INFORME ANUAL SOBRE DERECHOS HUMANOS EN CHILE 2017

EDICIONES
UNIVERSIDAD DIEGO PORTALES

CENTRO DE DERECHOS HUMANOS udp
FACULTAD DE DERECHO

Centro de Derechos Humanos, Facultad de Derecho, Universidad Diego Portales;
Tomás Vial Solar (editor general) / Informe anual sobre Derechos Humanos en Chile 2017

Santiago de Chile: la universidad: Centro de Derechos Humanos, Facultad de Derecho de la universidad, 2017, 1ª edición, p. 472, 15 x 23 cm.

Dewey: 341.4810983
Cutter: In38
Colección Derecho
Incluye presentación de los Dres. Tomás Vial Solar y Lidia Casas Becerra directora del Centro de Derechos Humanos de la universidad, notas al pie de página y biografías de los autores del informe 2017.

Materias:
Chile. Derechos Humanos.
Derecho al agua potable. Chile.
Empresas, aspectos sociales.
Derechos del niño. Chile
Personas LGTBI. Aspectos jurídicos.
Inmigrantes, situación jurídica.
Multiculturalismo, Chile.
Derechos de pueblos indígenas.
Identidad cultural. Chile.
Privacidad.
Control de la policía.
Derecho de acceso a la justicia.

INFORME ANUAL SOBRE DERECHOS HUMANOS EN CHILE 2017

Primera edición: noviembre de 2017
ISBN 978-956-314-392-8

Universidad Diego Portales
Facultad de Derecho
Av. República 105
Teléfono (56-22) 676 2601
Santiago de Chile
www.derecho.udp.cl

Editor general: Tomás Vial
Edición: Vicente Parrini
Diseño: Marisol González

Impreso en Chile por Salesianos Impresores S.A.

PRIVACIDAD: LA VIGILANCIA EN ESPACIOS PÚBLICOS[1]

1 Capitulo redactado por Domingo Lovera, que contó con la valiosa colaboración de los alumnos Mariela Córdova y Kurt Scheel. El autor está especialmente agradecido por su iniciativa y el ánimo en las tareas encomendadas.

SÍNTESIS

El presente capítulo ofrece un acercamiento inicial a la protección de la privacidad en el derecho internacional de los derechos humanos. El análisis se centra en un fenómeno que amenaza con extenderse: las actividades de vigilancia y control que un puñado de municipios ha iniciado a efectos de, según han dicho sus autoridades, prevenir/controlar de mejor manera el delito. Estos municipios han instalado cámaras de vigilancia en globos aerostáticos y drones, que captan "a granel" un sinnúmero de actividades habituales llevadas a cabo por personas identificadas o identificables. Bajo la premisa de que *el que nada hace nada teme* y de que el espacio público se ofrece al Estado y sus organismos como campo abierto a su intromisión, la vida de miles de personas es constantemente monitoreada.

Como se advertirá en este capítulo, ello se debe, en parte importante, al débil marco legal en el que operan las municipalidades –aunque lo mismo ocurre con respecto a otras instancias de videovigilancia–, así como al escaso control al que esas actividades de vigilancia son sometidas. Incluso cuando lo son, se encuentran con instancias judiciales o administrativas que han estado dispuestas a leer el conflicto en un marco legal débil, con aún mayor flexibilidad.

Lo descrito atenta contra los estándares del derecho internacional de los derechos humanos. Como se expone a continuación, en el derecho internacional de los derechos humanos, las actividades de intromisión estatal deben estar sujetas a un estricto escrutinio de legalidad y se demanda a los Estados la regulación detallada y acotada de las mismas. Además, se exige que los Estados justifiquen adecuadamente la necesidad de esa medida en una sociedad democrática y que dispongan, en todo caso, de un organismo independiente capaz de vigilar el respeto a los derechos de las personas. Este capítulo concluye que el Estado de Chile se encuentra al debe en cada uno de esos ámbitos.

PALABRAS CLAVES: vida privada, privacidad, cámaras de vigilancia, drones.

INTRODUCCIÓN

Hasta hace poco tiempo, la idea de privacidad era equiparada con las de seclusión, soledad y propiedad privada. Hoy, la idea de privacidad se ha expandido: no solo supone que las personas estamos dotadas de un cierto campo de inmunidad donde el Estado y terceros no pueden inmiscuirse arbitrariamente (y que incluye un cierto espacio de soberanía decisional), sino que ha avanzado a incorporar otras esferas, desligadas del espacio específico donde circula información, y donde dicha información y su dominio es lo que define el ámbito de protección del derecho.

De esta forma, la privacidad incluye hoy una serie de variables que van configurando la expectativa de privacidad con la que las personas esperamos movernos: espacios, tipos de relaciones, así como la información, conductas y situaciones en que estamos involucradas.[2] Incluso las actividades que las personas desarrollan en espacios públicos puedan estar cubiertas de una expectativa razonable de privacidad, en la medida que esa información –qué lugares visitamos, con quiénes nos juntamos, qué hábitos desplegamos, etc.– es crucial para nuestra autodeterminación: define la forma en que soberanamente nos presentamos a los y las demás, así como el tipo de relaciones que trabamos con ellos y ellas.

Hoy, el avance de la tecnología hace que esa autodeterminación informativa se vea seriamente afectada y, en especial, la privacidad condicionada. El Estado lleva adelante una serie de prácticas que se inmiscuyen en esos espacios de autodeterminación informativa y que pueden afectar –a veces de modo definitivo– la vida y actividades de las personas. Entre los años 2015 y 2017 se ha conocido una serie de iniciativas que son especialmente sensibles en este sentido. Algunas municipalidades –animadas, según han afirmado, por el combate contra la delincuencia– han comenzado a implementar sistemas de vigilancia por medio de cámaras situadas en globos aerostáticos y drones.

2 Manuel José Cepeda, "Privacy", Michel Rosenfeld y András Sajó (eds.), *The Oxford Handbook of Comparative Constitutional Law*, Oxford, Oxford University Press, 2012, pp. 971-5.

¿Han considerado esas prácticas el derecho a la privacidad de las personas cuyas imágenes, actividades, relaciones y hábitos son captados a diario por esos sistemas de vigilancia? La respuesta rápida de nuestras autoridades ha sido la de recurrir a una conocida expresión: el que nada hace, nada teme. ¿Qué problema debiera tener la persona que no anda por las calles cometiendo delitos –prosigue la idea– de ser captada por los sistemas de vigilancia que a diario se despliegan? La interpretación democrática de esa expresión (así como de las facultades estatales que la acompañan), sin embargo, debe llevarnos a las conclusiones opuestas. Justamente porque las personas nada han hecho es que esperan razonablemente que sus derechos, entre ellos la privacidad, no sean perturbados: porque nada han hecho las personas tienen expectativas altas de no ser objetos de vigilancia.

Por supuesto, nada de lo anterior equivale a demandar, sin más, el fin de las actividades de vigilancia del Estado –las caricaturas frente a críticas como las que acá se proponen abundan–. Pero sí, cosa distinta, a preguntarse por las condiciones en que estas actividades se desarrollan. ¿Cuáles son las fuentes legales, en caso de haberlas, que habilitan esas actividades? ¿Cuáles son las regulaciones a las que están sujetas? ¿Qué ocurre con la información que se recopila? ¿Cuáles son los usos que se le da a esa información? ¿Quién tiene acceso a esa información? ¿Dónde se almacena? ¿Por cuánto tiempo?

Todas estas son preguntas, al tiempo que demandas de regulación, razonables que pueden formularse a partir de los estándares del derecho internacional de los derechos humanos. Este capítulo –el primero sobre privacidad en la historia del *Informe*– ofrece una mirada inicial al respecto. Para ello, primero comienza identificando la recepción de la privacidad en los instrumentos internacionales de derechos humanos y algunos problemas a los que ha dado lugar esa recepción. Enseguida, ofrece una sistematización de las condiciones o requisitos que los Estados deben satisfacer a efectos de desarrollar actividades (intromisiones) que, *prima facie*, serían problemáticas para la privacidad. Por último, se analiza el caso puntual de los sistemas de vigilancia a través de globos aerostáticos y drones, advirtiendo los vacíos legales de regulación en que se despliegan.

1. PRIVACIDAD: RECEPCIÓN Y PROBLEMAS

La relevancia de la privacidad en el derecho internacional de los derechos humanos puede comenzar apenas a dibujarse a medida que vamos anotando su recepción en los diversos instrumentos que lo componen. La primera parte de esta sección (1.1) repasa, brevemente, esa recepción. La segunda parte (1.2) anota algunos problemas que afectan, con especial fuerza, la delimitación del contenido de la privacidad. Se

advertirán, solo de manera introductoria, los diferentes acercamientos a la privacidad y se dirá cuál es el que este capítulo privilegia.

1.1. Los instrumentos

En términos generales, los instrumentos del derecho internacional de los derechos humanos, el "International Bill of Rights", como se le denomina,[3] reconocen el derecho a la vida privada o privacidad. Ocurre así en instrumentos de alcance general como, por ejemplo, la Declaración Universal de Derechos Humanos (DUDH). Así, el art. 12 de la DUDH dispone:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

El art. 17.1 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), por su parte, afirma:

> Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

Agrega, enseguida, que las personas tienen derecho a la protección de la ley contra esos ataques.[4] A nivel de instrumentos regionales, la privacidad también ha sido ampliamente recibida. El art. 11.2 de la Convención Americana sobre Derechos Humanos (CADH), a propósito de la protección de la honra y la intimidad, sostiene que:

> Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

El art. 8.1 del Convenio Europeo de Derechos Humanos (CEDH) asegura a todas las personas el "derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia." Agrega, en seguida,

3 Louis Henkin y otros, *Human Rights* (2ª ed.), Nueva York, Foundation Press-Thomson Reuters, 2009, p. 215.

4 Es cierto que, al menos en términos explícitos, el Pacto Internacional sobre Derechos Económicos, Sociales y Culturales nada dispone sobre el derecho a la privacidad. Pero varias de sus disposiciones incluyen, dentro del manojo de posiciones jurídicas que protegen, algunas relativas a la vida privada. Ocurre así, por ejemplo, con el derecho a una vivienda digna, el que, entre otras cosas, debe asegurar privacidad para la vida individual y familiar. Gillian MacNaughton, "Beyond a Minimum Threshold: The Right to Social Equality", Lanse Minkler (ed.), *The State of Economic and Social Human Rights. A Global Overview*, Nueva York, Cambridge University Press, 2013, p. 283.

las condiciones conforme a las que la autoridad podrá regular el derecho.[5] El art. 7 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), a su turno, indica:

> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Agrega, enseguida, que toda persona tiene derecho a la protección de los datos de carácter personal (art. 8.1), añadiendo, en su artículo 8.2, que:

> Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

La privacidad también ha sido recogida en algunos instrumentos que abordan los derechos de colectivos específicos, como la Convención sobre los Derechos del Niño (CDN) que, en su art. 16.1, recurre a un lenguaje similar al del PIDCP y la CADH:

> Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.

Nota aparte merecen la Declaración de Naciones Unidas sobre los Derechos de los Pueblos Indígenas (DNUDPI) y la Convención sobre los Derechos de las Personas con Discapacidad (CDPCD). En el caso de la DNUDPI, el art. 12.1 reconoce el derecho de los pueblos indígenas a:

> manifestar, practicar, desarrollar y enseñar sus tradiciones, costumbres y ceremonias espirituales y religiosas; a mantener y proteger sus lugares religiosos y culturales y a acceder a ellos privadamente (…)

Este es un reconocimiento que contiene algunas particularidades. Primero, porque se trata de un derecho de titularidad colectiva. Segundo, porque, tratándose de un derecho reconocido para poder hacer efectiva la protección de su integridad cultural, pareciera estar atado a una variante –como veremos luego, no se trata de la única– espacial

5 Esto, en el art. 8.2 CEDH, cuyo análisis reservamos a efectos de la sistematización de los estándares del derecho internacional, más abajo.

de la privacidad (la referida a lugares religiosos y culturales). Sin embargo, debe allegarse una comprensión amplia del mismo derecho que incluye, además, el control libre de intromisiones indebidas sobre sus tradiciones, costumbres y ceremonias.[6]

Ahora bien, mirando a la CDPCD, se advierte que se ha recogido una versión más detallada, pero todavía abierta a la interpretación dinámica propia del derecho internacional, del derecho a la vida privada. Bajo el título "Respeto de la privacidad", el art. 22 dispone que:

> 1. Ninguna persona con discapacidad, independientemente de cuál sea su lugar de residencia o su modalidad de convivencia, será objeto de injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia o cualquier otro tipo de comunicación, o de agresiones ilícitas contra su honor y su reputación. Las personas con discapacidad tendrán derecho a ser protegidas por la ley frente a dichas injerencias o agresiones.
>
> 2. Los Estados Partes protegerán la privacidad de la información personal y relativa a la salud y a la rehabilitación de las personas con discapacidad en igualdad de condiciones con las demás.

Esta fórmula de reconocimiento es crucial para personas que, encontrándose en condiciones de residencia, se ven muchas veces expuestas a intromisiones lesivas de su privacidad. Pero, por supuesto, esta protección trasciende las condiciones de internación para amparar a las personas en situación de discapacidad siempre, cualquiera sea el lugar donde viven.[7]

Finalmente, no está demás advertir que el reconocimiento de la privacidad en la mirada constitucional comparada es prácticamente unánime en las constituciones posteriores a 1990, mientras en las anteriores es un derecho desarrollado y ya asentado, jurisprudencialmente.[8]

6 Jatindra Kumar Das, *Human Rights Law and* Practice, Delhi, PHI Learning, 2016, p. 443. Lo anterior, no obstante este tipo de reclamos suele encuadrarse, más que como un asunto de privacidad, como uno de autodeterminación. Johanna Gibson, "Community Rights to Culture: The UN Declaration on the Rights of Indigenous Peoples", en Stephen Allen y Alexandra Xanthaki (eds.), *Reflections on the UN Declaration on the Rights of Indigenous Peoples*, Oxford-Portland, Hart Publishing, 2011, pp. 436-7.

7 Valentina Della Fina, "Article 22 [Respect for Privacy]", en Valentina Della Fina y otros,(eds.), *The United Nations Convention on the Rights of Persons with Disabilities. A Commentary*, Cham, Springer, 2017, pp. 403-4.

8 Manuel José Cepeda, "Privacy", op. cit., p. 967. Vale la pena advertir que, a diferencia de lo que suele ser la regla general del reconocimiento de derechos en el derecho internacional de los derechos humanos, donde ese reconocimiento sigue a las recepciones domésticas, en el caso de la privacidad el camino fue el inverso. Oliver Diggelmann y Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", *Human Rights Law Review*, 14, 2014, pp. 441-2.

1.2 ¿Qué es la privacidad?

Esta pregunta se ofrece acá solo como una manera de abordar las diferentes concepciones que se han utilizado para delimitar el contenido de la privacidad. En efecto, uno de los principales problemas que afectan al derecho a la privacidad, como acertadamente ha señalado Solove, es que se trata de un concepto confuso. Lo anterior, principalmente, por su vaguedad, para lo que basta echar un vistazo a las disposiciones recién identificadas.[9] ¿Qué acercamientos se han utilizado para abordarla? Un reciente trabajo –quizá uno de los más comprensivos y disponible en Chile al respecto– los identifica del siguiente modo.[10] Una primera aproximación consiste en vincular la privacidad atendiendo "aquello que las normas y las cortes protegen cuando la invocan", lo que permite identificar, se afirma, "cuerpo, objetos, lugares".[11] En general, se trata de una estrategia que busca identificar aquello que distingue y singulariza a la privacidad de otros derechos.[12] Un segundo acercamiento consiste en definirla a partir de ideas o conceptos "asociados con ella … secreto, tranquilidad autonomía".[13] Un tercer acercamiento consiste en identificar "tipos de conducta o acciones que vulneran la privacidad".[14]

En vez de aventurarse en la difícil tarea de exponer la (siempre controvertida) esencia de algún concepto, cuestión que suele hacerse, además, en abstracto, este último acercamiento elabora una idea pragmática, histórica y culturalmente contextualizada, que permite identificar prácticas que deseamos proteger frente a intromisiones y perturbaciones que se desarrollan a partir de otras actividades (principalmente, aunque no exclusivamente, estatales). De este modo, "cuando protegemos la privacidad", cuidamos esas prácticas frente a "perturbaciones" indeseadas.[15] En otras palabras, se trata de identificar una serie de actividades que se inmiscuyen en la privacidad y que, por eso mismo, "son dañinas o problemáticas" –de lo que no se sigue, desde luego, que todas esas actividades gatillen siempre una reparación legal–.[16] A diferencia del primer enfoque, que termina asumiendo que la privacidad es una sola siempre y en todo lugar, y del segundo, que inevitablemente diluye la privacidad en otras consideraciones, el tercer acercamiento construye la privacidad "desde abajo", identificando los diferentes tipos de perturbaciones

9 Daniel J. Solove, *Understanding Privacy*, Cambridge, Harvard University Press, 2008, p. 1.
10 Rodolfo Figueroa, *Privacidad*, Santiago, Ediciones Universidad Diego Portales, 2014.
11 Ibíd, p. 107.
12 Daniel J. Solove, "Conceptualizing Privacy", *California Law Review*, 90, 2002, p. 1095.
13 Figueroa, *op. cit.*, p. 107.
14 Ibíd.
15 Solove, "Conceptualizing Privacy", *op. cit.*, p. 1092-3.
16 Solove, *Understanding Privacy*, *op. cit.*, pp. 8-10.

que invaden ciertas actividades haciéndolas imposibles, alterándolas gravemente y/o inhibiendo a los agentes de desarrollarlas.[17] Este es el enfoque que se privilegia en este capítulo, sin que esto signifique, por lo que se dirá a continuación, prescindir absolutamente de los otros acercamientos.

Ello, porque, si uno se pregunta cuál es el enfoque que se ha adoptado en el derecho internacional de los derechos humanos, podrá advertir que se ha privilegiado un acercamiento casuístico, y hasta cierto punto inagotable,[18] orientado a identificar los espacios (no solo físicos), objetos y cuerpos que la privacidad protege. Así, se ha dicho que la privacidad protege el control sobre el cuerpo, incluyendo decisiones relativas al cambio de nombre y otras vinculadas a la autonomía personal (tanto las relativas a la procedencia cultural como a la orientación sexual); que opera como una herramienta de salvaguarda de la inmunidad de las comunicaciones, incluidas las telefónicas y de correspondencia, frente a intromisiones indebidas; que ampara a las personas frente a revisiones, sea corporales o de sus domicilios, restringiéndolas a situaciones acotadas (como el levantamiento de evidencia en la persecución de delitos) o, en cualquier caso, sometiéndolas a controles (como los judiciales) que impidan su procedencia discrecional; y que prohíbe, salvo en caso de circunstancias bastante acotadas (como las antes descritas), la vigilancia, la interceptación de conversaciones y la captación de las mismas.[19]

La Observación General No. 16 del Comité de Derechos Humanos –sobre la que volveremos con más detalle en la siguiente sección– también adoptó un acercamiento similar.[20] Así, señaló que:

> El cumplimiento del artículo 17 exige que la integridad y el carácter confidencial de la correspondencia estén protegidos de jure y de facto. La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones. Los registros en el domicilio de una persona deben limitarse a la búsqueda de pruebas necesarias y no debe permitirse que constituyan un hostigamiento. Por lo que respecta

17 Ibíd, pp. 8-9.

18 Michael O'Flaherty, "Sexual orientation and gender identity", en Daniel Moeckli y otros (eds.), *International Human Rights Law* (2ª ed.), Oxford, Oxford University Press, 2014, p. 306.

19 David Weissbrodt y Connie de la Vega, *International Human Rights Law. An introduction*, Filadelfia, University of Pennsylvania Press, 2007, p. 67.

20 Comité de Derechos Humanos, Observación General No. 16, Artículo 17 (Derecho a la intimidad), U.N. Doc. HRI/GEN/1/Rev.7, 8 de abril de 1988.

> al registro personal y corporal, deben tomarse medidas eficaces para garantizar que esos registros se lleven a cabo de manera compatible con la dignidad de la persona registrada. Las personas sometidas a registro corporal por funcionarios del Estado o por personal médico que actúe a instancias del Estado serán examinadas sólo por personas de su mismo sexo.[21]

Indicó, además, que la información personal disponible en "computadoras, bancos de datos y otros dispositivos" también eran parte de la esfera privada de las personas.[22]

2. LOS ESTÁNDARES DEL DERECHO INTERNACIONAL

Ahora bien, sería un error concluir que el acercamiento desde el derecho internacional se agota, exclusivamente, en la recopilación casuística de espacios, cuerpos y objetos protegidos por la privacidad. En efecto, si se presta atención a lo que acá denominaremos estándares del derecho internacional de los derechos humanos, veremos que las pautas procedimentales que se han venido configurando permiten un acercamiento mucho más contextual a los problemas y lesiones a la privacidad, en línea con lo sugerido en la sección 1.2. Así, para efectos de este trabajo los estándares del derecho internacional apuntan a la configuración de las condiciones que habilitan la intervención estatal. Dicho de otro modo –y advirtiendo, como se dijo antes, que no toda actividad problemática para la privacidad gatilla su protección legal–, en esta sección se expondrán los requisitos que los Estados deben satisfacer para poder desarrollar prácticas y actividades sin infringir la privacidad, esto es, dentro del marco del derecho internacional al que se han comprometido autónomamente.

¿Qué requisitos deben satisfacer las actividades y prácticas estatales que, siendo, *prima facie*, intromisiones en la esfera de privacidad de las personas, se encuentran permitidas por el derecho internacional de los derechos humanos? Una de las primeras referencias específicas al respecto se encuentra, aunque de modo todavía poco sistematizado, en la Observación General No. 16, adoptada a propósito del art. 17 PIDCP.[23] Allí, se ha indicado que las intromisiones en la intimidad

21 Ibíd, párr. 8.
22 Ibíd, párr. 10.
23 Como se verá, se trata de un régimen regular que estructura las limitaciones y regulaciones de derechos en el ámbito del derecho internacional de los derechos humanos en un triple sentido: las limitaciones deben estar establecidas en una ley, deben perseguir fines legítimos en una sociedad democrática y encontrarse acotadas. Olivier De Schutter, *International Human Rights Law. Cases, Materials, Commentary*, Cambridge, Cambridge University Press, 2011 (reprin.), pp. 288-93.

de las personas requieren, en primer lugar, habilitación legal.[24] Desde luego que no basta con satisfacer el requerimiento formal, pues, en el contexto de las regulaciones del PIDCP, las regulaciones legales "debe[n] conformarse a las disposiciones, propósitos y objetivos del Pacto".[25] Ello quiere decir que las intromisiones en la privacidad de las personas deben estar reguladas en una ley y, además, satisfacer un cierto estándar material: deben perseguir un fin legítimo –típicamente, serán aceptables solo aquellas intromisiones que puedan justificarse como necesarias en una sociedad democrática–[26] y respetar los demás criterios que cada disposición contemple como fines aptos para la regulación de los derechos. Desde luego, las cláusulas de limitación o regulación de los derechos no pueden ser utilizadas para afectar al propio derecho.

Ahora bien, no basta apuntar a objetivos deseables o legítimos como razones suficientes para garantizar la inmunidad de la medida. En rigor, la responsabilidad de los Estados es la de mostrar cómo es que esas medidas en particular se encuentran conectadas con el fin que persiguen (conexión racional). Y, en caso de tratarse de medidas que afecten derechos humanos, debe, además, demostrarse que son "estrictamente necesarias" para poder satisfacer el fin legítimo.[27]

En tercer lugar, "se deben especificar con detalle las circunstancias precisas en que podrán autorizarse" injerencias en la vida privada de las personas.[28] De allí que las habilitaciones para las regulaciones de los derechos deban interpretarse en sentido estricto, evitando regulaciones vagas, delegaciones amplias y no sujetas a control posterior. Lo mismo corre para efectos de la configuración de bancos de datos o información personal, los que también deberán estar establecidos por ley.

Finalmente, a las condiciones regulares que el derecho internacional de los derechos humanos establece para las limitaciones de derechos, debe agregarse una consideración especial en el ámbito del derecho a la privacidad: la autodeterminación informativa, a saber, la posibilidad de acceder, revisar y demandar la actualización,

24 Ibíd, párr. 3.

25 Id.

26 Philip Alston y Ryan Goodman, *International Human Rights. The successor to International Human Rights in Context: Law, Politics and Morals*, Oxford, Oxford University Press, 2013, p. 160. En palabras de la propia observación:

"Como todas las personas viven en sociedad, la protección de la vida privada es por necesidad relativa. Sin embargo, las autoridades públicas competentes sólo deben pedir aquella información relativa a la vida privada de las personas cuyo conocimiento resulte indispensable para los intereses de la sociedad en el sentido que tienen con arreglo al Pacto. En consecuencia, el Comité recomienda que los Estados señalen en sus informes las leyes y reglamentos que regulan las injerencias autorizadas en la vida privada" (párr. 7).

27 De Schutter, *International Human Rights Law*, *op. cit*., pp. 313-4.

28 Comité de Derechos Humanos, Observación General No. 16, párr. 8.

rectificación o eliminación de datos personales, sea que estos estén contenidos en bancos de datos públicos o privados. Así, la observación dispone:

> Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación.[29]

A nivel regional, ha sido la Relatoría Especial para Libertad de Expresión la que ha ofrecido una mirada a estos estándares. Inicialmente lo hizo en su Informe Anual 2001,[30] donde sostuvo que la vida privada se encontraba protegida por la CADH y que debía cuidarse que sus regulaciones satisfagan las exigencias del derecho internacional de los derechos humanos, a saber:

> dictarse en conformidad con leyes legítimas y su contenido y finalidad deben atender el bien común y ser armonizadas sin limitar indebidamente el derecho a la libertad de expresión en la búsqueda y publicidad de información de interés público, entre otros.[31]

Del mismo modo, ese reporte abordó la situación del derecho de *habeas data* en la región. Sin embargo, y por razones obvias –a fin de cuentas, se trata de la Relatoría para la Libertad de Expresión–, se le trató con un acercamiento limitado, confiriéndole un lugar secundario. En un continente acertadamente preocupado por la protección de la libertad de expresión, como ahora, los informes de la Relatoría se han acercado a la privacidad a efectos de advertir cómo ella posee un umbral más bajo de protección tratándose de funcionarios públicos en el ejercicio de sus funciones. Ello explica que el análisis del *habeas data* no se haya incluido como una manifestación del derecho a la autodeterminación informativa, sino que en el contexto de las acciones de acceso a la información encaminadas a dotar de mayor transparencia

29 Ibíd, párr. 10.
30 Relatoría Especial para la Libertad de Expresión, Informe Anual 2001, https://www.oas.org/es/cidh/expresion/informes/anuales.asp
31 Ibíd, párr. 33.

al funcionamiento de los Estados de la región.[32] La contraposición, así, se ha trabado entre libertad de expresión y control político, de una parte, y las defensas que han enarbolado las autoridades, entre ellas el respeto a la privacidad, a efectos de escamotear el control ciudadano. Ese acercamiento, sin embargo, como se viene advirtiendo, es insuficiente para abordar las actividades y prácticas estatales que constituyen intromisiones en la esfera protegida de las personas.

Informes posteriores no han abordado sistemáticamente esta cuestión, aunque arrojan algunas luces acerca de otras esferas. A propósito de su informe sobre ciberseguridad, la Relatoría ha manifestado que el respeto a la libertad de expresión demanda la protección de la privacidad.[33] De este modo, llama a los Estados a proteger el anonimato e intimidad de las personas de modo de permitirles una participación libre de amedrentamientos en la esfera pública.[34] Por supuesto que el anonimato no debe garantizarse para ejecutar fines contrarios a la CADH (como la difusión de pornografía infantil). Pero de ello no se sigue que las autoridades no deban respetar las condiciones que les permitan moverse dentro de los parámetros autorizados. En resumen, el Estado tiene la obligación de establecer regímenes legales de protección de datos personales, regulando su almacenamiento (incluida su eliminación y uso para fines contrarios a los tratados), uso y transferencia,[35] así como asegurar el derecho de las personas a acceder, revisar y solicitar la modificación, en su caso, de su información personal en manos del Estado.[36]

Más recientemente, la Relatoría ha instado a los Estados a avanzar en políticas públicas orientadas a eliminar el tratamiento de datos personales o, en su defecto, a reducirlo solo para casos en que se encuentren legitimados o autorizados por la persona afectada.[37] En estos últimos casos, los Estados deben respetar importantes condiciones:

> 1) que los datos no se utilicen para fines distintos a los denunciados, 2) que el mantenimiento y almacenamiento de datos se haga conforme a dichos fines y solo durante el plazo informado y consentido, y 3) que los datos sean compartidos o difundidos sólo en las condiciones y para los fines consentidos e informados.[38]

32 La crítica se encuentra adecuadamente tratada en Pedro Anguita, *La Protección de datos personales y el derecho a la vida privada. Régimen jurídico, jurisprudencia y derecho comparado*, Santiago, Editorial Jurídica de Chile, 2007, pp. 82-3.

33 Relatoría Especial para la Libertad de Expresión, Informe Anual 2013, https://www.oas.org/es/cidh/expresion/informes/anuales.asp, párr. 130.

34 Ibíd, párrs. 133-5.

35 Ibíd, párrs. 138-9.

36 Ibíd, párr. 140.

37 Relatoría Especial para la Libertad de Expresión, Informe Anual 2016, https://www.oas.org/es/cidh/expresion/informes/anuales.asp, párr. 205.

38 Ibíd, párr. 206.

La vigilancia masiva de las comunicaciones cibernéticas, en sí "una injerencia en la privacidad de las personas", debe, por ello, someterse a las condiciones antes identificadas (legalidad, persecución de un fin legítimo, racionalidad medio-fin, necesidad, excepcionalidad, carácter taxativo y estricto de las autorizaciones).[39]

Otro lugar donde conviene mirar en búsqueda de estos estándares es en la jurisprudencia de la Corte Interamericana de Derechos Humanos (en adelante, Corte IDH). En *Tristán Donoso*,[40] la Corte decidió sobre la denuncia de interceptación y divulgación de una conversación entre un abogado y su cliente. La Corte indicó que, si bien el derecho a la vida privada no era absoluto, las injerencias en ese ámbito estaban sujetas a un estricto estándar de procedencia en línea con lo que acá se ha venido afirmando: debían estar previstas en una ley, perseguir un fin legítimo y "cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática".[41] La divulgación de la información, por su parte, fue también evaluada en tanto injerencia y, por lo mismo, objeto de escrutinio en los mismos términos antes citados. Por lo tanto, la injerencia solo sería compatible con la CADH si estaba autorizada en una ley (en sentido formal y material).

En el *Caso Escher*,[42] la Corte IDH, pronunciándose sobre la interceptación, captación y divulgación de conversaciones privadas por parte del Estado de Brasil, reiteró estas consideraciones. La Corte debía decidir acaso la intromisión denunciada era abusiva o arbitraria en los términos del artículo 11.2 de la CADH. Para ello, afirmó que debería evaluar si acaso esas injerencias estaban previstas en la ley, perseguían un fin legítimo y eran idóneas, necesarias y proporcionales.[43] Con respecto a la legalidad, sostuvo que era necesario que el instrumento que autorizaba las injerencias fuera una ley tanto en sentido material como formal. Además, las circunstancias y condiciones en que se autorizaban las injerencias debían encontrarse claramente establecidas, con suficiente detalle y precisión.[44] El robusto contenido que la Corte IDH confiere al estándar de legalidad es relevante porque, en caso de no respetarse –como ocurrió en *Escher*– estima que no debe proseguir al análisis de las demás etapas.

39 Ibíd, párrs. 213-26.
40 Corte IDH, *Tristán Donoso vs. Panamá*, 27 de enero de 2009.
41 Ibíd, párr. 56.
42 Corte IDH, *Escher y otros vs. Brasil*, 6 de julio de 2009.
43 Ibíd, párr. 129.
44 Ibíd, párrs. 130-1.

La Corte IDH ha tenido también ocasión de abordar estos estándares a propósito de la violencia sexual,[45] las relaciones entre libertad de expresión y vida privada,[46] la autonomía sexual y personal,[47] y las relaciones entre privacidad y el desarrollo de la propia personalidad y aspiraciones.[48]

A nivel europeo, es el propio CEDH el que establece las condiciones que habilitan la intervención de la autoridad. Así, el art. 8.2 CEDH dispone que:

45 Corte IDH, *Fernández Ortega y otros vs. México*, 30 de agosto de 2010. Donde, principalmente sobre la base de una concepción espacial, sostuvo que:
la protección de la vida privada, la vida familiar y el domicilio implica el reconocimiento de que existe un ámbito personal que debe estar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. En este sentido, el domicilio y la vida privada y familiar se encuentran intrínsecamente ligados, ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida privada y la vida familiar (párr. 157).
El ingreso a ese espacio, sin autorización legal o consentimiento de sus habitantes, constituye una "injerencia arbitraria y abusiva en su domicilio" (párr. 159).

46 Corte IDH, *Fontevecchia y Dámico vs. Argentina*, 29 de noviembre de 2011. Allí, sostuvo que el Estado tiene deberes negativos –de no intromisión arbitraria– y positivos –de adoptar medidas destinadas a asegurar el derecho– con respecto a la vida privada (párr. 49). Respecto a la articulación entre libertad e expresión y vida privada, razonó que:
la Corte debe encontrar un equilibrio entre la vida privada y la libertad de expresión que, sin ser absolutos, son dos derechos fundamentales garantizados en la Convención Americana y de la mayor importancia en una sociedad democrática. El Tribunal recuerda que el ejercicio de cada derecho fundamental tiene que hacerse con respeto y salvaguarda de los demás derechos fundamentales (párr. 50).

47 Corte IDH, *Atala Riffo* y Niñas v*s. Chile*, 24 de febrero de 2012. Sostuvo así en su párr. 161:
La vida privada es un concepto amplio que no es susceptible de definiciones exhaustivas y comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos. Es decir, la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás.

48 Corte IDH, *Artavia Murillo y otros vs. Costa Rica*, 28 de noviembre de 2012. Allí, la Corte sostuvo en términos elocuentes que:
El ámbito de protección del derecho a la vida privada ha sido interpretado en términos amplios por los tribunales internacionales de derechos humanos, al señalar que va más allá del derecho a la privacidad. La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad. Además, la Corte ha señalado que la maternidad forma parte esencial del libre desarrollo de la personalidad de las mujeres. Teniendo en cuenta todo lo anterior, la Corte considera que la decisión de ser o no madre o padre es parte del derecho a la vida privada e incluye, en el presente caso, la decisión de ser madre o padre en el sentido genético o biológico (párr. 143).

> No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Así, parte importante de las decisiones del Tribunal Europeo de Derechos Humanos (en adelante, TEDH) ha girado en torno a la delimitación de estas condiciones. En primer lugar, resulta claro que, en el contexto europeo, al igual que en el regional, las obligaciones estatales incluyen tanto deberes de abstención (obligaciones negativas) como obligaciones positivas: la de establecer un sistema efectivo que permita asegurar la vida privada de individuos y sus familias.[49]

Con respecto a los estándares propiamente tales, el TEDH ha señalado que las injerencias deben estar autorizadas por ley, expresión que cubre tanto legislación escrita como no escrita.[50] Sin embargo, el criterio mismo de legalidad es complementado en diversos sentidos: para el sistema europeo de derechos humanos, una ley satisface los estándares del CEDH si es que ella (i) es lo suficientemente accesible para los ciudadanos y ciudadanas, (ii) regula las hipótesis de interferencia con suficiente precisión "de modo de permitir a los ciudadanos regular su propia conducta"[51] e (iii) incorpora medidas efectivas de resguardo (por ejemplo, reglas sobre limitación temporal de las interferencias, precauciones precisas para evitar la apropiación de la información por terceras partes) que protejan a las personas frente a intromisiones arbitrarias.[52] Del mismo modo, ha dicho que las intromisiones, en especial tratándose de medidas secretas, deben ser claras y detalladas de modo de evitar la arbitrariedad.[53] Los Estados, además, deben mostrar que las interferencias satisfacen algunos de los objetivos listados en el artículo 8.2. Los objetivos mismos

49 Corte EDH, *Söderman vs. Sweden*, 12 de noviembre de 2013, párr. 78.

50 TEDH, *Case of the Sunday Times vs. The United Kingdom (No. 1)*, 26 de abril de 1979, párr. 47.

51 Ibíd, párr. 49. Es lo que ocurriría en caso de que las regulaciones legales permitieran que las injerencias fuera secretas o desconocidas para los afectados. Así lo sostuvo el TEDH, *Liberty and Others vs. United Kingdom*, 1 de julio de 2008:
It is not in dispute that the interference in question had a legal basis in sections 1-10 of the 1985 Act (see paragraphs 16-27 above). The applicants, however, contended that this law was not sufficiently detailed and precise to meet the "foreseeability" requirement of Article 8(2), given in particular that the nature of the "arrangements" made under section 6(1)(b) was not accessible to the public (párr. 60).

52 Richard Clayton y Hugh Tomlinson, *Privacy and Freedom of Expression*, Oxford, Oxford University Press, 2010 (2ª ed.), pp. 118-9.

53 TEDH, *Weber and Saravia vs. Germany*, 29 de junio de 2006, párr. 93.

allí listados son bastante amplios, lo que ha ido acompañado de una práctica decisional del Tribunal que ha conferido amplio margen a los Estados a la hora de definir esos intereses. Sin embargo, él mismo suele enfatizar el deber de cuidado de los Estados en el ejercicio de poderes tan intrusivos.[54] Finalmente, si las medidas afectan derechos humanos, estas deben ser necesarias en una sociedad democrática. Si bien el TEDH ha sostenido que los Estados gozan de un amplio margen de apreciación para determinar cuándo está presente esa necesidad, ha indicado que la medida será necesaria mientras logre demostrarse que ella, interpretada de manera restringida, responde a un interés social acuciante y es proporcionada.[55] El Tribunal ha entendido que se satisface este estándar, también, si el Estado ha dispuesto de garantías suficientes y efectivas contra los abusos que se puedan cometer, medidas que deberán evaluarse dependiendo del caso concreto y que incluyen la evaluación de la naturaleza de las medidas, su duración, las bases y condiciones para poder ordenarlas, el tipo de autoridad competente para ordenarlas, implementarlas y supervisarlas, así como los tipos de resguardos.[56]

Todavía a nivel europeo –pero ahora en lo concerniente a la aplicación de la Carta de los Derechos Fundamentales de la Unión Europea– el Tribunal Europeo de Justicia (en adelante TEJ) ha tenido oportunidad de referirse a la configuración de la protección de datos personales y las obligaciones que surgen para los Estados. En el conocido caso *Digital Rights Ireland*,[57] el TEJ sostuvo que las intromisiones en los derechos reconocidos en los artículos 7 y 8 de la CDFUE debían encontrarse establecidas por ley, respetar la esencia de los derechos y sujetarse al test de proporcionalidad.[58] De conformidad a este test, el TEJ evalúa si las medidas eran estrictamente necesarias. Así, por ejemplo, más recientemente ha sentenciado que los sistemas de recopilación masiva o indiscriminada de datos afectan decisivamente la proporcionalidad de las interferencias, en la medida que es tal la cantidad de información a la que se tiene acceso, que permite trazar conclusiones bastante precisas relativas a los hábitos, movimientos, lugares de visita y de permanencia de las personas. Sin duda –prosiguió el TEJ– existe la posibilidad de configurar perfiles sobre las personas construidos a partir de información especialmente sensible.[59]

54 Véase, en general, Alastair R. Mowbray, *Cases and Materials on the European Convention on Human Rights*, Oxford, Oxford University Press, 2007 (2ª ed.), pp. 591-3.
55 TEDH, *Sommer vs. Germany*, 27 de abril de 2017, párr. 55.
56 TEDH, *Weber and Saravia vs. Germany*, párr. 106.
57 TEJ, *Digital Rights Ireland*, 8 de abril de 2014.
58 Ibíd, párr. 38.
59 TEJ, Tele 2, *Sverige AB v Post-och Telestyrelsen and Secretary of State for the Home Department v. Watson, Brice, and Lewis*, 21 de diciembre de 2016, párrs. 97-101.

Además, las limitaciones serán admitidas solo si satisfacen intereses generales reconocidos por la Unión Europea o son establecidas para proteger los derechos de los demás.[60] Si bien en ese mismo caso el TEJ sostuvo que la retención de datos era una intromisión relevante, ella no afectaba la esencia en sí del derecho cuando (como entonces) se establecían principios y mecanismos de resguardo y protección que regulan la actividad de los agentes recolectores.[61]

3. UN PROBLEMA: LAS CÁMARAS DE VIGILANCIA

Como se ha visto, aún a modo genérico, los Estados llevan adelante, y pueden desarrollar, una serie de actividades y prácticas que, en principio, podrían estar justificadas, siempre que no infrinjan las obligaciones que surgen del derecho internacional de los derechos humanos. Esta sección comienza (3.1) identificando cuáles son esas actividades a las que prestará atención este capítulo, a saber: la vigilancia en los espacios públicos por medio de cámaras situadas en globos aerostáticos y drones. Una vez presentadas y justificada la importancia de mirar a esas actividades –respecto de las que, como se verá, el propio derecho internacional de los derechos humanos ha llamado la atención– se avanzará a (3.2) la evaluación de la regulación legal de esas actividades en Chile.

3.1. Privacidad y nuevas tecnologías

Como se ha señalado, la protección legal de la privacidad busca resguardarla frente a una variedad de actividades y prácticas que resultan problemáticas, dañinas o lesivas para ella. De todas esas actividades, este capítulo se enfocará en las que se encuentran vinculadas al uso de cámaras de vigilancia dispuestas en globos y drones que algunas municipalidades han comenzado a utilizar durante el último año.[62]

¿Por qué es esto relevante? Como se indicó en la introducción de este capítulo, las autoridades que promueven este tipo de medidas de vigilancia insisten en que si las personas no han hecho nada malo (cometer delitos, incurrir en faltas),[63] no tienen nada que ocultar; entonces

60 TEJ, *Digital Rights Ireland*, párr. 38.

61 Ibíd, párr. 40.

62 El énfasis en el uso de las tecnologías, por lo tanto, deja afuera otras formas de recopilación de información que son igualmente dañinas para la privacidad, como la interrogación. Del mismo modo, el capítulo advertirá, principalmente al anotar la falta de regulación en medio de la que actúan los municipios, problemas derivados de esa captación como el procesamiento y diseminación de esa información.

63 *La Hora 20*: "Presentan recurso contra los drones de vigilancia", 23 de mayo de 2017. "Nuestra prioridad", afirmó el alcalde Las Condes, Joaquín Lavín, "es la seguridad de la comuna y además, quien nada hace, nada teme".

no deberían temer a la observación, incluso continua, del Estado. ¿Es cierto que no hay nada que temer? ¿No hay, fuera del interés estatal (legítimo) en el control de la delincuencia, otros intereses que debieran ser objeto de consideración? Lo primero que debiera anotarse, es que no es cierto que cuando las personas no han cometido delitos o faltas ("nada malo") no tengan nada que ocultar. Pero más equivocado aún es creer que la privacidad es una herramienta a la que se recurre para esconder cosas malas (ilegales). De hecho, la mayor parte de las veces las personas reclaman privacidad para dejar al margen del conocimiento de terceras personas acciones que son completamente legales. Pero también –y esto conviene reiterarlo– se recurre a la privacidad para proteger actividades que no se han querido esconder (como el mismo hecho de salir a la calle) en lo absoluto.[64]

Enseguida, y en relación a esto último, debe enfatizarse que las personas son titulares del derecho a la privacidad también en el espacio público o espacios de libre acceso. Hasta cierto punto, la vida en el espacio público asegura (o aseguraba) un cierto grado de privacidad. No es que las personas no se vean unas a otras, pero sí que se proteja una relativa conciencia de que allí, afuera, en medio de la masa, es (o era) posible obtener ciertas cuotas de anonimato. Lo cierto es que, tanto en el derecho internacional de los derechos humanos,[65] como en el derecho constitucional comparado,[66] el espacio público no elimina las expectativas de privacidad de las personas. La privacidad, entonces, es más que una forma de secreto e involucra una gama variopinta de situaciones –algunas de las cuales demandan secreto, desde luego, pero sin agotar su contenido–.[67]

Estas ideas no son en absoluto ajenas a nuestra cultura jurídica. De hecho, no es posible afirmar descansando en la práctica constitucional nacional, que las personas, una vez situadas en el espacio público, carezcan de cualquier protección frente a las fotografías o grabaciones de terceras personas (mientras realizan, como se dijo antes, acciones completamente legales como tomar sol). Existe una variedad de casos vinculados al uso comercial de la imagen de personas, no solamente famosas, cuyos rostros han sido utilizados sin su consentimiento. Esos

64 Daniel Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven y Londres, Yale University Press, 2011, pp. 23-7.

65 Clayton y Tomlinson, *Privacy and Freedom of Expression*, *op. cit*., p. 93, 96-7; N.A. Moreham, "Privacy in Public Places", *Cambridge Law Journal*, 65(3), 2006. Así, el TEDH sostuvo en *Hannover vs. Germany*, 24 de junio de 2004, que el derecho a la privacidad protege más allá del círculo íntimo, para alcanzar la integridad física y sicológica de las personas, incluidas una dimensión social y sus relaciones con otras personas; también Comisión de Venecia, *On video surveillance in public places by public authorities and the protection of human rights*, CDL-AD(2007) 014, 16-7 de marzo de 2007, párrs. 24-5.

66 Manuel José Cepeda, "Privacy", *op. cit*., p. 971-2.

67 Solove, *Nothing to Hide*, *op. cit*., p. 27.

casos han sido resueltos a favor de la privacidad (como la facultad constitucionalmente protegida, pero inevitablemente mercantil, de poder decidir cómo "invertir" con su propia imagen), aun cuando las imágenes han sido captadas en espacios públicos.[68] Sin embargo, un razonamiento similar se ha mantenido para situaciones que no involucran el valor comercial de los cuerpos.[69] Lo mismo ha ocurrido a nivel de control de constitucionalidad[70] y administrativo.[71]

¿Qué es, en particular, lo problemático de las actividades de monitoreo y vigilancia constante y masiva que desarrolla el Estado? Estas actividades son problemáticas en tanto pueden acarrear (nótese que el "pueden acarrear" es crucial a efectos de entender las recomendaciones que acompañan este capítulo) daños complejos para la privacidad de las personas.[72] La recopilación de información obtenida por medio de la vigilancia sin autorización de las personas, genera el malestar e incomodidad –cuando no ansiedad– de estar constantemente bajo control.[73]

Pero no solo eso. La cantidad de información que una vigilancia constante es capaz de producir, acompañada de su procesamiento (agregación), facilita los usos secundarios que se hace de esa

68 Pedro Anguita se refiere a este cúmulo de casos, acertadamente, como "derecho a la propia imagen y valor comercial", en Pedro Anguita, "Jurisprudencia constitucional sobre el derecho a la propia imagen y a la vida privada en Chile (1981-2004): un intento de sistematización", Felipe González (ed.), *Libertad de Expresión en Chile*, Santiago, Universidad Diego Portales, 2006, pp. 377-93.

69 Véase el análisis de este desarrollo jurisprudencial en Gastón Gómez, *Derechos fundamentales y recurso de protección*, Santiago, Universidad Diego Portales, 2005, pp. 325-33 y Figueroa, *Privacidad*, *op. cit*., pp. 360-73.

70 Tribunal Constitucional, Sentencia Rol 1894, 12 de julio de 2011, citando a don Eduardo Novoa Monreal:
Que la intimidad no sólo puede darse en los lugares más recónditos, sino que también se extiende, en algunas circunstancias, a determinados espacios públicos donde se ejecutan específicos actos con la inequívoca voluntad de sustraerlos a la observación ajena (considerando 23).

71 Así, el Consejo para la Transparencia ha dicho que:
resulta indudable que la garantía constitucional de la vida privada comprende también a las imágenes captadas por cualquier medio, como por ejemplo los globos aerostáticos instalados por la Municipalidad, y el tratamiento que de ellas pueda realizar la autoridad, como la entrega de dichas imágenes a un tercero, se encuentra limitado en función de la protección de este derecho (considerando 5).
la posibilidad de captar imágenes de personas en ámbitos públicos y otros exclusivamente privados y difundir dichas imágenes, sin poder contar con el consentimiento del titular, aparece como una afectación de los derechos de dichas las personas, en particular, el derecho a la imagen, a la privacidad e, incluso a la intimidad (considerando 6).
Consejo para la Transparencia, Decisión Amparo Rol C2493-15, 26 de enero de 2016.

72 La taxonomía que acá se sigue ha sido tomada de Solove, *Understanding Privacy*, op. cit., pp. 101-70.

73 Ibíd, pp. 106-12. Desde luego que se trata de un malestar que trasciende la mera sensación personal y que puede terminar afectando el ejercicio de otros derechos, como la libertad de desplazamiento, cuando frente a estas formas de control social alteramos hábitos o desplazamientos –es decir cuando dejamos de hacer cosas que eran completamente legales–.

información –incluida la diseminación de información sensible y la extorsión del afectado–, permitiendo conectarla a sujetos específicos a los que pertenece. Ello permite, por caso, develar patrones (como hábitos) que, en principio, no hay razón para exponerlos a conocimiento estatal. Menos, desde luego, tratándose de actividades completamente lícitas. El TEJ, en el caso *Digital Rights*, lo sintetiza de esta acertada manera:

> Los datos, tomados como un todo, permiten dibujar conclusiones bastante precisas relativas a la vida de las personas cuyos antecedentes han sido captados, tales como hábitos diarios, lugares permanentes o temporales de residencia, movimientos diarios y otros, las actividades desarrolladas, las relaciones sociales de esas personas y los ambientes sociales frecuentados por ellas.[74]

El TEDH, por su parte, ha sostenido, en sentido similar, que:

> Hay un número relevante de elementos a ser considerados para determinar acaso la vida privada de una persona se ha afectado por medidas adoptadas fuera de su hogar o en sus instalaciones privadas. Mientras hay ocasiones en que las personas, con conocimiento o intencionalmente, toman lugar en actividades en el espacio público que saben que son o pueden ser grabadas o reportadas, la expectativa de privacidad de esas personas es un elemento relevante pero no concluyente (…) Consideraciones relativas a la privacidad pueden ser muy relevantes, sin embargo, tratándose de medidas de grabación sistemáticas o permanentes de los espacios públicos.[75]

Si la persona que nada hace, nada debe temer, entonces no debiera estar sujeta a sistemas de vigilancia que permiten que una cantidad relevante de información pueda serle vinculada de manera automática, revelando, así, información sensible. Todo lo anterior, además, con respecto a actividades que son perfectamente legales.[76]

¿Es esto relevante en el derecho internacional de los derechos humanos? Desde luego que sí. El desarrollo de la privacidad en el contexto de las nuevas tecnologías, las que están vinculadas no solo al uso de internet, sino que también a las nuevas herramientas con que cuentan los órganos estatales para efectos de llevar adelante actividades de vigilancia, indica que existe una preocupación especialmente sensible respecto a las formas en que los Estados se embarcan en actividades de

74 TEJ, *Digital Rights Ireland*, párr. 99.
75 TEDH, *Peck vs. United Kingdom*, 28 de enero de 2003, párr. 58 (citando *P.G. and J.H.*).
76 Ibíd, p. 117.

recolección de información respecto de sus ciudadanos y ciudadanas, el tratamiento que se hace de esa información y los usos que se da a la misma.

De acuerdo al sistema universal de derechos humanos, los avances tecnológicos han conferido a los Estados importantes herramientas para embarcarse en procesos de vigilancia masiva y recopilación indiscriminada de datos personales de ciudadanos y ciudadanas.[77] Si bien se acepta que la tecnología puede transformarse en herramienta útil para la consecución de ciertos fines legítimos que los Estados pueden perseguir –como el enfrentamiento del terrorismo, que no es nuestro caso, o el control del delito –,[78] se enfatiza que esas actividades deben respetar los estándares del derecho internacional de los derechos humanos.

Específicamente tratándose de las actividades de vigilancia llevadas a cabo por los Estados,[79] se ha enfatizado que estos deben no solamente abstenerse de entrometerse en la privacidad de las personas, sino que, además, crear las condiciones adecuadas para prevenir tales violaciones.[80] ¿Qué condiciones? Una legislación adecuada de protección que se conforme a los estándares del derecho internacional, una revisión de los procedimientos internos y el establecimiento de un órgano independiente de supervisión, capaz de asegurar la adecuada transparencia y rendición de cuentas de las actividades de vigilancia estatal.[81]

En lo que respecta a la idea de legislación adecuada, se ha vuelto a insistir en la necesidad de regular las intromisiones por medio de leyes en sentido tanto formal como material. Del mismo modo, se rechazan las facultades de intromisión genéricas y se demandan medidas

77 Asamblea General de Naciones Unidas, *Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age*, A/RES/68/167, 21 de enero de 2014; Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *El derecho a la privacidad en la era digital*, A/HRC/27/37, 30 de junio de 2014, párrs. 2-3; Consejo de Derechos Humanos, *The right to privacy in the digital age*, A/HRC/34/L.7/Rev.1, 22 de marzo de 2017.

78 Aunque debe anotarse que, en contextos de populismo penal y "psicología del miedo", el recurso al control del delito como fin legítimo merece un escrutinio más estricto a efectos de evaluar la necesidad y proporcionalidad de las medidas. Consejo de Derechos Humanos, Joseph Cannataci, *Report of the Special Rapporteur on the right to privacy,* A/HRV/34/60, 24 de febrero de 2017, párr. 42 a., b.

79 El énfasis de las resoluciones e informes que ahora se identifican, pone el acento en las actividades de vigilancia, cuando no espionaje, cibernético. Como se verá, sin embargo, se reiteran las condiciones de legalidad, necesidad y proporcionalidad que se han identificado antes (en 2) y que, para estos efectos, son igualmente aplicables. Véase, a modo de ejemplo, la opinión de la Comisión de Venecia, *On video surveillance in public places*, *op. cit*.

80 Asamblea General de Naciones Unidas, *Resolution adopted by the General Assembly on 18 December 2013*, op. cit., párr. 4 b); Consejo de Derechos Humanos, *The right to privacy in the digital age*, párr. 5.

81 Asamblea General de Naciones Unidas, *Resolution adopted by the General Assembly on 18 December 2013*, párr. 4 b) c) d).

necesarias y proporcionadas. Ello solo es posible (pero no suficiente) si las injerencias están establecidas en una ley "lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia …".[82] Finalmente, las medidas no deben lesionar los derechos en su esencia, estándar que es bastante complejo ya de satisfacer –indica el mismo informe– tratándose de programas de "vigilancia en masa o 'a granel' [los que] pueden considerarse arbitrarios, aunque persigan un objetivo legítimo …".[83]

¿Sugiere el derecho internacional –y este mismo capítulo, hacia sus conclusiones– que el Estado debe abdicar del uso de las tecnologías a efectos del control del delito y abandonar todo monitoreo? Por supuesto que no. Pero sí que esas actividades, precisamente por su grado de intromisión en la privacidad de las personas, se encuentren estrictamente reguladas y supervisadas. Una forma de satisfacer esa exigencia es ofreciendo a las personas medidas preventivas, garantías procesales y un esquema de supervisión efectiva.[84] Esto es relevante porque indica que no basta con que exista alguna fuente normativa genérica a la que se pueda echar mano para justificar las intromisiones (veremos que este es el caso de Chile), sino que es necesario que esas fuentes normativas –además de ser leyes en el sentido antes dicho– creen recursos e instituciones adecuadas para efectos de proteger los derechos de las personas.[85]

3.2 La situación de Chile: globos y drones

¿Cuál es la situación de Chile, a este respecto? Preocupante. ¿Cómo se encuentra el país frente al cumplimiento de esas obligaciones? Muy en deuda. En primer lugar, y en términos generales, Chile carece de una legislación vigorosa de protección a la privacidad de las personas. La ley actualmente vigente (Ley 19.628)[86] ha sido criticada, entre otras cosas, por establecer como regla general la publicidad de la información, carecer de un órgano adecuado para el amparo de la información personal

82 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *El derecho a la privacidad en la era digital*, *op. cit*., párrs. 21-3, 28-9.

83 Ibíd, párr. 25. En efecto, se indica en el informe en cuestión que:
Uno de los factores que deben considerarse al determinar la proporcionalidad es qué se hace con los datos a granel y quién puede acceder a ellos una vez recopilados. Muchos marcos nacionales carecen de "limitaciones de uso", permitiendo así la recopilación de datos para un objetivo legítimo, pero su uso posterior para otros (párr. 27).
El relator especial para el derecho a la privacidad, por su parte, se pregunta si acaso no será más proporcional frente a estas medidas de recopilación masivas la utilización de medidas acotadas. Consejo de Derechos Humanos, *Report of the Special Rapporteur on the Right to Privacy*, *op. cit*., párr. 42 c.

84 Consejo de Derechos Humanos, *The right to privacy in the digital age*, *op. cit*., párr. 5 f), g).

85 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *El derecho a la privacidad en la era digital*, *op. cit*., párr. 37

86 Sobre Protección de la Vida Privada.

y prescindir, en una serie amplísima de hipótesis, del consentimiento de las personas –los titulares de derechos fundamentales–.[87] Todavía en términos generales, la regulación misma de la videovigilancia en Chile ofrece vacíos importantes que han permitido su proliferación sin sujeción a los estándares mínimos de razonabilidad –del modo en que esos estándares se han desarrollado a nivel del Tribunal Constitucional, de la misma (aunque deficiente) Ley 19.628[88] y el derecho internacional de los derechos humanos–.

Veamos el caso en concreto que aborda este capítulo. Entre 2015 y 2017 varias municipalidades anunciaron e implementaron el uso de cámaras de vigilancia a través de globos aerostáticos o drones. Mientras se terminaba de redactar este capítulo, además, la Municipalidad de Las Condes anunciaba la implementación de cámaras de reconocimiento facial.[89] Un primer antecedente relevante a considerar, es la acción de protección que se presentó en contra de los municipios de Lo Barnechea y Las Condes apenas se puso en marcha el sistema de vigilancia con globos aerostáticos.[90] En ese recurso se reclamaba, entre otras, que esos sistemas de vigilancia bien podrían terminar invadiendo espacios privados y que, en general, su funcionamiento estaba en manos de empresas privadas.[91]

87 Véase, en términos generales, Anguita, *La Protección de Datos Personales*, *op. cit*., pp. 331-2. Como se dirá enseguida, esta ley confiere a los organismos públicos amplias facultades para efectos de crear bases de datos, al tiempo que las municipalidades –no obstante estar comprendidas bajo sus regulaciones– no suelen apuntar a aquella como una norma que gobierne sus actividades de vigilancia.

88 Por ejemplo, el sistema de videovigilancia en Chile se encuentra regulado por instrucciones internas de Carabineros de Chile y sobre la base de facultades normativas bastante débiles. Luis Cordero, "Videovigilancia e intervención administrativa: Las cuestiones de legitimidad", *Expansiva: en foco*, 137, 2008, pp. 10-12. Por lo demás, la misma regulación administrativa –contenida originalmente en una orden general reservada– carece de regulaciones adecuadas en lo relativo al respeto a la privacidad de las personas. Véase, en general, Patricio Palacios, *Análisis crítico del régimen jurídico de videovigilancia de las Fuerzas de Orden y Seguridad Pública*, Tesis para optar al grado de Magíster con mención en Derecho Público, Universidad de Chile, Facultad de Derecho, 2007. Con respecto a las cámaras de vigilancia de la denominada Unidad Operativa de Control de Tránsito, la normativa no regula la eliminación de la información por ellas captada. Sí existe, en cambio, regulación administrativa orientada a determinar los valores y cobros de la información que esas cámaras capten, en caso de que terceras personas deseen "darle un nuevo uso informativo para fines comerciales o como herramienta de servicio a la comunidad". Decreto 41, Ministerio de Transporte y Telecomunicaciones-Subsecretaría de Transportes de 2005. Existen algunas innovaciones más recientes en lo relativo al uso de cámaras en la Ley 20.844, sobre Derechos y Deberes de Asistentes y Organizadores de Espectáculos de Fútbol Profesional.

89 *El Mercurio*: "Las Condes implementa cámaras con reconocimiento facial para detectar a delincuentes", 23 de junio de 2017, C1.

90 Como se dirá inmediatamente, las mismas municipalidades apuntan a la sentencia que decidió el recurso de protección como fuente normativa de sus atribuciones y reglamentación.

91 Los antecedentes están tomados de Corte Suprema, *Soffge Guemes, Stephanie y otros c/ Ilustre Municipalidad de Las Condes y otro*, 1 de junio de 2016.

En lo medular, la Corte sostuvo que la realización material de las funciones de las municipalidades en cuestión, a través de empresas privadas, en caso alguno implicaba una delegación de potestades.[92] En lo que respecta a la legalidad en general de los municipios, la Corte entendió –en contra de los estándares del derecho internacional antes descritos– que "es indiscutible que el apoyo y fomento a la seguridad ciudadana es, actualmente, una relevante función municipal",[93] citando enseguida el artículo 4 letra j) de la Ley Orgánica Constitucional de Municipalidades (LOCM). Dicho precepto dispone que las municipalidades podrán desarrollar funciones relacionadas con:

> El desarrollo, implementación, evaluación, promoción, capacitación y apoyo de acciones de prevención social y situacional, la celebración de convenios con otras entidades públicas para la aplicación de planes de reinserción social y de asistencia a víctimas, así como también la adopción de medidas en el ámbito de la seguridad pública a nivel comunal, sin perjuicio de las funciones del Ministerio del Interior y Seguridad Pública y de las Fuerzas de Orden y Seguridad.

No hay, desde luego, evaluación de legalidad estricta (esto es, identificación de fuentes normativas que expresamente confieran la facultad), menos un escrutinio de la especificidad y proporcionalidad de las medidas. Fuera de estas referencias generales, el resto de la sentencia de la Corte Suprema se instala, prácticamente, en perfecta oposición al derecho internacional de los derechos humanos, los desarrollos del derecho constitucional comparado y la propia práctica constitucional doméstica. Así, cuestiona que en el espacio público exista una expectativa "mayor" de privacidad, salvo tratándose de ciertos ilícitos penales –contradiciendo su propio desarrollo al respecto–, mientras extiende autorización para el uso de cámaras de vigilancia por analogía, pues ya existen para otros supuestos legales sin suscitar "censura alguna". Para concluir, emite –casi como si estuviera dictando un reglamento– lo que denomina un régimen de autorización en el que ordena (i) grabar solo en espacios públicos, (ii) para lo que un funcionario municipal deberá certificar que esta regla se respete. Además, (iii) dispone la destrucción cada 30 días de las grabaciones –salvo en caso de imágenes de delitos—y (iv) configura un régimen de acceso a la información para ciudadanos.[94]

92 Ibíd, considerando 6.
93 Ibíd, considerando 7.
94 Como acertadamente se ha indicado, este régimen es, en sí mismo, una forma de corroborar que se afectará la privacidad, incluida la de los espacios privados. Tomás Ramírez, "Nuevas tecnologías al servicio de la seguridad pública y su impacto en la privacidad: criterios de ponderación", *Revista Chilena de Derecho y Tecnología*, 5, 2016, 71-2.

La sentencia en comento traza distinciones demasiado gruesas, al tiempo que descansa en un paradigma ya superado de la privacidad (como secreto). Si bien no hay dudas de que el Estado no se encuentra –ciertamente no cuando se trata del control del delito– en el mismo pie que un tercero particular (como los diarios que captaban imágenes de mujeres en playas, aduciendo que ellas se encontraban en espacios públicos), su posición está lejos de conferirle carta blanca a las actividades de monitoreo y vigilancia estatal, sobre todo si estas se construyen sobre la base de analogías y atribuciones genéricas.

Como resultado de ese recurso, y en parte a propósito de la discusión que las iniciativas en comento suscitaron, el Consejo para la Transparencia (CPLT) –advirtiendo el vacío en que operaban las municipalidades– emitió una serie de recomendaciones que buscan acotar el ejercicio de las actividades de vigilancia.[95] En términos generales, se trata de recomendaciones tributarias de la sentencia de la Corte Suprema. Al igual que esta, el CPLT entiende que el artículo 4 letra j) de la LOCM basta para conferir legalidad a la actividad de vigilancia de las municipalidades.[96] Ahora bien, a pesar de este reconocimiento genérico de atribuciones legales, el CPLT avanza al establecimiento de regulaciones a la captación y tratamiento de las imágenes, en mayor sintonía con el derecho internacional de los derechos humanos. En especial, recomienda límites respecto al uso de las imágenes, responsabilidad y seguridad por las mismas, disposición y control de los datos y acceso de las personas a las imágenes –entre otros derechos–.[97]

Volvamos a los estándares enunciados en la sección anterior. De conformidad a estos, las actividades estatales que se entrometen en la privacidad de las personas deben estar precisamente establecidas en una ley accesible a ellas; perseguir un fin legítimo; y ser necesarias (proporcionales y sin afectar la esencia del derecho) en una sociedad democrática. ¿Cuál es el caso de las municipalidades que se han embarcado, hasta ahora, en estas actividades de vigilancia? Para la preparación de este capítulo se presentaron solicitudes de acceso a la información ante los municipios de Las Condes, Lo Barnechea y Providencia. Todos municipios que han anunciado e implementado sus sistemas de vigilancia. Se solicitó, principalmente, identificación

95 Consejo para la Transparencia, *Formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades conforme a las disposiciones de la Ley N° 19.628*, Oficio N° 002309, 6 de marzo de 2017.

96 Ibíd, párr. 4. Tampoco se preocupó de examinar la especificidad de las atribuciones ni proporcionalidad de las medidas en un par de amparos de acceso a la información que ha tenido ocasión de resolver. Como se dirá, esto se debe, en parte importante, a las funciones que desempeña el CPLT cuando resuelve esos amparos.

97 Ibíd, párrs. 5-8.

de las fuentes normativas conforme a las que implementaban sus sistemas de cámaras y tratamiento de datos.[98] De manera más o menos concurrente, los municipios afirmaron que sus facultades legales se encuentran contenidas en: (i) el artículo 4 letra j) de la LOCM; (ii) la sentencia de la Corte Suprema antes señalada; y (iii) las recomendaciones del CPLT.[99]

Desde luego, y como se ha indicado en la sección anterior, las actividades de intromisión en la vida privada de las personas demandan algo más que una atribución genérica, como las funciones conferidas "en el ámbito de la seguridad pública a nivel comunal". En efecto, las intromisiones deben estar establecidas expresamente (y no solo ser inferidas a partir de facultades generales) en la ley, ser específicas y ofrecer mecanismos adecuados de resguardo contra arbitrariedades de las autoridades involucradas. El mismo Tribunal Constitucional ha advertido en un par de ocasiones, de hecho, que la atribución discrecional a órganos del Estado para recabar datos y antecedentes, sin limitación, afecta el derecho a la privacidad.[100] Tan problemática es, sin embargo, la falta de definición respecto a los contornos de la facultad municipal, que, por lo menos en el caso del municipio de Las Condes, este decidió mover sus cámaras de los espacios públicos a condominios privados provocando una nueva discusión –y un nuevo recurso de protección cuya decisión permanecía pendiente al cierre de la edición de este capítulo–.

En lo que respecta a la sentencia de la Corte Suprema, debe anotarse que ella, en el mejor de los casos, gobierna la suerte de los municipios de Las Condes y Lo Barnechea. Pero carece de obligatoriedad para los demás municipios u órganos que se embarquen en estas actividades. Por lo demás, y frente a la ausencia de un órgano independiente de control –como se dirá enseguida–, ¿cómo se controlará que lo que la sentencia ordena en tanto régimen de autorización sea respetado? Ya es cuestionable que sea el mismo municipio el que debe cuidar que esto sea así –misma orientación que ofrece el CPLT, no obstante solicita conocer las innovaciones que

98 Las respuestas se encuentran contenidas en Municipalidad de Lo Barnechea, Oficio Adm. Municipal N° 186/2017, 20 de abril de 2017; Municipalidad de Las Condes, Oficio N° 334, 5 de mayo de 2017; Municipalidad de Providencia, Oficio N° 3764, 16 de mayo de 2017.

99 Aunque dichas recomendaciones fueron mencionadas solo por la Municipalidad de Providencia.

100 Tribunal Constitucional, Sentencia Rol 389, 28 de octubre de 2003. El Tribunal, adecuadamente, advierte que resulta crucial en su decisión la falta de resguardo para las personas, así como de elementos que orienten la actuación estatal:
sin trazar en la ley las pautas o parámetros, objetivos y controlables, que garanticen que el órgano administrativo pertinente se ha circunscrito a ellos, asumiendo la responsabilidad consecuente cuando los ha transgredido (considerando 25).

las municipalidades ejecuten al respecto–. ¿Retiene jurisdicción la Corte Suprema con respecto al cumplimiento de estas directrices? Discutible, ¿por cuánto tiempo, bajo qué condiciones? Lo más probable es que las infracciones al ya deficiente régimen de autorización, si no se reclaman frente al propio agente municipal, deban alegarse por medio de un nuevo recurso de protección.[101]

¿Qué ocurre con las recomendaciones del CPLT? ¿Son suficientes a este respecto? Tampoco. El problema de las recomendaciones es, precisamente, que se trata de recomendaciones. Sin ir más lejos, en el oficio de respuestas de la Municipalidad de Providencia – las municipalidades de Las Condes y Lo Barnechea simplemente prescinden de ellas– se indicó que "se debe tener en consideración" esas recomendaciones. Son, por lo tanto, insuficientes para satisfacer los estándares de legalidad (en tanto obligatoriedad) desarrollados por el derecho internacional. De conformidad a estos estándares, como se ha indicado, la satisfacción de la legalidad no implica solo la posibilidad de poder apuntar a disposiciones legales que, de algún modo –como ocurre con la LOCM–, permitan inferir competencias estatales. Además, deben proveer medidas suficientes de salvaguarda y resguardo frente a los abusos de la autoridad, medidas que una simple recomendación –una suerte de recopilación de buenas prácticas– está lejos de alcanzar (máxime cuando el órgano de control dista de ser un órgano independiente, sino que es el propio municipio). Por otra parte, las recomendaciones, al reconocer competencias genéricas a las municipalidades, incurren en la misma falta de escrutinio de las atribuciones específicas que deben permitir a los órganos del Estado entrometerse en los que el mismo CPLT denomina como datos personales (y que, en virtud de su tratamiento, como se dirá luego, devienen en sensibles).

Resulta preocupante advertir la libertad con que se sienten (y actúan) las municipalidades en cuestión. Ninguna de las respuestas entregadas ante las consultas sobre el marco normativo que gobierna sus actividades de vigilancia incluyó la Ley 19.628.[102] Si bien esta ley es

101 Si el régimen legal se encuentra establecido, además, en los términos que la propia Corte Suprema ha trazado, entonces deberá demostrarse que la ilegalidad en que incurre la municipalidad arranca no del incumplimiento de obligaciones legales, sino de la falta de adecuación a un régimen de autorización establecido en otra sentencia de protección.

102 Los municipios, en cambio, si han recurrido a la Ley 19.628 a efectos de negar la entrega de información a particulares que han solicitado segmentos de grabaciones. En cualquier caso, se trata de un argumento a mayor abundamiento. Para los municipios la principal razón para negar esa información la constituye el posible entorpecimiento que podría causarse a la prevención, investigación y persecución de crímenes y delitos. En el caso de la Municipalidad de Lo Barnechea, sin embargo, el CPLT acertadamente rechazó la excusa, advirtiendo que aquella no había aportado antecedente alguno que demostrara cómo ello acontecería. Consejo para la Transparencia, Decisión Amparo Rol C2828-15, 28 de enero de 2016, considerando 6.

deficiente en términos de la protección de datos personales, como ya se ha indicado, ofrece algunas alternativas de control. En primer lugar, dispone que se entenderá por datos personales "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables" (artículo 2 letra f). El profesor Anguita, comentando esta definición, indica que son datos personales "el nombre, edad, sexo, estado civil, profesión, domicilio, números de teléfonos".[103] ¿Se incluye la imagen? En la medida que las cámaras captan la figura de personas "identificadas o identificables", se trata, no cabe duda, de lo que la ley denomina "datos".[104]

Sin embargo, la misma ley confiere a los organismos públicos una facultad genérica para crear bases de datos respecto a materias de su competencia (artículo 20), cláusulas que los propios órganos en cuestión –como vimos a propósito de las respuestas municipales– y los de control –a propósito de la sentencia de la Corte Suprema o algunas decisiones del CPLT–[105] han leído con bastante bondad, prestando escasa atención a los derechos de privacidad involucrados y a las exigencias que ello gatilla. Volvemos así a los problemas ya detectados. La normativa a la que echan mano las municipalidades para justificar sus competencias carece de la especificidad requerida por los estándares del derecho internacional de los derechos humanos. Este es un problema grave.

A mayor abundamiento, persisten dudas –todavía al amparo de la Ley 19.628– sobre el tratamiento que las municipalidades hacen de los datos recopilados. Primero, porque las municipalidades carecen de autorizaciones normativas específicas, como lo exige la ley, para proceder al tratamiento de los datos. Como se ha dicho antes, el tratamiento de datos recopilados "a granel" permite a los organismos públicos reconstruir perfiles y avanzar hacia la identificación de información que ya no solo es personal, sino que, en los términos de la Ley 19.628, sensible:

103 Anguita, *La Protección de datos personales*, *op. cit*., pp.294-5.

104 Así lo entiende Luis Cordero, aunque comentando las cámaras de videovigilancia policial. Cordero, "Videovigilancia e intervención administrativa", op. cit., p. 20. También lo entendió así el CPLT en su oficio de recomendaciones a las municipalidades. Consejo para la Transparencia, *Formula recomendaciones respecto a la instalación de dispositivos de videovigilancia*, op. cit., párrs. 2 y 3.

105 Más abajo se indica que, en el caso del CPLT, es su propia posición orgánica la que conspira contra una mayor intervención.

tal es el caso de los hábitos (artículo 2 letra g).[106] Y tratándose de datos de este tipo, las exigencias de legalidad y especificidad debieran ser aún más estrictas, como lo son en la ley que principia prohibiendo el tratamiento de esta clase de datos.[107]

Finalmente, y en contraposición de los estándares del derecho internacional, Chile carece de un organismo especializado de supervigilancia del respeto de la privacidad de las personas. Ya se ha visto que tanto en la sentencia de la Corte Suprema, como en las recomendaciones del CPLT, de existir un órgano de control debe ser la propia municipalidad. Siguiendo la sentencia –recuérdese que, tanto para los municipios de Lo Barnechea como de Las Condes, las recomendaciones no figuran en su marco normativo–, las municipalidades indican que, transcurrido 30 días, la información se sobrescribe (en el caso de Lo Barnechea) o es destruida (en el caso de Las Condes).[108] Pero una cosa es lo que las municipalidades dicen que hacen, otra distinta –y esta es la garantía del derecho internacional– es que exista una normativa y un órgano independiente de supervisión que se encarga de cuidar que ello sea efectivamente así.

Es cierto que la Ley 20.285, sobre Acceso a la Información Pública, dispone que será misión del CPLT "velar por el adecuado cumplimiento de la ley N 19.628" (artículo 33 letra m) –en cuyo ejercicio dictó las recomendaciones antes identificadas–. Sin embargo, la actividad del CPLT a este respecto se juega –y esto no es responsabilidad del CPLT, precisamente– en la protección de datos personales en poder de organismos públicos y respecto de los que otros particulares requieran acceso. Fuera de las recomendaciones, que responden a situaciones más bien acotadas, el CPLT vela por el cumplimiento adecuado de la ley sobre datos personales en un contexto de acceso a la información y transparencia, lo que inevitablemente altera su acercamiento a las cuestiones

106 Los datos sensibles, dispone el precepto en cuestión, son:
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.
Desde luego que el concepto mismo de datos sensibles puede leerse bajo el paradigma de privacidad (o intimidad, como dispone el precepto recién transcrito) como secreto, entendido como equivalente a espacio cerrado. Ello lo haría irrelevante para la discusión que acá se plantea.

107 En la Ley 19.628, el tratamiento de datos sensibles se encuentra prohibido, a menos que una ley, el consentimiento del titular o el otorgamiento de beneficios de salud así lo permitan (artículo 10). No hay duda que la exigencia de legalidad debe interpretarse en sentido estricto, y no con la amplitud en que se ha leído la atribución genérica relativa al tratamiento de datos personales del artículo 20.

108 Salvo que las imágenes hayan detectado la ocurrencia de algún delito, en cuyo caso son entregadas a los "órganos judiciales competentes" –aunque probablemente está pensando en el Ministerio Público–. Municipalidad de Las Condes, Oficio N° 334.

sobre privacidad.[109] De este modo, no es un organismo adecuado de conformidad a los estándares del derecho internacional de los derechos humanos para la defensa de datos personales frente al Estado.[110]

CONCLUSIONES

El derecho a la privacidad protege a las personas también en los espacios públicos. Sobre esto no hay duda en el derecho internacional de los derechos humanos y ha sido la conclusión del desarrollo sostenido de la jurisprudencia constitucional nacional (y comparada). De conformidad a los estándares del derecho internacional de los derechos humanos, sin embargo, la privacidad –como los demás derechos– no es absoluta. Puede estar sujeta a regulaciones que permitan actividades de intromisión estatal.

Estas regulaciones son admisibles solo en la medida que se encuentren establecidas por ley, estén justificadas en una sociedad democrática y se sometan a supervisión de un órgano independiente al que se le encomiende la protección de los derechos de las personas –con independencia del sistema de tribunales donde podrá buscarse reparación a las afectaciones–. El Estado de Chile, como se ha dicho en este capítulo, se encuentra al debe en esta materia. Si bien es cierto que la prevención y persecución del delito son fines legítimos que el Estado puede trazarse, esos propósitos no se pueden conseguir a cualquier costo.[111]

Las hipótesis de intromisión en la vida privada de las personas deben encontrarse establecidas en una ley, y sus condiciones de procedencia ser específicas y acotadas. Nada de eso ocurre en Chile. Las

109 Del mismo modo, si vale la pena el parangón, en que la Relatoría Especial para la Libertad de Expresión procedió a acercarse al estudio de las acciones de *habeas data* desde la óptica de la transparencia y la rendición de cuentas (n. 31). Rajevic ha identificado, también, esa 'tensión' en que se debe mover el CPLT al momento de tener que resolver solicitudes de acceso a la información. Enrique Rajevic, "Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación", *Expansiva: en foco*, p. 162, 2010.

110 Así, el Consejo para la Transparencia, en una decisión de amparo citada antes para mostrar cómo ha recogido la tesis de privacidad en el espacio público, rechazó una solicitud de información presentada por un particular respecto a un bloque de imágenes captadas por el sistema de globos aerostáticos de la Municipalidad de Las Condes. Para hacerlo, presentó importantes argumentos relativos a los estándares que el derecho internacional de los derechos humanos sobre privacidad, incluida la ausencia de normas lo suficientemente determinadas y específicas para permitir el acceso de terceras personas. Lo cierto es que esas normas tampoco permiten –ni de manera determinada ni específica– las facultades municipales para proceder a la captación y tratamiento de la información. Sin embargo, y a riesgo de ser majadero, debe insistirse en que el consejo no tutela vía amparos, porque no puede hacerlo, las captaciones de datos realizadas por órganos públicos ni su sustento (o la falta de este) normativo. Y eso es lo que lo hace insuficiente. Consejo para la Transparencia, Decisión Amparo Rol C2493-15.

111 Comisión IDH, *Informe sobre Seguridad Ciudadana y Derechos Humanos*, OEA/Ser.L/V/II.Doc. 57, 31 de diciembre de 2009, párrs. 169-81.

municipalidades han procedido a instalar cámaras de vigilancia en globos y drones que captan información "a granel" –probablemente una de las situaciones más preocupantes para el derecho internacional–, a partir de lecturas descuidadas de sus propias atribuciones. Chile tampoco cuenta con una instancia de protección de los datos personales de ciudadanos y ciudadanas. Las instancias (como los tribunales y el CPLT) que hoy tienen algo que decir, además, han sido igualmente benevolentes con las municipalidades a la hora de leer sus competencias.

Debe advertirse que las deudas del Estado de Chile en materia de vigilancia pública van más allá de la situación específica de las actividades de monitoreo municipal. Como se ha indicado a lo largo de este capítulo, parte importante de la preocupación que evidencia el estado actual de las regulaciones en Chile dice relación, precisamente, con la falta de observación de los estándares del derecho internacional de los derechos humanos. No se trata, entonces, de exigir la eliminación *a todo evento* de las actividades de vigilancia estatal, sino de someterlas a regulaciones estrictas cuando puedan afectar el ejercicio de derechos como la privacidad y otros (libertad de movimiento, libertad de expresión y reunión, por ejemplo) que se encuentran en íntima relación con ella.

En ese sentido, debe anotarse que el Gobierno de la Presidenta Bachelet ha enviado recientemente un proyecto de ley que actualiza la Ley 19.628 (sobre protección y tratamiento de datos personales y crea la agencia de Protección de Datos Personales).[112] Desde luego que no basta con la actualización de la legislación, sino que –lo que se viene acá señalando– de su adecuación a los estándares expuestos en este capítulo. Si bien el proyecto se presenta como una oportunidad para abordar sistemáticamente la regulación general o marco de las actividades de monitoreo y vigilancia de espacios públicos, el mismo guarda silencio al respecto. En lo que concierne estrictamente a este capítulo, ello es especialmente problemático si se anota que el proyecto insiste en conferir una autorización genérica a los organismos públicos para el tratamiento de datos que diga relación con "el cumplimiento de sus funciones legales" (artículo 20). Todavía más si se agrega que el proyecto dispone que el consentimiento del titular no será necesario para el tratamiento de datos cuando así lo autorice una ley (artículo 12 inciso 1) o la captación se haya realizado en fuentes de acceso público (artículo 13 letra a). En conjunto con la lectura amplísima que se ha hecho de la legislación vigente –incluso extendiendo autorizaciones por analogía, como en el caso de las municipalidades–, este proyecto, a este respecto, deja las cosas tal como están.[113]

112 Boletín N° 11.144-07.

113 O incluso peor. Esto, porque el proyecto deja el tratamiento de datos sensibles al margen de la necesidad de consentimiento de las personas cuando se trate de datos que el titular haya "hecho manifiestamente públicos" (artículo 16 letra a).

RECOMENDACIONES

En este contexto, este capítulo concluye ofreciendo las siguientes recomendaciones:

1. La ausencia de regulaciones específicas en materia de vigilancia y monitoreo, no es sinónimo de autorización. Los municipios y otras entidades estatales debieran abstenerse de seguir implementando sus sistemas de vigilancia a través de cámaras situadas en globos y drones por ser actos ilegales y afectar desproporcionadamente la privacidad de las personas.
2. Se recomienda al Estado adecuar la legislación nacional en materia de privacidad a los estándares del derecho internacional de los derechos humanos, incluidas las actividades de vigilancia y monitoreo.
3. Es de suma importancia advertir que la atribución genérica de facultades intrusivas no satisface los estándares del derecho internacional. La regulación estricta de las actividades de intromisión del Estado, pasa, en primer término, por la actualización de la legislación en materia de protección de datos personales. El proyecto identificado antes, en los términos en que hoy se encuentra, no satisface esta exigencia.
4. Por eso mismo, es importante entender que el proyecto de ley debiera verse como una oportunidad no solo para que el Estado de Chile pueda alinearse con los estándares del derecho internacional a los que voluntariamente se ha sometido, sino que, también, para abrir espacios significativos a la intervención de la sociedad civil. Chile cuenta con organizaciones de la sociedad civil altamente capacitadas –como el caso de Derechos Digitales y Datos Protegidos– cuyo trabajo ha sido reconocido en la región. Su intervención debiera ser significativa.
5. El Estado también tiene una responsabilidad adicional en el contexto de la discusión de las reformas anunciadas. Recientemente, el informe del Relator Especial para el derecho a la privacidad, ha indicado que los Estados –y Chile no ha sido la excepción– han preferido jugar "la carta del miedo", trabando así una oposición de suma cero entre privacidad, de una parte, y seguridad, de otra.[114] Anotando el contexto y oportunidad que abre el envío del proyecto de ley antes identificado, se recomienda al Estado no establecer oposiciones entre privacidad, de una parte, y seguridad, de otra, cotejando adecuadamente los distintos intereses y derechos en juego.

114 Consejo de Derechos Humanos, *Report of the Special Rapporteur on the right to privacy*, *op. cit*., párr. 42.