vigilancia. Todo esto, con el objeto de generar confianza pública en los mecanismos de videovigilancia a través de la determinación de reglas y estándares que atiendan a las particularidades que presenta dicha tecnología.

f) Evaluar la conveniencia de generar un marco normativo que aborde los desafíos propios de videovigilancia y el reconocimiento facial

En línea con la recomendación anterior, también resulta adecuado evaluar la utilidad de contar con un marco normativo específico para los sistemas de videovigilancia y de reconocimiento facial utilizados por el Estado, de forma tal de entregar lineamientos claros que todos ellos deban cumplir, y que se ajusten a las particularidades de esta tecnología y de su interacción con otras, como la de inteligencia artificial.

Actualmente, esto resulta esencial en nuestro país, donde el estándar normativo aplicable se sustenta fundamentalmente en la LPVP en los casos en que existe tratamiento de datos personales, y en la jurisprudencia de la Corte Suprema y las recomendaciones del Consejo. No siendo estos dos últimos antecedentes vinculantes para las nuevas implementaciones de estas tecnologías. Finalmente, hay que destacar que esto también ha sido propuesto por la doctrina, que ha manifestado “parece útil contar con un marco normativo general que sistematice el uso de la tele vigilancia para distintas funciones (tránsito, seguridad pública, fiscalización medio ambiental, entre otros fines” (Canales y Lara, 2018, p. 30).

2. Recomendaciones particulares

a. Fomentar que los servicios públicos -especialmente municipales- **informen al Servicio de Registro Civil e Identificación los bancos de datos que se encuentran en su poder**, sobre todo si los bancos contienen información sobre videovigilancia y reconocimiento facial. En esta misma línea, se sugiere que los encargados de los bancos de datos de servicios públicos sean **capacitados en los procedimientos para la inscripción** de dichos bancos en dicho organismo público.

b. Se sugiere designar formalmente en cada servicio a un **funcionario o funcionaria responsable de gestionar y resguardar los bancos de datos que contienen información personal.**

c. El uso de mecanismos de videovigilancia y de tecnología de reconocimiento facial debe ser **siempre evidente y manifiesto** para cualquiera que se aproxime al lugar (y que se encuentre en él) donde se están usando dichas tecnologías. Es esencial que las personas tengan conciencia de que están siendo grabados en determinado momento y/o de que se exponen a tecnología de reconocimiento facial.

d. Establecer **políticas que regulen y que reduzcan la discrecionalidad de las autoridades públicas** en relación a la localización de cámaras de videovigilancia y de uso de tecnología de reconocimiento facial, así como respecto a la inclusión de individuos en listas de seguimiento o vigilancia (watchlists) con las cuales se contrastan las imágenes que son captadas.

e. Hacer aplicables las normas y recomendaciones que se formulen sobre mecanismos de videovigilancia al **uso de tecnología de reconocimiento facial**, cuando dichos sistemas se utilicen asociados o de forma conjunta. Esto permitirá evitar cualquier vacío en la aplicación de la normativa.

f. Implementar por los responsables de bancos de datos que utilicen esta clase de tecnologías, **políticas de tratamiento de datos personales** adecuadas y transparentes para todos los titulares de datos, que cubran todos los aspectos esenciales del tratamiento, incluyendo, al menos, la identidad del responsable, finalidad del mismo, tipo de datos tratados, duración del tratamiento, derechos de los titulares, información sobre destinatarios, información sobre mandatarios o encargados del tratamiento, información sobre el uso de tecnología de reconocimiento facial o inteligencia artificial.

g. Disponer de **instrumentos de política interna adicionales** que incluyan las especificaciones, reglas y procedimientos atingentes a la retención y eliminación de imágenes, las cuales se encuentren sujetas a revisiones periódicas para asegurar que sus disposiciones y los fundamentos para adoptarlas siguen vigentes.

h. En cuanto a la **retención de grabaciones** en el contexto de videovigilancia efectuadas por autoridades públicas para fines de seguridad, se deberá estar a lo que disponga la normativa aplicable, así como a las recomendaciones que al efecto emita el Consejo para la Transparencia. En el caso de municipalidades, las recomendaciones vigentes sugieren un plazo máximo de retención de 30 días, sin perjuicio de que puedan existir ciertas circunstancias específicas en las que, ante la verificación de un interés legítimo relevante y conforme al ordenamiento jurídico, se haga necesario o prudente que este tiempo de almacenamiento varíe en lo estrictamente necesario en relación a una grabación particular. Entre estas circunstancias específicas, el Consejo ha identificado, por ejemplo, la existencia de solicitudes de acceso a las captaciones por parte de un titular de datos que estén pendientes de resolución; las solicitudes de entrega de las grabaciones que se fundamenten en una atribución legal de la entidad u organismo requirente, y que estén pendientes de cumplimiento; o las grabaciones que hayan captado un ilícito penal, civil, administrativo u otra falta, a efectos de ser entregadas a las autoridades competentes. Estas circunstancias, sin perjuicio del análisis caso a caso que debe hacer cada institución responsable de datos.

i. Establecer **obligaciones particulares y robustas de seguridad y confidencialidad** para quienes hacen tratamiento de datos biométricos en el contexto de sistemas de reconocimiento facial que atiendan a las características y riesgos propios de esta tecnología. Estas medidas deben atender, por ejemplo, al uso de plantillas biométricas por terceros; la conservación de las planillas biométricas; su almacenamiento en un dispositivo personal frente al almacenamiento centralizado; los mecanismos de cifrado de los datos biométricos y la gestión de claves; las medidas anti-suplantación; los mecanismos automatizados de supresión de datos; los procedimientos de acceso a la información del sistema, etc. Estas medidas deben evolucionar conforme evoluciona la tecnología.

j. Por su parte, y a nivel general, se sugiere que cada servicio público establezca **estándares de ciberseguridad aplicables a los bancos de datos que contienen información personal** como, por ejemplo, poseer un registro de incidencias; controlar el acceso a los bancos de datos mediante autenticación, gestión de soporte y copias de respaldo de datos. Además, dichos estándares, idealmente deben ser certificados por una empresa externa que pueda garantizar la seguridad de la información.

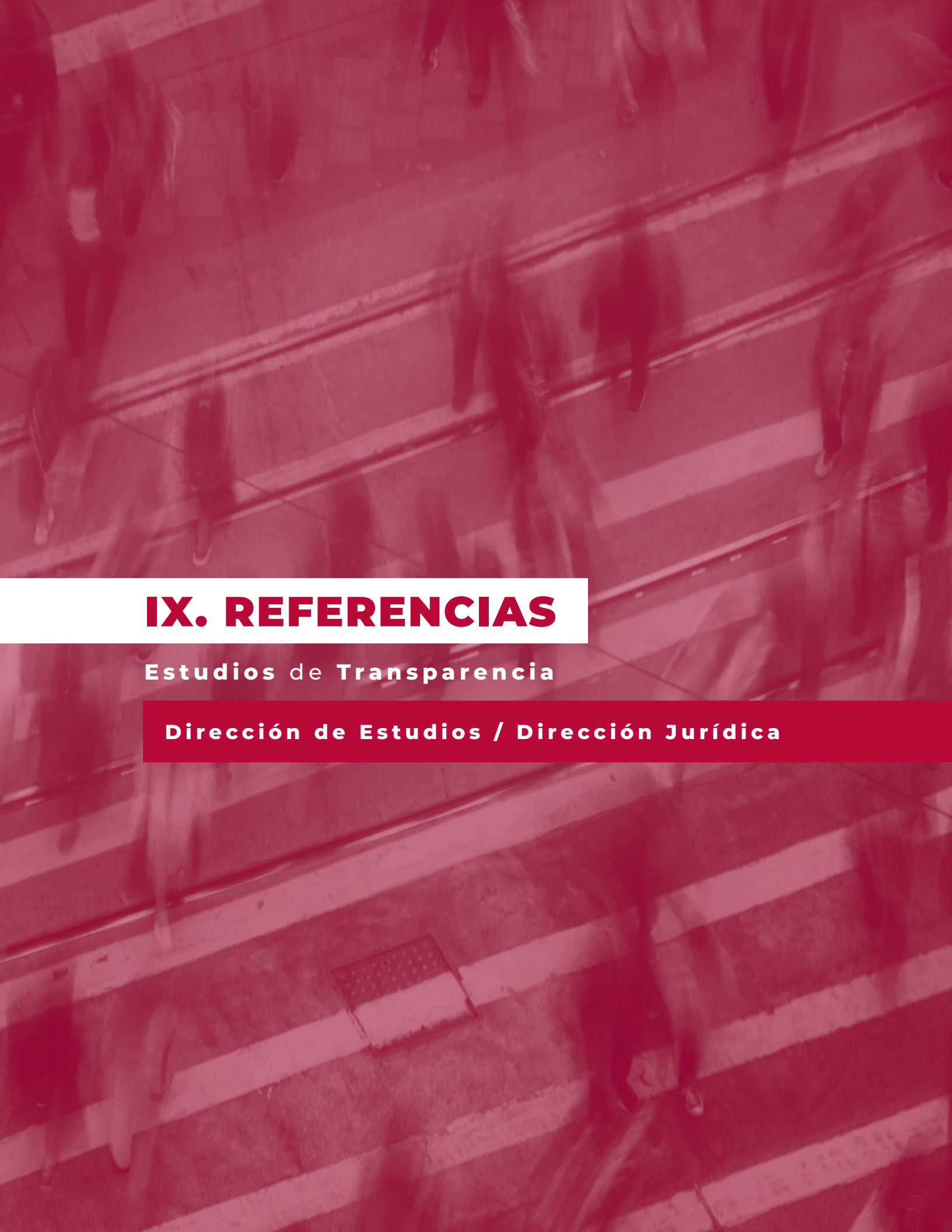
k. Realizar **evaluaciones de impacto de protección de datos** que cubran al menos los aspectos establecidos por el RGPD en su artículo 35.

l. Incorporar **prácticas continuas de capacitación** para todos los funcionarios cuyas tareas se relacionen con los sistemas de videovigilancia y/o tecnología de reconocimiento facial que incorporen elementos de protección de datos personales.

m. Evaluar permanentemente los **riesgos de la externalización** de servicios en esta materia, así como las obligaciones a las que está sujeto el tercero que actúe como mandatario o encargado del tratamiento.

n. Tener presente la **protección de datos desde el diseño y por defecto** que establece el artículo 25 del RGPD, y las Recomendaciones sobre Protección de Datos Personales del Consejo para la Transparencia, en el desarrollo e implementación de los mecanismos de videovigilancia y reconocimiento facial.

o. Implementar medidas y procedimientos que aseguren el respecto a los **derechos de los titulares sobre sus datos personales** independiente que el tratamiento se efectúe en contextos de videovigilancia y/o de sistemas de reconocimiento facial. En este contexto, particular atención se debe prestar a garantizar el derecho de los titulares a obtener copia de las grabaciones donde ellos aparezcan, ya sea cuando se ejerzan los derechos que consagra la normativa de datos personales, o cuando se requiera el acceso a través del derecho de acceso a la información pública que establece la Ley de Transparencia.



IX. REFERENCIAS

Estudios de **Transparencia**

Dirección de Estudios / Dirección Jurídica

Alessandri, Arturo, Manuel Somarriva y Antonio Vodanovic. (2005). Tratado de Derecho Civil. Partes Preliminar y General. Tomo Primero. Editorial Jurídica de Chile.

Álvarez, Daniel. (2019). La inviolabilidad de las comunicaciones privadas electrónicas. LOM Ediciones.

Arzoz Santisteban, Xavier. (2015). "Derecho al Respeto de la Vida Privada y Familiar", en Lasagabaster Herrarte, Iñaki (Dir.), Convenio Europeo de Derechos Humanos. Comentario Sistemático. (3ª ed.). Civitas-Thomson Reuters.

Agencia Española de Protección de Datos, AEPD. (2018). Guía sobre el uso de videocámaras para seguridad y otras finalidades. Recuperado el 27 de septiembre de 2021 de: https://www.aepd.es/es/documento/guia-videovigilancia.pdf

Agencia Española de Protección de Datos, AEPD. (2020). Nota Técnica: 14 equívocos con relación a la identificación y autenticación biométrica. Recuperado el 18 de octubre de 2021 de: https://www.aepd.es/media/notas-tecnicas/nota-equivocos-biometria.pdf

Becker, Sebastián, y Romina Garrido. (2017). La biometría en Chile y sus riesgos. Revista Chilena de Derecho y Tecnología, 6(1), 67-91. https://dx.doi.org/10.5354/0719-2584.2017.45825

Canales, María Paz y Juan Carlos Lara (2018). La Construcción de Estándares Legales para la Vigilancia en América Latina. Parte III: Propuesta de Estándares Legales para la vigilancia en Chile. Recuperado el 7 de octubre de 2021 de: https://www.derechosdigitales.org/wp-content/uploads/propuesta-estandares-legales-vigilancia-chile.pdf

Carey, Peter. (2015). Data Protection. A Practical Guide to UK and EU Law. (4ª ed.). Oxford University Press.

Carey, Peter. (2020). Data Protection. A Practical Guide to UK and EU Law. (6ª ed.). Oxford University Press.

Cea Egaña, José Luis. (2019). Derecho Constitucional Chileno. Derechos, deberes y garantías. Tomo II. (3ª ed.). Ediciones Universidad Católica de Chile.

Cerda, Alberto. (2012). Legislación sobre protección de las personas frente al tratamiento de datos personales. Material de estudio del Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile.

Contreras, P., García G., y Martínez V. (2016). Diccionario Constitucional Chileno. (2ª ed.). Editorial Hueders.

Contreras, Pablo (2021). Orwellian nightmares and drone policing in Chilean municipalities: Legality, surveillance and the politics of low cost. Latin American Law Review, no. 7 (2021): 61-80. https://doi.org/10.29263/lar07.2021.04

Cordero, Luis. (2009). Videovigilancia e intervención administrativa: las cuestiones de legitimidad, en Arrieta, Raúl y Carlos Reusser (Coor.), Chile y la Protección de Datos Personales. ¿Están en crisis nuestros derechos fundamentales? (81- 99). UDP-Expansiva.

Díez-Picazo, Luis María. (2003). Sistema de Derechos Fundamentales. Civitas-Thomson Reuters.

Estudio Nacional de Transparencia (ENT) (2020). Consejo para la Transparencia. Recuperado 26 de octubre de 2021 de: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2021/07/Estudio-Nacional-Transparencia-2020.pdf

European Data Protector Supervisor, EDPS. (2010). The EDPS video-surveillance guidelines. Recuperado el 27 de septiembre de 2021 de: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf.

European Data Protector Supervisor, EDPS. (2020). Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video. Versión 2.0. Recuperado el 4 de octubre de: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

European Data Protector Supervisor, EDPS. (2021). Video-surveillance. Recuperado el 27 de septiembre de 2021 de: https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

Escalante, Fernando. (2008) El Derecho a la Privacidad. Serie Cuadernos de Transparencia, IFAI, México.

Figueroa, Rodolfo. (2014). Privacidad. Ediciones Universidad Diego Portales.

Gil, Elena. (2016) Big Data, Privacidad y Protección de Datos. Agencia Española de Protección de Datos, Madrid, España.

Global Privacy Assembly, GPA. (2020). Adopted resolution on facial recognition technology. 42nd closed sesión of the Global Privacy Assembly. Recuperado el 13 de octubre de 2021 de: https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-EN.pdf

Gutiérrez Gutiérrez, Ignacio (Coord.) (2015). Elementos de Derecho Constitucional Español. (2ª ed.). Marcial Pons.

Iosa, Juan (2017). Libertad negativa, autonomía personal y constitución. Rev. chilena de derecho [online]. 2017, vol.44, n.2, pp.495-518. ISSN 0718-3437. Recuperado el 22 de septiembre de 2021 de: http://dx.doi.org/10.4067/S0718-34372017000200495

Information Commissioner's Office, ICO. (2017). In the picture: A data protection code of practice for surveillance cameras and personal information. Version 1.2. Recuperado el 27 de septiembre de 2021 de: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Information Commissioner's Office, ICO. (2021). The use of live facial recognition technology in public places. Recuperado el 7 de octubre de 2021 de: https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Jijena, Renato (2013). Tratamiento de datos personales en el Estado y acceso a la información pública. Revista chilena de derecho y tecnología. Universidad de Chile.

Li, Lixiang. et. al. (2020). A Review of Face Recognition Technology. IEEE Access, Vol. 8. Recuperado el 8 de noviembre de 2021 de: https://ieeexplore.ieee.org/abstract/document/9145558

Maqueo, María. et al. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de Derecho, Vol. XXX N°1, pp. 77-96.

Pica, Rodrigo y Matías Vargas (2021). Desafíos del derecho de protección de datos personales y la autodeterminación informativa en Chile, en Moreno, Ángela e Isabel Serrano (Dir.), El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad (235-275). Tirant Lo Blanch.

Surveillance Camera Commissioner, SCC. (2020). Facing the Camera. Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales. Recuperado el 28 de septiembre de 2021 de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

UN Office of the High Commissioner for Human Rights, OHCHR. (2021). The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights. A/HRC/48/31. Recuperado el 16 de octubre de 2021 de: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

Working Party 29, WP29. (2012). Opinion 3/2012 on developments in biometric technologies. OO720/12/EN WP193. Recuperado el 7 de octubre de 2021 de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Working Party 29, WP29. (2015). Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. 01673/15/EN WP231. Recuperado el 8 de octubre de 2021 de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

consejo para la
Transparencia