Informe legal *Indigenous Surveillance*

Efectos de la vigilancia electrónica sobre los derechos fundamentales de las comunidades mapuche

Autoría:	Este informe fue hecho para el proyecto *Indigenous Surveillance* por el investigador Rodrigo Vargas.
Fecha y lugar de última versión:	04 de agosto del 2019 / www.indigenoussurveillance.net
Versión:	1.0
Derecho de autor:	Esta obra está bajo el Dominio Público, por lo que puedes usarlo y reutilizarlos libremente, reconociendo la autoría del investigador y del proyecto *Indigenous Surveillance*.

I. Preámbulo

En una primera categorización, según el sujeto quien las realiza, la vigilancia puede ser ejercida por agentes del Estado -solos o en coordinación con privados- o pueden ser realizadas en forma íntegra por privados.

En cuanto a sus fines, se ha observado que las actividades de vigilancia se han empleado para la investigación penal de delitos comunes, para la investigación penal de delitos categorizados como terroristas, en el ejercicio de funciones de inteligencia del Estado, en una función de seguridad pública o de prevención de delitos y, finalmente, con fines intimidatorios o disuasivos respecto de comunidades u organizaciones.

También, estas medidas se pueden clasificar en torno a la intrusividad o el alcance que tengan, que iría desde medidas que funcionan de manera pasiva en lugares públicos, como puede ser el caso de las cámaras de vigilancia fijas instaladas en carreteras, hasta medidas de vigilancia activa, de gran alcance, y que afecten espacios o comunicaciones privadas, como puede ser el caso de la operación de drones con cámaras de alta resolución sobre propiedad privada, o la interceptación de comunicaciones privadas.

Por otro lado, respecto a la legalidad de dichas medidas, se pueden ordenar desde aquellas que, respecto a casos legítimos, están bien reguladas por una ley y que solo se limitan a la intromisión necesaria para obtener un fin legítimo. También está un área intermedia, donde las medidas se aplican en base a fundamentos legales poco claros o excediendo las autorizaciones legales. También hay medidas evidentemente ilegales, ya sea porque incumplen las regulaciones existentes (como es el caso de la utilización de técnicas de reconocimiento facial sin contar con las autorizaciones requeridas por la ley de protección de datos personales), o porque se comenten delitos al utilizar estas técnicas (como podría ser el caso de la utilización de malware de vigilancia, que podría constituir un delito informático).

Finalmente, todas estas técnicas de vigilancia pueden afectar derechos fundamentales de las personas, reconocidos en el derecho interno (en la Constitución Política de la República) y en el derecho internacional de los Derechos Humanos (en la Declaración Universal de Derechos Humanos, la Convención Americana de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, entre otros).

A saber, se pueden afectar derechos tales como el derecho a la privacidad y la honra, a la inviolabilidad del hogar y las comunicaciones, a la protección de datos personales, a la libertad personal y seguridad, a la libertad de expresión e información, a la asociación y reunión, y a la igualdad ante la ley y a la no discriminación arbitraria.

II. El caso mapuche

Las comunidades mapuche se han visto especialmente expuestas a la vulneración de sus derechos en comparación al resto de la población del país. Los motivos son varios desde la perspectiva de las tecnologías de vigilancia. En primer lugar, en la medida que estas técnicas de vigilancia han sido desplegadas de manera especialmente sistemática en su contra con la excusa del combate al

terrorismo, los territorios que el Estado chileno considera "rojos" forman una suerte de frontera para la experimentación con nuevas técnicas de vigilancia.[1]

Por otro lado, si bien varias de las técnicas de vigilancia están reguladas por la ley común, como es el caso de la interceptación de comunicaciones, regulada en el Código Procesal Penal, en el caso de su aplicación en territorios mapuche se registra una tendencia sistemática a ser aplicada en base a la legislación antiterrorista, tanto respecto de la persecución de delitos categorizados como terroristas, como también por parte de los servicios de inteligencia del Estado.

El problema viene dado por el hecho de que las leyes antiterroristas se han aplicado de manera sesgada en contra de comuneros y defensores mapuche, pese a la virtual inexistencia de actividades terroristas en la zona, conforme a la falta de sentencias condenatorias en materia penal. En su investigación sobre la jurisprudencia en casos de delitos terroristas, la investigadora Myrna Villegas afirma que "si a los nueve condenados post reforma procesal penal le restamos las siete condenas que fueron anuladas por la CIDH en el caso Norín Catrimán vs. Chile, coincidimos en la existencia de solo dos sentencias condenatorias, pero asociadas a una misma persona: un informante de la policía en casos de terrorismo en la Araucanía".[2] Como concluye[3] la autora:

> "Cruzando el río Bío Bío y hacia el sur lo que se observa es la repetición de algunos imputados en varias causas, así como de personas pertenecientes a las mismas familias. Da la impresión de que existe una tendencia a perseguir por esta clase de delitos y otros asociados al conflicto territorial a quienes se erigen como cabezas de los movimientos o comunidades, judicializando a autoridades ancestrales".

Además de los problemas propios de la aplicación de medidas de vigilancia, se suman los problemas de carácter político y jurídico propios de su realización en el marco de las leyes antiterroristas chilenas. Como señaló el Relator Especial de las Naciones Unidas sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo en su informe sobre la visita realizada a Chile en 2013, "partes de esta legislación (La ley 18.314) aún no están en conformidad con las normas internacionales de derechos humanos y una serie de inconsistencias existen entre la ley y la garantía de respeto al principio de legalidad y el derecho al debido proceso. El Relator Especial considera que el uso de la legislación antiterrorista en contra de los reclamantes de tierras mapuche es parte del problema, y no parte de la solución. Se ha convertido en contraproducente para una solución pacífica de la cuestión mapuche y debe cesar".[4]

Además de la utilización de las tecnologías de vigilancia en el marco de la ley Antiterrorista con fines de persecución de delitos terroristas, también se ha detectado la utilización de la Ley 19.974 sobre el sistema de Inteligencia del Estado, que contiene una mayor variedad de posibilidades de vigilancia, y que si bien en su diseño presenta mayores controles de legalidad, en la práctica es más susceptible de su aplicación abusiva, en la medida que las órdenes judiciales que autorizan su aplicación son de carácter reservado. La información obtenida a través de medidas de vigilancia con fines de inteligencia a menudo es utilizada en investigaciones penales. Este fue el caso de la denominada Operación Huracán, que es uno de los casos paradigmáticos de los abusos contra los derechos fundamentales que se pueden cometer en nombre de la vigilancia contra el terrorismo.

---

[1] El equipamiento de Carabineros para combatir la violencia rural en la macrozona sur. Emol. 28 de junio 2018 https://www.emol.com/noticias/Nacional/2018/06/28/911531/El-equipamiento-de-Carabineros-para-combatir-la-violencia-rural-en-la-macrozona-sur.html

[2] Villegas, Myrna (2018). Tratamiento jurisprudencial del terrorismo en Chile. En: Política Criminal, Vol. 13, N.º 25, p. 508.

[3] Íbid., pp. 510-511.

[4] Consejo de Derechos Humanos de las Naciones Unidas (2014). Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Ben Emmerson. Adición. Misión a Chile. A/HRC/25/59/Add.2. Párrafo 85, p. 19.

Además de los potenciales sesgos que puedan tener los agentes del Estado en la aplicación de la ley y que han sido denunciados en forma sistemática,[5] las comunidades mapuche han resultado especialmente perfiladas, por ejemplo, en la medida que han sido perseguidos a través de instrumentos legales asociados a la persecución del terrorismo a nivel de la inteligencia estatal, cuando se trata de casos de actividades de reivindicación política legítima, o solo cuando se trata de delitos comunes. O incluso, potencialmente pueden verse afectados por sesgos en la tecnología misma, como puede ser el caso de las fallas en reconocimiento facial, que tiende a tener un mayor índice de falsos positivos cuando se aplica en tiempo real, y respecto de mujeres y de personas de color u origen étnico distinto a los hombres blancos que desarrollaron estas tecnologías.

La utilización de estas técnicas de vigilancia, en la mayoría de estos casos afecta de manera evidente a los derechos a la privacidad y a la inviolabilidad de las comunicaciones privadas. Así, por ejemplo, se ve en la sentencia de la Corte Interamericana de Derechos Humanos en el caso "Escher y otros contra Brasil" del 2009, que trata sobre interceptación y divulgación ilegal de comunicaciones telefónicas por parte de Agentes del Estado. En este caso, se parte desde un concepto bastante simple del derecho a la privacidad, entendido como la facultad de cada persona de poder mantener en secreto determinadas acciones o informaciones respecto de otros. En términos de la Corte Intermericana "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública".[6]

En este caso, la Policía Militar del estado de Paraná, interceptó y monitoreó conversaciones telefónicas de miembros de organizaciones sociales y políticas asociadas al movimiento de trabajadores sin tierra. Esta interceptación y monitoreo, si bien fueron hechos a través de una orden judicial, fueron divulgados a medios de comunicación de alcance regional y nacional de manera irregular por el Secretario de Seguridad Pública. Además, si bien se obtuvo la autorización para la interceptación de las comunicaciones telefónicas mediante una orden judicial, esta fue solicitada por funcionarios policiales militares incompetentes para investigar los supuestos delitos de carácter civil que perseguían, y fueron concedidos en una resolución sin fundamentos por parte del funcionario judicial encargado.

En este caso, se alegó una infracción a los derechos contenidos en el artículo 11 de la Convención Interamericana de Derechos Humanos,[7] en particular el derecho a la vida privada, la honra, y el secreto de las comunicaciones privadas, y al derecho a la libertad de asociación contenido en el artículo 16 de la convención,[8] entre otros.

---

[5] Amnistía Internacional denunció que la ley antiterrorista en Chile criminaliza a la comunidad mapuche. France 24. 10 de agosto 2018 https://www.france24.com/es/20180809-amnistia-ley-antiterrorista-mapuche-chile

[6] Corte Interamericana de Derechos Humanos (2009), Caso Escher y otros v. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200. Párrafo 113, p. 34.

[7] Artículo 11. Protección de la Honra y de la Dignidad
1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. 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.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

[8] Artículo 16. Libertad de Asociación
1. Todas las personas tienen derecho a asociarse libremente con fines ideológicos, religiosos, políticos, económicos, laborales, sociales, culturales, deportivos o de cualquiera otra índole.
2. El ejercicio de tal derecho sólo puede estar sujeto a las restricciones previstas por la ley que sean necesarias en una sociedad democrática, en interés de la seguridad nacional, de la seguridad o del orden públicos, o para proteger la salud o la moral públicas o los derechos y libertades de los demás.
3. Lo dispuesto en este artículo no impide la imposición de restricciones legales, y aun la privación del ejercicio del derecho de asociación, a los miembros de las fuerzas armadas y de la policía.

En la resolución del caso, la Corte Interamericana consideró que el derecho a la privacidad (entendido en este caso simplemente como el derecho a mantener secreto el contenido de sus comunicaciones) se puede afectar cuando las actividades de los agentes estatales sean ilegítimas, para lo cual desarrolla un test de tres etapas,[9] a saber:

> "(El derecho a la vida privada) puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello,
> (1) deben estar previstas en ley,
> (2) perseguir un fin legítimo y
> (3) ser necesarias en una sociedad democrática".

En la resolución del caso Escher y otros contra Brasil, el análisis se limitó a declarar la ilegalidad de las medidas de interceptación de comunicaciones y su posterior divulgación, restando el análisis sobre los fines y la necesidad y proporcionalidad de las mismas. Asimismo, en el caso de la aplicación de tecnologías de vigilancia en las regiones del "conflicto mapuche", podremos ver muchos casos en que bastará con comprobar la ilegalidad de la aplicación de determinadas medidas para concluir que son afectaciones ilegítimas a derechos fundamentales.

Ahora bien, como veremos a continuación, las tecnologías de vigilancia pueden afectar una serie de derechos fundamentales aun cuando la vigilancia se realice de manera conforme a las leyes vigentes. Además del derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas, se han detectado potenciales afectaciones a derechos tales como: el derecho a la igualdad y no discriminación arbitraria, el derecho a la libertad individual y la seguridad, el derecho al debido proceso y a defensa, el derecho a la libertad de expresión, el derecho a asociación, entre otros.

En la jurisprudencia chilena, también ha habido casos relevantes que analizan la interacción entre el despliegue de tecnologías de vigilancia por parte del Estado y el derecho a la privacidad. Así, por ejemplo, en el caso conocido como globos de vigilancia,[10] se realizó un análisis sobre la legalidad y constitucionalidad de la instalación de cámaras de alta resolución en comunas de sectores de ingresos elevados de la ciudad de Santiago, las que tenían la capacidad de moverse y de captar imágenes de lugares públicos y privados, incluyendo el interior de viviendas.

En este caso, la Corte Suprema rechazó finalmente la acción presentada por particulares en asociación con grupos de la sociedad civil para evitar el despliegue de estos globos de vigilancia, estableciendo una serie de condiciones para la operación de estas tecnologías, lo que supone que se da por hecho que este tipo de tecnologías afectará la privacidad, y se acepta esta vulneración en favor del derecho a la seguridad pública.[11] Respecto al conflicto jurídico del caso, del análisis de la sentencia[12] de la Corte se desprende que:

> "[E]l problema no es la existencia de medios tecnológicos que puedan afectar la privacidad de las personas, sino el uso inadecuado de medios que persiguen fines lícitos, que son «vigilar lo que ocurre en la vía pública para avisar a las autoridades policiales de la comisión de un delito flagrante o la ocurrencia de un accidente de tránsito o peatonal para darles aviso a las mismas autoridades y entidades de salud, como la de aportar un elemento probatorio en un proceso penal o infraccional»".

---

[9] Corte Interamericana de Derechos Humanos (2009), Op. Cit. Párrafo 116, p. 35.
[10] Corte Suprema de Chile (2016). "Soffge y otros contra Ilustre Municipalidad de Las Condes y otro". Causa rol 18.481-2016. Sentencia en recurso de Apelación a Acción de Protección.
[11] Ramírez Hermosilla, Tomás (2016). Nuevas tecnologías al servicio de la seguridad pública y su impacto en la privacidad: criterios de ponderación. En: Revista Chilena de Derecho y Tecnología, vol. 5, N.º 1, p. 72
[12] Corte Suprema de Chile (2016). "Soffge y otros contra Ilustre Municipalidad de Las Condes y otro". Sentencia en recurso de Apelación a Acción de Protección.

En la práctica, el deficiente control sobre la utilización de estas tecnologías ha supuesto en algunos casos que no pasen siquiera los controles de legalidad que harían legítimo su funcionamiento. En el caso de la denominada Operación Huracán, por ejemplo, el Instituto Nacional de Derechos Humanos (INDH) interpuso recursos de amparo, en las causas Rol 51 y 53 de 2018 de la Corte de Apelaciones de Temuco, en favor de un grupo de alcaldes y un funcionario municipal, todos miembros de la Asociación de Municipalidades con Alcaldes Mapuche (AMCAM) en contra de Carabineros de la IX zona Araucanía, por la interceptación de comunicaciones telefónicas amparadas en la Ley de Inteligencia.

En los fallos de ambas acciones judiciales, la Corte de Apelaciones de Temuco determinó que dichas interceptaciones serían legales en la medida que la decisión de ordenar dichas medidas "fue librada por autoridad competente, en ejercicio de sus atribuciones y dentro de las facultades que le confieren la Constitución y las leyes" (considerando quinto). Añade que la declaración de legalidad de las medidas de investigación de la ley de inteligencia procede, sin perjuicio de que con resultado de investigaciones penales o administrativas posteriores se determine que los antecedentes aportados para otorgar dichas medidas sean falsos, toda vez que es el Ministerio Público quien tendría la facultad de dirigir la investigación penal.[13] Dicha conclusión resulta totalmente antojadiza, como se verá cuando analicemos la forma en que los mecanismos de interceptación de comunicaciones han sido utilizados en la práctica, en especial en el caso Operación Huracán, pero también en otros casos anteriores.

Del mismo modo, las tecnologías de televigilancia en la denominada zona roja, se ha visto que estos operan con escasos controles prácticos, lo que ha supuesto que en varios casos se haya comprobado su utilización con fines distintos a los que autorizaría la ley (incluso si obviamos que dicha autorización legal para su operación no es del todo clara), comprobándose casos en que se han utilizado con fines de hostigamiento y seguimiento de actividades de carácter político, o incluso abiertamente para la invasión de la privacidad de personas.

En consecuencia, consideramos necesario realizar un análisis de fondo sobre la finalidad y necesidad de las medidas, de modo de describir con mayor claridad la forma en que estas tecnologías pueden vulnerar derechos fundamentales, en especial, de las comunidades mapuche.

En primer lugar, distinguiremos entre dos tipos de técnicas. Por un lado, las técnicas de vigilancia que suponen la observación de la conducta de las personas, o televigilancia; y por otro, las técnicas que suponen la intervención de terceros en las comunicaciones.

III. Televigilancia

En esta categoría, que incluye la instalación de cámaras de vigilancia en espacios públicos o privados, y la operación de vehículos aéreos con la capacidad de capturar imágenes, pudiendo ser estos tripulados (helicópteros, por ejemplo) o no tripulados (drones y globos de vigilancia).

Las bases legales para su operación vienen dadas, principalmente, por las siguientes normativas: la ley orgánica constitucional de Carabineros de Chile N° 18.961 que habilita al organismo para implementar planes de prevención del delito; la norma reglamentaria Orden General N° 996 denominada directiva para los servicios del sistema de vigilancia policial preventiva por cámaras de televisión de Carabineros de Chile; la ley orgánica constitucional de municipalidades N° 18.695 que autoriza a los municipios

[13] Corte de Apelaciones de Temuco (2018). "Recurso de amparo en favor de Vergara Montecinos Mauricio" y "Recurso de amparo en favor de Painequeo Tragnolao Manuel y Otros", causas Rol 51 y 53 del año 2018. Sentencias en recurso de Amparo.

para implementar planes de prevención del delito y el decreto ley 3.607 del año 1981 que autoriza el funcionamiento de agencias privadas de vigilancia.[14]

Pese a esta aparente legalidad de la implementación de sistemas de televigilancia, se ha criticado que esta solo corresponde a una autorización genérica derivada de las facultades de implementación de planes de prevención del delito, reglamentada en virtud de la potestad reglamentaria de Carabineros de Chile, correspondiendo a la Orden General Nº 966. Al tratarse de actividades que pueden restringir derechos fundamentales, están sujetas al principio de reserva legal. Asimismo, se ha criticado que "en estas no existe una descripción de la actividad regulada, sino que simplemente habilitan a los órganos estatales referidos para instalar y monitorear los dispositivos. En ellas no se encuentran claramente establecidos los fines del monitoreo, como tampoco los lugares que pueden ser monitoreados ni el tipo de información que se puede registrar o el tratamiento que debe darse a ésta".[15]

Este vacío en la regulación específica del desarrollo de las actividades de televigilancia fue "solucionado" a través del establecimiento del denominado régimen de autorización por parte de la Corte Suprema en el caso globos de vigilancia, en el cual la corte permitió la operación de este sistema en la medida que el espacio a grabar se limitara al espacio público y a lugares privados abiertos solo en el caso del seguimiento de un hecho ilícito, que un funcionario municipal fiscalizara al menos una vez que no se captaran imágenes de lugares privados, que se eliminaran las grabaciones cada 30 días, estableciendo un proceso para que las personas pudiesen acceder a eventuales grabaciones suyas.[16]

Este régimen de autorización posteriormente sirvió de base al Oficio Nº 002309 del Consejo para la Transparencia,[17] que establece un régimen de control de las actividades de vigilancia por parte de municipalidades, con algún mayor nivel de detalle. Aunque esta regulación es aún más detallada que la de la sentencia de la Corte Suprema, sigue sin ser una regulación de carácter legal, como correspondería por ser actividades que pueden restringir derechos fundamentales.

Los cuestionamientos respecto a la legalidad de las medidas de televigilancia se acentúan en el caso de la implementación de cámaras con tecnología de reconocimiento facial, como ha ocurrido en este caso en las cámaras instaladas en espacios públicos por la municipalidad de Temuco,[18] respecto de las cuales podemos concluir que dada la falta de autorización legal para su instalación, y los efectos que tienen sobre la conducta de las personas, no pueden en ningún caso considerarse como una intrusión legítima sobre los derechos fundamentales de las personas. Las tecnologías de reconocimiento facial han mostrado una serie de problemas en su funcionamiento, en concreto, en la medida que presentan una tasa considerable de falsos positivos, fallas que se acentúan respecto de personas de color y mujeres, en la medida que los sets de imágenes utilizados para entrenar los sistemas de inteligencia artificial que hacen funcionar las tecnologías de reconocimiento tienden a tener mayor presencia de hombres de piel clara.[19] Estos sesgos étnico y de género claramente podrían trasladarse al caso de su aplicación en territorios con mayor porcentaje de población mapuche en Chile, aumentando la

[14] Ramírez Zolezzi, Julio, y Valenzuela Herrera, Pecky (2017). Videovigilancia en el espacio público: el monitoreo de la ciudad como dispositivo del control poblacional. Memoria para optar al grado de licenciado en ciencias jurídicas y sociales. Universidad de Chile, p. 25.
[15] Íbid., pp. 26-27.
[16] Ramírez Hermosilla (2016). Op. Cit., pp. 70-71.
[17] Consejo para la Transparencia (2017). Oficio Nº 002309, formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley Nº 19.628. Disponible en: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2019/01/Recomendaciones-dispositivos-de-vigilancia.pdf
[18] Con instalación de 66 cámaras inician modernización del sistema de televigilancia de Temuco. El Austral. 9 de agosto 2018 https://www.soychile.cl/Temuco/Sociedad/2018/08/09/549476/Con-instalacion-de-66-camaras-inician-modernizacion-del-sistema-de-televigilancia-de-Temuco.aspx
[19] Buolamwini, Joy y Gebru, Timmit (2018). Gender Shades: Intersectional accuracy disparities in commercial gender classification. En: Proceedings of Machine Learning Research, Vol. 81 N.º 1, pp. 2 y 8.

posibilidad de falsos positivos, y teniendo como consecuencia una afectación a derechos tales como el debido proceso, y a la no discriminación arbitraria.

Dado que en la legislación chilena, los datos biométricos, como es el caso de la forma de la cara de una persona, califican dentro de la categoría de datos sensibles para la Ley de Datos Personales, en cuanto se refieren a las características físicas de las personas y, por tanto, "en la medida que es posible relacionar datos biométricos con otros datos (personales o no) y así obtener características únicas, tales como las raciales, étnicas o de otro tipo, que permitirían saber no sólo la identidad de un individuo, sino además aspectos sensibles relacionados a su físico o su estado de salud".[20]

Conforme a la Ley 19.968 de Datos Personales, el tratamiento de los datos sensibles sólo puede realizarse cuando hay autorización legal, consentimiento del titular de los datos, o sean necesarios para el otorgamiento de beneficios de salud al titular de estos. Ninguno de los tres casos se daría respecto a la implementación de tecnología de reconocimiento facial, toda vez que no hay una autorización expresa de la ley, ni consentimiento de los titulares de los datos, sino que probablemente se han implementado en base a la misma autorización legal genérica que se ha utilizado para justificar la implementación de sistemas de televigilancia en Chile, es decir, mediante la Ley Orgánica de Carabineros de Chile y la ley Orgánica de Municipalidades, que otorgan facultades de prevención del delito.[21]

Esta autorización genérica, que ya es discutible para justificar la instalación de cámaras de televigilancia, es aún más insuficiente para justificar el tratamiento de datos sensibles y, en consecuencia, sería una afectación ilícita de derechos fundamentales, en la medida que no pasaría por el test de legalidad, bajo el criterio del caso Escher y otros contra Brasil, sin necesidad de entrar a un análisis sobre su finalidad y necesidad.

Luego del análisis de legalidad de este tipo de medidas, corresponde un análisis respecto a sus fines. En principio, todas estas medidas se han implementado con fines de prevención del delito, tanto en la medida que disuadirían a las personas de cometer delitos al saberse observados, como también en cuanto podrían servir como elementos de prueba en un juicio.

Ahora, respecto a la facultad de disuasión de delitos, este podría considerarse un fin legítimo, incluso cuando hay cuestionamientos respecto a la efectividad de estas medidas, en cuanto muchos delitos, especialmente los violentos, son realizados de forma espontánea, sin pensar en las consecuencias.[22] Pero, aunque aceptáramos que estas medidas de vigilancia tienen la capacidad de prevenir delitos, o que al menos sirven para obtener evidencia para un juicio, también tenemos que aceptar que estas pueden ser utilizadas para fines ilegítimos. Así, por ejemplo, puede haber fines de hostigamiento y seguimiento a actividades políticas, como muestra la evidencia en el caso de las comunidades mapuche. En estos casos, las actividades de vigilancia no quedan cubiertas por las normas legales que autorizarían su funcionamiento, en la medida que las autorizaciones legales, por precarias que sean, solo permiten el desarrollo de actividades de prevención del delito y/o de seguridad pública.

Finalmente, incluso en los casos en que las cámaras se instalan o registran actividades que ocurren en lugares públicos, estas pueden afectar el derecho a la privacidad (y por extensión, otros derechos como el derecho de asociación y el derecho a la libertad de expresión), en la medida que afectarán las

[20] Garrido Iglesias, Romina, y Becker Castellaro, Sebastián (2017). La biometría en Chile y sus riesgos. En: Revista Chilena de Derecho y Tecnología, Vol 6 N.º 1, p. 75.
[21] Ramírez Zolezzi, Julio y Valenzuela Herrera, Pecky (2017). Videovigilancia en el espacio público: el monitoreo de la ciudad como dispositivo del control poblacional. Memoria para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales, pp. 25-26.
[22] Clarke, Roger (2014). The regulation of civilian drones' impacts on behavioural privacy. En: Computer Law & Security Review N.º 30, p. 290.

expectativas de privacidad que pueden tener las personas, sin posibilidad de que estas pudieran optar por no ser sujetos de estas medidas.

Respecto a las expectativas de privacidad en el espacio público, se puede sostener, como lo plantea Slobogin, que se afectaría el "derecho a ser anónimo en público", entendido como la certeza de que al estar en un lugar público, una persona cualquiera tiene expectativas de mantenerse como parte de la masa, como alguien sin nombre ni digno de ser destacado, mientras no haga o diga algo que amerite atención del gobierno, como es el caso de alguna actividad delictual.[23] En términos sencillos "el anonimato en público promueve la libertad de acción y una sociedad abierta. La falta de este promueve conformidad y una sociedad opresiva".[24]

En el caso de los vehículos aéreos no tripulados, estos ofrecen el mayor riesgo de afectar derechos fundamentales, en la medida que posee potencialidades únicas, a saber, sus capacidades aéreas y de movilidad, su menor notoriedad en términos de no ser escuchados o vistos por los sujetos vigilados, y la mayor capacidad de tener equipamiento especializado que expande el ámbito de posibilidades de vigilancia.[25] Como señala Clarke, los drones permiten superar barreras en el alcance de la "línea de visión" que tienen las cámaras fijas en un punto terrestre, permitiendo ángulos de visión nuevos, monitoreo continuo de puntos antes no accesibles, mayor facilidad para el seguimiento de objetivos, entre otros.[26] Asimismo, la posibilidad de los drones de operar en forma subrepticia supone una forma de vigilancia encubierta, que "hace surgir un 'efecto panóptico', en cuanto "la vigilancia visible afecta al comportamiento, incluyendo (deseablemente) comportamientos ilegales, pero también aquellos que sean considerados como indeseables por quienes tienen el poder institucional o de mercado. La vigilancia encubierta, por su parte, da lugar a un efecto 'panóptico': las personas temen que puedan ser sujetos de observación en cualquier momento, y que, por lo tanto, una mayor variedad de comportamientos pueda ser considerado indeseable por quienes tienen el poder. Esto resulta en una forma de autodisciplina y en un efecto intimidatorio sobre un amplio rango de comportamientos, y en la paralización de la libertad de expresión".[27]

Una de las formas en que los sistemas de vigilancia afectan los derechos fundamentales es a través del denominado "efecto intimidatorio" que tiene sobre conductas legítimas de las personas. Es decir, en la medida que se despliegan tecnologías de vigilancia, sean éstas visibles y conocidas por las personas, o que al menos se tenga el temor de ser un potencial sujeto de observación, las personas dejarán de hacer cosas que de otro modo habrían hecho. Esta inhibición de comportamientos no sólo es producto del temor a una sanción legal, sino aún más relevante para el sano ejercicio de individuos y comunidades libres en democracia, "para evitar otros tipos de riesgos, tales como el estigma de ser etiquetados por el Estado como inconformistas, disidentes o criminales, o por un temor más amplio a que la información recopilada pueda ser filtrada o revelada públicamente, con el fin de avergonzarlos o que sea usada con fines perjudiciales por terceros".[28]

Sin embargo, a pesar de la amplia literatura al respecto, hay que tener en consideración que este efecto intimidatorio de la televigilancia ha sido desestimado hasta la fecha por parte de la jurisprudencia nacional, siendo el caso más notorio la sentencia de la Corte Suprema que confirma el fallo de la Corte de Apelaciones de Santiago que permite el vuelo de drones de vigilancia con fines de prevención del

[23] Slobogin, Cristoper (2002). Public privacy: Camera surveillance of public places and the right to anonimity. En: Mississipi Law Journal, Vol. 72, p. 235.
[24] Íbid., p. 236.
[25] Bracken-Roche, Ciara (2016). Domestic drones: the politics of verticality and the surveillance industrial complex. En:, Geographica Helvetica N.º 71, p. 169
[26] Clarke, Roger (2014). Op. Cit., p. 289.
[27] Clarke, Roger (2014), Op. Cit., p. 287.
[28] W. Penney, Jonathon (2016). Chilling Effects: Online Surveillance and Wikipedia Use. En: Berkeley Law Journal, Vol. 31 Issue 1, p. 126-127.

delito por parte de las municipalidades de Las Condes y Lo Barnechea en el año 2017. En esta sentencia se concluye[29] que, pese a que los recurrentes alegaron un efecto inhibitorio en sus conductas realizadas en público, que afectaría sus derechos a la libertad de expresión y reunión, entre otros, no se podría verificar use efecto sobre su conducta, en cuanto:

> "[t]al circunstancia se relativiza con el ejemplo que da la Municipalidad recurrida en cuanto al comportamiento de la ciudadanía en Plaza Italia ante eventos deportivos, lugar en el que pese a la existencia de cámaras de vigilancia, la gente concurre en forma masiva a expresar sus emociones. Por ello y a falta de mayores antecedentes concretos sobre el comportamiento de las personas en lugares públicos con cámaras, se impide adquirir el convencimiento de que las garantías constitucionales en análisis se vean realmente amagadas con la utilización de drones de vigilancia".

Finalmente, un último argumento respecto de los efectos de estas medidas viene dado por la creciente imposibilidad que tienen las personas de escapar de sus efectos. Así, como ya hemos descrito, la instalación de cámaras de televigilancia en dispositivos aéreos no tripulados, que poseen una gran movilidad, autonomía de vuelo, la facultad de acceder a ángulos de visión que no son posibles a nivel del suelo, y además son bastante sigilosos en su actuar, van limitando cada vez más la posibilidad de escapar de sus efectos, al menos en espacios públicos o espacios privados abiertos.

En el caso del empleo de cámaras de reconocimiento facial, el alcance de estas tecnologías, en especial si son utilizadas para el seguimiento en tiempo real de las personas, hace que las personas estén perdiendo su capacidad de escapar al hecho de ser sujetos de la vigilancia. Así, en la medida que se vayan implementando en cada vez más lugares, estas podrían reemplazar la necesidad de pedir una orden judicial para ubicar a una persona en base a la ubicación mediante GPS o por triangulación de la información enviada a antenas de telefonía celular y, en consecuencia, si se implementa de manera masiva, podría terminar creando un mundo en que el gobierno podría seguir los movimientos de una persona en tiempo real.[30]

IV. Interceptación de comunicaciones

En los casos de interceptación de comunicaciones, en las materias relevantes a esta investigación, existen dos mecanismos legales para poder ordenarlas. Por un lado, el sistema de investigación penal, regulado en los artículos 222 a 225 del Código Procesal Penal, y en leyes especiales que se remiten a ésta. Por otro lado, está el sistema de inteligencia del Estado, tratado en la Ley 19.974. Ambos, a su vez, tienen como norma superior en jerarquía al artículo 19 Nº 5 de la Constitución Política de la República, que protege el derecho a la inviolabilidad de las comunicaciones privadas, como un derecho autónomo, en la medida que protege las comunicaciones de la intervención de terceros, sin que sea relevante su contenido.[31]

En el primer caso, la investigación penal mantiene un régimen que ofrece un diseño con bastantes garantías, a saber: se requiere autorización judicial previa, la que deberá basarse en una solicitud del Ministerio Público a un Juez de Garantía, basada en la existencia de sospechas fundadas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de un crimen (esto es, un hecho sancionado con una pena de al menos cinco años y un día de prisión), y que la medida sea imprescindible para la investigación.

---

[29] Corte de Apelaciones de Santiago (2017). "González Carbacho Sergio y Otros contra Iltma. Municipalidad de Las Condes". Causa rol 34.360-2017. Sentencia de recurso de protección, confirmada por la Corte Suprema.
[30] Garvie, Clare, et al (2016). The perpetual line-up. Unregulated police facial recognition in America. Georgetown Law Center on Privacy and Technology, p. 64.
[31] Álvarez Valenzuela, Daniel (2019). La inviolabilidad de las comunicaciones privadas electrónicas. Santiago: LOM Ediciones, p. 65

Dicha orden tiene un plazo de duración de 60 días, renovables por una vez con autorización del juez, no puede afectar las comunicaciones del afectado con su abogado defensor (salvo que existan sospechas fundadas de que el abogado también tenga responsabilidad en los hechos, con autorización expresa del juez), y se debe limitar a las conversaciones relevantes para la investigación. Estas medidas deben ser notificadas al afectado por la interceptación con posterioridad a su realización, y no pueden utilizarse en un proceso penal si no se han obtenido conforme a los requisitos establecidos por la ley.

Este sistema se aplica también en leyes especiales, como es el caso de la Ley 20.000 (Ley de drogas) y la ley 18.314 (Ley antiterrorista), con ligeras variaciones. Así, en la ley de drogas, los requisitos para la identificación del afectado por la interceptación telefónica son más flexibles, exigiéndose solo circunstancias que permiten individualizarlo o determinar su identidad. En el caso de la ley antiterrorista, estas medidas no pueden afectar a una serie de autoridades políticas y militares.

No obstante, la regulación garantista de la interceptación de comunicaciones en los procesos penales, en la práctica se han manifestado una serie de irregularidades en su aplicación, y una falta de control efectivo por parte de los jueces de garantía, como las demostradas en el caso mapuche, y entre las que podemos mencionar las siguientes: la solicitud de órdenes genéricas, en las que solo se mencionan números telefónicos, pero no los nombres o circunstancias que vinculan a esas personas a los hechos; la interceptación de comunicaciones de los afectados por las medidas con sus abogados defensores; la solicitud de autorización retroactiva de interceptaciones ya realizadas; la interceptación de comunicaciones con personas no relacionadas con hechos delictivos, tales como autoridades políticas, o activistas; la falta de fundamentación de las órdenes de interceptación por parte de los jueces; la falta de control respecto de la ejecución de las medidas, respecto a su duración, a la notificación a los afectados, a la custodia durante su utilización y su posterior destrucción de los registros de las comunicaciones.

De esta serie de problemas, es necesario prestar atención especial a la interceptación de comunicaciones entre los afectados y sus abogados defensores. Si bien el Código Procesal Penal prohíbe esta situación, en la práctica está legitimada por el Instructivo General Nº 060-2014 del Ministerio Público, que "en términos sencillos y directos instruye a los fiscales y policías a escuchar todas las comunicaciones entre el abogado defensor y el cliente imputado que se produzcan en el contexto de una autorización judicial".[32] Este sistema permite a los fiscales escuchar las conversaciones completas entre los imputados y sus abogados, a efectos de distinguir si se trata de conversaciones privadas, o si se aplica la excepción a la prohibición en caso de que el abogado también sea responsable de los hechos delictivos, y en caso de escucharlas, deben comunicar al juez de garantía.

Si bien pueden darse casos en que se escuchen comunicaciones privadas entre el afectado por la medida y su abogado de manera accidental (por ejemplo, en el caso de que no se haya imputado aún al afectado por la medida y se desconozca si tiene abogado defensor o no, o en caso de que el abogado se comunique con el afectado por un medio no asociado a su nombre, como podría ser un teléfono móvil de prepago recién comprado), el instructivo legitima que se escuchen las conversaciones enteras, aun cuando existen posibilidades para excluirlas del registro apenas se determine que se trata de una conversación con un abogado defensor, o de excluirlas previamente en caso de conocerse dicha información.

El problema es que, además de afectar el derecho a la privacidad y a la inviolabilidad de las comunicaciones, también afecta el derecho a la defensa, en cuanto podría permitir obtener pruebas

[32] Bown Intveen, Waldo (2017). Interceptaciones telefónicas de conversaciones entre abogado defensor e imputado. Tesis para optar al grado de magíster en derecho, Universidad de Chile, p. 18.

incriminatorias, la estrategia de la defensa o, incluso, al alterar la percepción del fiscal o de la policía respecto del imputado.[33]

Si bien se han detectado este tipo de problemas en las órdenes de interceptación de comunicaciones del sistema procesal penal, estos se manifiestan de manera particularmente grave en el caso de los procedimientos especiales de obtención de información establecidos en el Título V de la ley 19.974, sobre el sistema de inteligencia del Estado, en la medida que estos presentan una serie de problemas de diseño, sin muchas de las garantías establecidas en el sistema procesal penal. Dichos procedimientos son:

a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;
b) La intervención de sistemas y redes informáticos;
c) La escucha y grabación electrónica incluyendo la audiovisual, y
d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

Estos procedimientos también tienen una serie de controles formales para su otorgamiento, a saber: están establecidos por ley y para ser decretados requieren autorización judicial, por un ministro de la Corte de Apelaciones respectiva, mediante resolución fundada; se establecen límites a la procedencia de estos procedimientos pues solo se pueden solicitar en cuanto sea información "estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas", y; se establecen fines en principio legítimos para su utilización, es decir, resguardar la seguridad nacional y la protección de la población "de las amenazas del terrorismo, el crimen organizado y el narcotráfico".

En primer lugar, las medidas de vigilancia de la ley de inteligencia son más amplias, incluyendo, por ejemplo, la posibilidad de intervenir sistemas informáticos, la que puede resultar especialmente peligrosa para los derechos fundamentales. Como señaló[34] el relator especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos:

> "La manipulación por parte de autoridades estatales del software, datos, sistemas informáticos, red, u otro dispositivo electrónico sin el permiso de la persona u organización responsable o conocimiento de los usuarios (hacking gubernamental) es una práctica altamente intrusiva que presenta serios riesgos para el ejercicio de los derechos humanos en línea. En caso de ser autorizada por ley, esta práctica debe estar limitada a la vigilancia en el contexto de la investigación de graves delitos. Su empleo para cualquier otro fin debe estar expresamente prohibido".

Asimismo, el diseño de las medidas de vigilancia en los casos de la ley de inteligencia tienen menores controles, a saber: la calificación de su necesidad es determinada por el funcionario de inteligencia competente, en vez del juez que la solicita; tienen una duración más amplia, de 90 días, renovables con autorización del ministro competente; son solicitadas y decretadas sin conocimiento ni intervención de los afectados por la medida; no hay un deber de destrucción de los registros ya utilizados o irrelevantes; no hay una prohibición expresa de la exclusión de los abogados defensores; no hay un procedimiento reglado para la solicitud de las medidas, siendo usualmente solicitadas de manera verbal y sin quedar registro de las mismas, ni de sus fundamentos.[35]

---

[33] Íbid., pp. 41-42.
[34] Lanza, Edison (2017). Informe anual de la Comisión Interamericana de Derechos Humanos 2016. Volumen II. Informe de la Relatoría Especial para la Libertad de Expresión, Párrafo 1289, p. 397
[35] Cámara de Diputados de Chile (2018). Op . Cit. Testimonio de Francisco Ljubetic, p. 141.

Es particularmente grave la falta de comunicación a los afectados por las medidas, lo que se podría justificar en los casos de uso exclusivo para la inteligencia del Estado (esto, sin tomar en consideración las críticas que se han manifestado por la doctrina respecto de los programas de vigilancia secretos), pero en la medida que estas interceptaciones de comunicaciones se han terminado liberando de su secreto y siendo utilizadas en procesos penales, terminan afectando de manera evidente y grave los derechos a la privacidad, a la inviolabilidad de las comunicaciones y al debido proceso.

En la práctica, en el caso chileno, se ha comprobado cómo se han utilizado las medidas de vigilancia que permite la ley de inteligencia para fines de persecución penal, en una actividad coordinada entre el Ministerio Público y las unidades de inteligencia de Carabineros de Chile, como se pudo ver en especial en el caso de la Operación Huracán. Así, por ejemplo, se desprende de las declaraciones de Leonardo Osses, ex capitán de Carabineros, miembro de la Unidad de Inteligencia Operativa Especializada de Temuco, ante la Comisión Investigadora de la Cámara de Diputados, quién dijo:[36]

> "[e]l fiscal señaló que pedir una autorización de esas características al juzgado de garantía era super complejo. Dio el ejemplo de que en una oportunidad para solicitar una interceptación telefónica a un juzgado de garantía era supercomplicado, y en base a la nomenclatura que había en inteligencia tenían la posibilidad de solicitar una interceptación de tipo informática, por lo cual la misma ley sobre el sistema de inteligencia del Estado permite realizar instrucciones informáticas, en este caso específicamente a un ministro de Corte".

Si bien el artículo 225 del Código Procesal Penal prohíbe utilizar los resultados de las medidas de interceptación de comunicaciones como pruebas en el proceso penal, lo que impediría en principio la utilización de comunicaciones interceptadas por el procedimiento de la ley de inteligencia, en la práctica hemos visto que las unidades de inteligencia de las policías han trabajado en coordinación con el Ministerio Público, utilizando así información de inteligencia en procesos penales.

La falta de control judicial de estas medidas de vigilancia, utilizadas más allá de los fines legales que permitieron su interceptación, supone que se acepten medidas que afectan ilegítimamente una serie de derechos más allá de la mera inviolabilidad de las comunicaciones, o el debido proceso, que ya mencionamos. Por ejemplo, pueden afectar el derecho a la libertad individual, en la medida que se puedan dictar medidas precautorias en los procedimientos penales, o como se argumentó en el caso de escuchas telefónicas a alcaldes mapuche, que se afecte este derecho a través de la amenaza de ser sujetos de una operación policial o de inteligencia de carácter irregular.

Así, como ya señalamos en el caso de las medidas de televigilancia, en el caso de la interceptación de comunicaciones también se pueden manifestar efectos intimidatorios sobre derechos tales como la libertad de expresión, la libertad de asociación, la libertad ambulatoria y seguridad, entre otros. Una muestra práctica de estos efectos, la podemos ver en el testimonio de Héctor Llaitul ante la comisión investigadora de la Cámara de Diputados sobre la Operación Huracán, donde señala "que se le intervienen los teléfonos, está el sistema de escuchas, se accede a la mensajería, están los registros, las pistas, los archivos, las carpetas. Una cantidad innumerable de intervenciones telefónicas, de las comunicaciones. Ellos lo sabían y, de alguna manera, tenían mucho cuidado al respecto".[37]

El despliegue de estas tecnologías de vigilancia se ha vuelto cada vez más intensivo e invasivo, dejando pocos espacios libres de la posibilidad de vigilancia. Esto pone en riesgo no solo las libertades

[36] Cámara de Diputados de Chile (2018). Informe de la Comisión Especial Investigadora de la actuación de los organismos policiales, de persecución criminal y de inteligencia en torno a la supuesta existencia de pruebas falsas en el marco de la denominada "Operación Huracán". Declaración de Leonardo Osses, p. 48.
[37] Cámara de Diputados de Chile (2018). Informe de la Comisión Especial Investigadora de la actuación de los organismos policiales, de persecución criminal y de inteligencia en torno a la supuesta existencia de pruebas falsas en el marco de la denominada "Operación Huracán". Testimonio de Héctor Llaitul, p. 16.

individuales de las personas, sino que también afecta a la esfera pública, poniendo en riesgo derechos tales como la libertad de asociación. En ese sentido, se ha dicho que "las interacciones públicas libres de vigilancia tienen un valor político distintivo. Es más, se puede mostrar que no solo el uso, sino que la recopilación de información puede ser problemático, en la medida que la recopilación de información cambia el contexto de las relaciones sociales y, en consecuencia, debilita las posibilidades de la autodeterminación colectiva".[38]

Este efecto de la vigilancia sobre libertades colectivas ha sido observado también en la jurisprudencia de la Corte Interamericana de Derechos Humanos, en el caso Escher y otros contra Brasil. En esta sentencia se hizo un análisis[39] de cómo las injerencias ilegítimas en el derecho a la privacidad de los afectados también tuvieron un efecto negativo sobre su derecho a la libertad de asociación, considerando que:

> "[l]a intervención arbitraria de las comunicaciones de personas [pertenecientes a una asociación], restringe no sólo la libertad de asociación de un individuo, sino también el derecho y la libertad de determinado grupo a asociarse libremente, sin miedo o temor". La libertad para asociarse y buscar ciertos fines colectivos es indivisible, de modo que una restricción a la posibilidad de asociarse representa, directamente, un límite al derecho de la colectividad de alcanzar los fines que se proponga (…) tanto la intervención, como el monitoreo y grabación de las comunicaciones telefónicas de las víctimas, se llevaron a cabo con el objeto de ejercer un control sobre sus actividades asociativas, [y] la publicación de dichas comunicaciones, resguardadas por secreto de justicia, fue efectuad[a] expresamente para deslegitimar el trabajo de las asociaciones que integraban las víctimas".

Finalmente, la existencia de amplias medidas de vigilancia de las comunicaciones, en especial cuando son secretas para las personas afectadas como es el caso de las medidas de la ley de inteligencia, terminan generando una falta de control efectivo de los jueces encargados de autorizar las medidas, pudiendo llegar a transformarse en un mero control formal que timbra órdenes, sin ser un verdadero mecanismo de rendición de cuentas respecto del rol de los órganos del Estado en la afectación de derechos fundamentales.[40]

Como hemos visto recientemente en el caso de la Operación Huracán, la existencia de mecanismos de vigilancia con escaso control por parte de los tribunales, terminó permitiendo abusos totalmente desproporcionados, a través de medidas de vigilancia con la mera apariencia de legalidad, pero que terminaron incluyendo incluso la realización de montajes y la implementación de pruebas falsas, las que se terminaron descubriendo de manera incidental.

****

[38] Stahl, Titus (2016). Indiscriminate mass surveillance and the public sphere. En: Ethics and Information Technology, Vol. 18 N.º 1, pp. 37-38.
[39] Íbid., párrafo 165, p. 49.
[40] Setty, Sudha (2015). Surveillance, secrecy, and the searc for meaningful accountability. En: Stanford Journal of International Law, Nº 69, p. 90.