Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina

Por Verónica Ferrari y Daniela Schnidrig
con la colaboración de la Electronic Frontier Foundation

Agosto 2016

ELECTRONIC FRONTIER FOUNDATION

CELE
Centro de Estudios en Libertad de Expresión y Acceso a la Información

Daniela Schnidrig es parte del equipo de Global Partners Digital, donde coordina un proyecto de políticas de ciberseguridad. Se desempeñó como investigadora en derechos humanos y políticas de Internet en el Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Universidad de Palermo (CELE), fue asesora en la Comisión Bicameral para la Reforma, Actualización y Unificación de los Códigos Civil y Comercial de la Nación del Congreso de la Nación Argentina. Colaboró con la Asociación por los Derechos Civiles (ADC) en proyectos de derechos sexuales y reproductivos y con Human Rights Watch. Daniela es abogada graduada de la Universidad Torcuato Di Tella en Buenos Aires.

Verónica Ferrari es investigadora en los proyectos de derechos humanos e Internet del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE). Antes de unirse al CELE, se desempeñó como coordinadora del área de comunicación y prensa en organizaciones no gubernamentales como el Instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP) y el Instituto Latinoamericano de Seguridad y Democracia (ILSED). Verónica es licenciada en Ciencias de la Comunicación por la Universidad de Buenos Aires.

Agradecemos la contribución de Katitza Rodríguez, International Rights Director por la revisión sustantiva del informe, Kim Carlson y David Bogado por la corrección de estilo y traducción. Gracias también a Ramiro Ugarte quien realizó una consultoría para EFF en este proyecto escribiendo el anexo del informe argentino con los nuevos desarrollos a partir de noviembre de 2015 hasta marzo de 2016, y su correspondiente Preguntas Frecuentes (FAQ).

El presente informe forma parte del proyecto regional "Vigilancia y Derechos Humanos" llevado a cabo en ocho países de América Latina por la Electronic Frontier Foundation (EFF), una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital. El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo (UP) tiene como objetivo producir, desde una perspectiva académica, investigaciones que se constituyan en herramientas útiles para los distintos sectores involucrados en la defensa y promoción de los derechos de libertad de expresión y acceso a la información. Dentro del CELE, funciona la Iniciativa por la Libertad de Expresión en Internet (iLEI), un programa especial dedicado a promover mejores políticas en materia de internet.

Índice de contenido

1.

Fuerza Normativa de Tratados Internacionales de Derechos Humanos que Puedan Afectar la Vigilancia de las Comunicaciones

1.1 ¿Cómo Recoge el Estado la Obligación de Cooperación Internacional en Materia de Intercambio de Información?

Son numerosos los tratados internacionales que contienen previsiones sobre derechos que pueden ser afectados por la vigilancia de las comunicaciones. El primer derecho asociado con la vigilancia es el derecho a la privacidad y a la intimidad, contemplados por distintos instrumentos internacionales.

Por ejemplo, la Convención Americana sobre Derechos Humanos—en adelante, CADH—prevé en su artículo 11 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." La Declaración Universal de Derechos Humanos—en adelante, DUDH—contempla una redacción muy similar en su artículo 12, al igual que el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, que establece lo mismo y agrega que "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Los tratados de derechos humanos ratificados por la Argentina son plenamente vinculantes y aplicables en el derecho interno. La Corte Suprema de Justicia de la Nación dejó esto en claro en el fallo "Ekmekdjian c. Sofovich," un caso sobre libertad de expresión y derecho a réplica del año 1992. Al respecto, la Corte sostuvo que la Convención de Viena—en vigor en Argentina desde 1980—le confiere primacía a las convenciones de derecho internacional por sobre el derecho interno y que, además, "cuando la Nación ratifica un tratado que firmó con otro Estado, se obliga internacionalmente a que sus órganos administrativos y jurisdiccionales lo apliquen a los supuestos que ese tratado contemple, siempre que contenga descripciones lo suficientemente concretas de tales supuestos de hecho que hagan posible su aplicación inmediata."[1]

En 1994, durante la última reforma a la Constitución Nacional argentina, esta doctrina fue expresamente adoptada al establecer la jerarquía constitucional de los tratados internacionales de derechos humanos ratificados por el país.[2]

Esto no deja lugar a dudas que las protecciones a la posible afectación de derechos humanos en casos de vigilancia de las comunicaciones por el Estado, contempladas en tratados de derechos humanos ratificados por Argentina, son plenamente operativos y deben ser respetados por el Estado.

1.2 ¿Tiene Tratados Internacionales que Incluyen la Doble Incriminación como Condicionante para Cooperar?

Respecto al requisito de la doble incriminación (*dual criminality*) como condicionante para la cooperación jurídica internacional en materia penal, deben analizarse los distintos tratados celebrados con otros países.

Argentina cuenta con la Ley No. 24.767 de Cooperación Internacional en Materia Penal, que regirá para casos con Estados con los que no se haya celebrado un tratado de cooperación, o para cuestiones que no estén incluidas en dichos tratados. Esta ley dispone que, para que proceda la extradición de una persona, el hecho material del proceso deberá constituir un delito en la ley argentina y la ley del Estado requirente, y que tenga prevista una pena privativa de libertad con mínimo y máximo tales que su semisuma sea al menos de un año.[3]

Para los casos en los que exista un tratado de asistencia o de cooperación internacional, deberá respetarse lo que éste establezca. Algunos instrumentos de cooperación contienen el requisito de doble incriminación, como por ejemplo el Tratado de Extradición entre la República Argentina y la República Oriental del Uruguay,[4] que establece que los delitos que dan lugar a la extradición son aquellos "tipificados como delito por las leyes de ambas Partes, cualquiera sea la denominación de dicho delito, que sean punibles con una pena privativa de libertad cuya duración máxima no sea inferior a dos años."[5]

En cambio, el Convenio entre la República Argentina y la República del Salvador sobre Asistencia Jurídica en Materia Penal,[6] por ejemplo, establece que "La asistencia se prestará aun cuando el hecho por el cual se procede en, la Parte requirente no sea considerado como delito por la legislación de la Parte requerida."

En definitiva, habrá que analizar cada tratado de cooperación en particular, pero es positivo que el requisito de doble incriminación esté incluido en la Ley de Cooperación Internacional.

2.

Marco Constitucional

El marco jurídico constitucional argentino protege derechos fundamentales que pueden ser afectados por la vigilancia de las comunicaciones.[7] Como comentamos en la sección anterior, los tratados internacionales de derechos humanos ratificados por el país tienen jerarquía constitucional, por lo tanto todas las protecciones a derechos relacionados con la vigilancia que éstos contengan son plenamente exigibles en nuestro régimen jurídico.

Además de la protección del derecho internacional, la Constitución Nacional contempla la protección de distintos derechos relacionados que podrían ser afectados por la vigilancia de las comunicaciones. Respecto del derecho a la intimidad y a la privacidad, la Constitución Nacional sostiene que "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe."[8]

La Constitución establece, también, la inviolabilidad del domicilio y de las comunicaciones, en tanto "...El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación..."[9] Si bien menciona a la correspondencia epistolar, la Corte Suprema ha ampliado esta protección, entendiendo que las comunicaciones a través de Internet también están protegidas por esta cláusula constitucional.[10] (Ver sección "Jurisprudencia").

Por último, la figura del habeas data también está contemplada en la Constitución. Ésta dispone que "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística."[11]

La Constitución prevé, además, la acción de amparo. Ésta es una acción expedita y rápida, que podrá interponerse "siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva."[12] Ésta

fue la herramienta legal que utilizó Halabi, un abogado que solicitó a la Corte Suprema que declara la inconstitucionalidad de un artículo sobre retención obligatoria de datos porque era violatorio de la intimidad y además violaba el secreto profesional. Sobre este caso nos explayaremos en la sección "Jurisprudencia."

Podemos concluir que el marco constitucional argentino contempla una fuerte protección a los derechos a la intimidad, privacidad, protección de datos personales e inviolabilidad de las comunicaciones. A continuación, analizaremos el marco más amplio de las leyes y normativa que regulan esta protección de forma específica.

3.

Marco Legal

3.1 La Vigilancia de las Comunicaciones en el Contexto Penal

La legislación penal argentina contiene varias disposiciones respecto de la interceptación de comunicaciones privadas. Por un lado, se criminaliza la interceptación de comunicaciones privadas por parte de terceros. Por otro lado, se regulan las condiciones en las que el Estado puede interferir comunicaciones en el marco de un proceso penal.

En cuanto a las condiciones en las que el Estado puede interferir comunicaciones en el marco de un proceso penal, encontramos algunas disposiciones en el nuevo Código Procesal Penal Nacional aprobado en noviembre de 2014.[13] Este nuevo cuerpo normativo iba a entrar en vigencia en marzo de 2016,[14] pero un decreto presidencial de diciembre de 2015 postergó su implementación con el argumento de que la puesta en práctica del nuevo cuerpo normativo "en las actuales condiciones pondría en grave riesgo la correcta administración de justicia."[15] Este decreto establece, asimismo, que será la Comisión Bicameral de Monitoreo e Implementación del nuevo Código Procesal Penal del Congreso —junto con el Ministerio de Justicia— la encargada de establecer un nuevo cronograma para la puesta en práctica del nuevo cuerpo normativo.[16]

El nuevo código establece, en su sección de principios y garantías procesales, el deber de respetar la protección de la intimidad y la privacidad, abarcando las comunicaciones. Este nuevo cuerpo sostiene que:

> *Se debe respetar el derecho a la intimidad y a la privacidad del imputado y de cualquier otra persona, en especial la libertad de conciencia, el domicilio, la correspondencia, los papeles privados y comunicaciones de toda índole. Sólo con autorización del juez y de conformidad con las disposiciones de este Código podrán afectarse estos derechos.*[17]

En la sección correspondiente ampliaremos sobre el procedimiento penal para ordenar la interceptación de una comunicación.

3.2 Delitos Electrónicos y Otras Sanciones

En cuanto a la criminalización de la interceptación de comunicaciones, el Código Penal contempla las siguientes penas para la violación de la privacidad:

> *Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.*
>
> *En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.*
>
> *La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.*
>
> *Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.*[18]

Se pena además, a quien a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido, con una pena agravada si se trata de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.[19]

El Código Penal contempla penas también contra quienes hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros, con la excepción de quienes hubieran obrado con "el propósito inequívoco de proteger un interés público."[20]

Por último, se pena a quien "a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por

disposición de la ley; ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales", agravando la pena si se trata de un funcionario público.[21]

La Ley No. 25.520 de Inteligencia Nacional, que analizaremos más en detalle en la sección siguiente, incorporó en 2015 ciertas disposiciones penales para castigar a quien, participando en forma permanente o transitoria de las tareas reguladas en dicha ley, "indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos."[22]

Esta ley también tipifica el delito de quien, con orden judicial y estando obligado a hacerlo, "omitiere destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones."[23] Siguiendo lo que establece esta normativa, se castiga también a todo funcionario o empleado público que realice acciones de inteligencia prohibidas por las leyes.[24]

3.3 Vigilancia de las Comunicaciones de las Actividades de Inteligencia y Contrainteligencia

El marco regulatorio de las actividades de inteligencia está dado en Argentina, en primer término, por la Ley 25.520 de Inteligencia Nacional de 2001[25] y por la ley 27.126 que la modifica en muchos de sus aspectos más sustanciales.[26] Forman parte de este marco normativo, asimismo, los decretos que promulgan[27] y reglamentan[28] ambas leyes y por un decreto reciente que establece la denominada Nueva Doctrina de Inteligencia Nacional.[29]

La ley 27.126 aprobada en 2015 modifica aspectos de la normativa y, fundamentalmente, disuelve el organismo encargado de las actividades de inteligencia y lo reemplaza por la Agencia Federal de Inteligencia (AFI).

Según este marco regulatorio, los organismos de inteligencia deberán desarrollar sus actividades en línea con lo que establecen la Constitución Nacional y los tratados de derechos humanos suscriptos por la Argentina, analizados anteriormente.[30]

Según este cuerpo normativo la "inteligencia nacional" en Argentina se define como la actividad que consiste en la "obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación."[31]

Este marco legislativo vinculado a la inteligencia nacional, tal como señala la Asociación por los Derechos Civiles (ADC) en un trabajo reciente sobre esta temática, debe leerse en conjunto con las leyes de Defensa Nacional[32] y de Seguridad Interior.[33] ADC, en su informe, señala que este grupo de normas "busca delimitar actividades y establecer prohibiciones taxativas con el objetivo explícito de impedir abusos" y agrega que uno de sus objetivos principales es el de distinguir los conceptos y actividades vinculados, por un lado, a la defensa nacional y, por otro, a la seguridad nacional.[34]

Por un lado, la ley de Defensa Nacional regula lo vinculado a las actividades de inteligencia militar que apuntan a enfrentar las "agresiones externas". La ley es clara al señalar que, en ningún caso, se incluirá cuestiones vinculadas a la política interna dentro de estas actividades.[35]

Por su parte, la ley de Seguridad Interior excluye a las fuerzas armadas de las tareas de seguridad interior. Se exceptúan situaciones en las que el Poder Ejecutivo considere que no puede afrontar determinada amenaza con fuerzas de seguridad interna como la Policía Federal, las policías provinciales, la Gendarmería Nacional, etcétera. Esta ley regula, asimismo, lo que tiene que ver con las actividades de inteligencias llevadas a cabo por las fuerzas de seguridad y policiales.[36]

Como señalamos antes, el marco regulatorio actual señala que el funcionamiento del sistema de inteligencia en Argentina deberá ajustarse estrictamente a las previsiones que aparecen en la Constitución Nacional y en las normas legales y reglamentarias vigentes.[37] Y establece que ningún organismo de inteligencia argentino podrá:

> *Realizar tareas represivas, poseer facultades compulsivas, cumplir, por sí, funciones policiales. Tampoco podrán cumplir funciones de investigación criminal, salvo ante requerimiento específico y fundado realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción,[38] o que se encuentre, para ello, autorizado por ley, en cuyo caso le serán aplicables las reglas procesales correspondientes.[39]*

A partir de la modificación que trajo la ley 27.126, el marco legislativo establece que son las autoridades máximas de cada organismo del sistema de inteligencia las que ordenan estas actividades. De todas formas, señala que "en caso de urgencia" estas actividades podrán iniciarse, debiendo ser informadas de manera inmediata a esas máximas autoridades.[40]

Específicamente, en cuanto a la interceptación y captación de comunicaciones privadas, el marco legislativo argentino en materia de inteligencia establece que solo se podrán solicitar mediante una autorización judicial.[41] La ley agrega que esta autorización, "deberá formularse por escrito y estar fundada indicando con precisión el o los números telefónicos o

direcciones electrónicas o de cualquier otro medio, cuyas comunicaciones se pretenda interceptar o captar."[42]

Si bien esta cuestión será analizada más en detalle en otro apartado, vale la pena señalar que, a partir de la reforma del sistema de inteligencia nacional en el 2015, se transfirió la Dirección de Observaciones Judiciales, el único órgano del Estado argentino que podía llevar adelante las interceptaciones o captaciones de las comunicaciones—siempre que sean autorizadas u ordenadas por la autoridad judicial competente, como señalamos antes—al ámbito de la Procuración General de la Nación del Ministerio Público, un "órgano independiente con autonomía funcional y autarquía financiera."[43] A través de un decreto de necesidad y urgencia de diciembre de 2015, el por entonces recientemente asumido presidente Macri decidió el traspasó de este organismo a la Corte Suprema de Justicia de la Nación.[44]

El marco legislativo argentino señala que los organismos de inteligencia deben enmarcar sus actividades "inexcusablemente" dentro de lo que establece la Ley de Protección de Datos Personales,[45] que analizaremos más adelante.

La revelación o divulgación de información adquirida por los organismos de inteligencia con motivo del ejercicio de sus funciones, requerirá sin excepción de una orden o dispensa judicial, como se comentó en apartados anteriores.[46]

La ley de Inteligencia Nacional hace también referencia a los bancos de datos almacenados por los órganos que componen el sistema de inteligencia argentino. Según la ley, estos organismos deberán tenerlos centralizados en el denominado Banco de Protección de Datos y Archivos de Inteligencia, que estará a cargo de un funcionario que deberá velar por las "las condiciones y procedimientos respecto a la recolección, almacenamiento, producción y difusión de la información obtenida, mediante tareas de inteligencia."[47]

La regulación establece, también, que cada uno de estos bancos de protección de datos tendrá que controlar el ingreso y la salida de información garantizando su reserva constitucional y legal; que los datos recabados por las actividades de inteligencia que no sirvan para los fines establecidos por el marco que regula esta actividad, serán destruidos; y garantizar que no se almacene información por motivos de raza, creencias religiosas, acciones privadas, actividades políticas, pertenencia a organizaciones sociales, entre otras.[48]

Como se explicó anteriormente, la ley establece sanciones penales para aquellos integrantes de los servicios de inteligencia que indebidamente intercepten, capten o desvíen comunicaciones que no le estuvieran dirigidas.[49]

3.3.1 Nueva Doctrina de Inteligencia Nacional

En el marco de este proceso de reforma del sistema de inteligencia en Argentina al que hicimos mención en secciones anteriores, en el 2015, se aprobó la denominada "Nueva Doctrina de Inteligencia Nacional para el proceso de reforma y modernización del Sistema de Inteligencia"[50] que, gran medida, apunta a definir los nuevos objetivos y tareas de la AFI.

Según el decreto que la crea, esta nueva doctrina apunta a una reforma y modernización del Sistema de Inteligencia Nacional.[51] Incluye una visión integral del concepto de inteligencia definida como "recolección, gestión y análisis de la información"[52] y entendido como una "actividad institucional que se inscribe dentro del marco del Estado constitucional social y democrático de derecho y que apunta a dar cuenta de los desafíos, coacciones y conflictos que ponen en riesgo la defensa y la seguridad democráticas del pueblo argentino."[53]

El primero de los anexos que acompaña el decreto que fija este cuerpo doctrinario, señala que las actividades de inteligencia en Argentina "se inscriben en la esfera específica del sistema democrático de defensa nacional y de seguridad interior y constituyen acciones fundamentales para la estabilidad y protección del sistema democrático."[54]

Y, señala, específicamente, que la inteligencia nacional debe velar por la protección y el cuidado de los argentinos, y no "espiarlos" *(las comillas están en el original).* Por ello, define al sistema de inteligencia nacional en tanto un observatorio que se dedicará, exclusivamente, a "la producción y gestión de conocimientos acerca del conjunto de problemáticas relevantes en materia de defensa nacional y seguridad interior."[55]

Esta nueva doctrina define a la seguridad interior como la que comprende "los fenómenos delictivos violatorios de las libertades y derechos de las personas y del Estado constitucional social y democrático de derecho."[56] Y, en particular señala que las actividades de inteligencia en ese ámbito atenderán cuestiones como el terrorismo, la criminalidad organizada, con especial énfasis en el narcotráfico y la trata de personas.

Dentro de las actividades de inteligencia se incluirá la producción de información vinculada con los "atentados contra el orden constitucional y la vida democrática". En este grupo de acciones se incluyen, según esta nueva doctrina, las actividades de grupos económicos o financieros que realicen corridas bancarias y cambiarias, desabastecimientos, y que puedan derivar en un "golpe de mercado."

Siguiendo un análisis preliminar realizado por ADC, puede ser problemático ampliar los "actos de fuerza contra el orden institucional y el sistema democrático" que ya aparecen definidos en la Constitución Nacional dado que "podría incentivar prácticas estatales que podrían derivar en la violación de derechos de la ciudadanía. Los atentados al orden

constitucional se encuentran claramente definidos en la Constitución y el poder ejecutivo no debería ampliar esos supuestos por vía reglamentaria."[57]

Dentro de las funciones que tiene el nuevo organismo encargado de la inteligencia en Argentina y en lo vinculado a seguridad interior, aparece la producción de inteligencia referida a delitos federales complejos como los ciberdelitos, "el uso fraudulento y la difusión ilegal de contenidos."[58]

Cabe señalar, por lo menos, la vaguedad en las definiciones. Por ejemplo, no se desprende del documento qué se entiende por ciberseguridad, un término, por demás, complejo y problematizado a nivel global en las discusiones sobre regulación y gobernanza de Internet. Este cuerpo doctrinario tampoco da precisiones sobre qué tipo de prácticas podrían caer bajo la muy amplia "difusión ilegal de contenidos." Por ejemplo, cabe preguntarse si la difusión de contenidos en línea que violan los derechos autorales[59] podría ser una actividad susceptible de actividades de inteligencia. Todas estas, cuestiones que podrían ser peligrosas en términos de vigilancia y ejercicio de derechos en internet.

3.4 Vigilancia de las Comunicaciones en la Normativa de Telecomunicaciones

3.4.1 Argentina Digital

El marco regulatorio actual en materia de telecomunicaciones está dado por la ley "Argentina Digital,"[60] aprobada en diciembre de 2014. La aprobación se dio luego de una muy rápida discusión en el Congreso argentino y sin la debida participación de todos los sectores involucrados en este sector clave.[61] Esta ley reemplaza a la normativa anterior de 1972, salvo en las cuestiones que no se opongan a las previsiones establecidas en esta nueva ley.[62]

En cuanto al tema de la vigilancia, la ley "Argentina Digital" establece la inviolabilidad de las comunicaciones realizadas a través de las redes y servicios de telecomunicaciones. Según la ley, la interceptación, así como su posterior registro y análisis, sólo podrá realizarse mediante el requerimiento de un juez competente.[63]

Otro artículo establece las obligaciones para los usuarios de los denominados servicios de tecnologías de la información y comunicación. Esta ley, en su artículo 60, señala que los usuarios de estos servicios deberán permitir el acceso del personal que trabaja en las empresas que proveen los servicios de telecomunicaciones y del recientemente creado Ente Nacional de Comunicaciones (ENACOM)[64] "a los efectos de realizar todo tipo de trabajo o verificación necesaria."[65]

Organizaciones de la sociedad civil advirtieron, en su momento, que la redacción amplia y vaga de este artículo implicaría un riesgo a la privacidad de los usuarios e ir a contramano del articulado de la Constitución Nacional que, como mencionamos antes, establece la inviolabilidad del domicilio.[66]

3.4.2 Reglamento de Calidad de los Servicios de Telecomunicaciones

Otra normativa a tener en cuenta en materia de telecomunicaciones es el Reglamento de Calidad de los Servicios, elaborado por la Secretaría de Comunicaciones en 2013.[67] De acuerdo al nuevo marco normativo dado por Argentina Digital,[68] este organismo, sus funciones y prerrogativas quedan bajo la órbita de la nueva autoridad de aplicación, el ENACOM. Analizaremos los problemas que podría tener este reglamento en materia de vigilancia en el apartado vinculado a retención de datos.

3.4.3 Ley 25.891 de Servicios de Comunicaciones Móviles

Esta ley[69] que, si bien no ha sido reglamentada, se encuentra dentro de la normativa vigente de acuerdo al Portal Nacional de Usuarios de Telecomunicaciones, sitio oficial en la materia.[70]

Esta normativa de 2004 instituye un Registro de Usuarios de teléfonos móviles con el objetivo de detectar actividades ilícitas realizadas a través de estos dispositivos. Esta norma ordena la creación de una base de datos para registrar teléfonos móviles perdidos o robados que, además, a la que el Estado puede acceder "de manera inmediata, a toda hora y todos los días del año," ante requerimiento del Poder Judicial y/o el Ministerio Público."[71]

La ley va en contra de la normativa de datos personales en tanto los prestadores del servicio de telefonía móvil están obligados a recolectar, retener y divulgar datos personales sin límites ni finalidades establecidos por la ley. La norma, que carece de una definición sobre qué tipo de datos pueden ser solicitados, obliga a las prestadoras de telefonía móvil compartir "toda la información sobre clientes y usuarios" (por la vaguedad del articulado, esto puede contemplar desde desde datos personales del titular del equipo, el modelo del mismo hasta información sobre las comunicaciones que realiza).

Además, como señalamos, no establece un plazo máximo de retención de datos personales ni prohíbe a los prestadores la transferencia de los mismos o un uso distinto de aquel para el que fueron recolectados.[72]

3.5 Normativa sobre Retención de Datos

En Argentina no existe legislación sobre la conservación obligatoria de datos de tráfico por parte de las empresas prestadoras de conexión. Sin embargo, existen algunas cuestiones en el Reglamento de Calidad de los Servicios de Telecomunicaciones antes citado. El reglamento

fue elaborado por la antes denominada Secretaría de Comunicaciones.[73] A partir de la aprobación de la ley "Argentina Digital," este organismo se fusionó con la Comisión Nacional de Comunicaciones convirtiéndose, en, primero en la AFTIC, luego fusionada bajo el ENACOM.

De acuerdo a este reglamento, los prestadores de servicios de telecomunicaciones deberán garantizar el libre acceso del recientemente creado ENACOM a las instalaciones y sistemas vinculados a la prestación del servicio, y brindar toda la información que les sea requerida en las formas y en los plazos que este organismo establezca.[74]

Este reglamento, asimismo, señalaba que este organismo público, a fin de cumplir con los estándares de calidad establecidos en el reglamento, podría "requerir a los prestadores de servicios de telecomunicaciones la información que estime pertinente, fijando un plazo para su presentación."[75] El reglamento, agrega que, a fin de implementar el sistema de evaluación de la calidad del servicio, los prestadores deberán proveer a la autoridad de aplicación "el libre acceso a sus redes y a su información."[76]

Si bien, más adelante, la resolución indica que la medición de la calidad del servicio deberá efectuarse en concordancia con el marco de protección de los datos personales,[77] estos artículos tienen, cuanto menos, una redacción confusa que podría llevar a un trato inadecuado de los datos de los usuarios[78] y echaría por tierra lo antes mencionado sobre la necesidad que exista una autorización judicial en el marco de una investigación.

Y, específicamente, en cuanto a retención de los datos, el artículo 8 de este reglamento, señala que los prestadores de telecomunicaciones deben conservar, en archivos electrónicos y por un plazo mínimo de tres años, los datos recogidos por sus sistemas que sirvieran de base para el cálculo de los indicadores de calidad establecidos por esta normativa. Asimismo, señala que la autoridad de aplicación podrá requerir "la entrega total o parcial de los mismos y proceder a su almacenamiento durante el lapso que considere conveniente,"[79] aspecto que consideramos discrecional y que podría ser contrario a los estándares internacionales.

3.6 Reglas para el Allanamiento del Domicilio y Registro y Secuestro de Equipos Informáticos

Como explicaremos más adelante, los códigos de procedimiento son dictados en cada jurisdicción, por lo tanto las normas para el procedimiento de allanamiento variarán en cada provincia. Aquí analizaremos el procedimiento contenido en el Código Procesal Penal de la Nación, que se aplica para delitos federales.

3.6.1 Orden de Registro

Si hubiere motivos para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito o que allí se pueda efectuar la detención del imputado o de alguna persona evadida o sospechada de haber participado de un hecho delictivo, el juez ordenará, a requerimiento de parte y por auto fundado, el registro de ese lugar.[80]

El registro puede ser llevado a cabo personalmente por el representante del Ministerio Público Fiscal, o podrá encomendar la diligencia al funcionario debidamente individualizado del Ministerio Público Fiscal o de la policía u otra fuerza de seguridad que estime pertinente.[81]

3.6.2 Allanamiento de Morada

En principio, debe realizarse en horario diurno. Si existiera peligro en la demora, podrá procederse en cualquier horario, explicitando las circunstancias extraordinarias en la orden de allanamiento.[82] El allanamiento será ordenado por el juez y no podrá ser suplido por el consentimiento de quien habita el lugar.[83]

3.6.3 Excepciones al Requisito de Orden Judicial

Podrá llevarse a cabo un allanamiento sin orden judicial cuando:

- Por incendio, explosión, inundación u otro estrago se hallare amenazada la vida de los habitantes o la propiedad;
- Mediare denuncia, cuya entidad resulte verosímil de acuerdo a las circunstancias, de que una o más personas han sido vistas mientras se introducían en una casa o local con indicios manifiestos de comisión de un delito;
- Se introdujere en una casa o local algún sospechado de delito a quien se persigue para su aprehensión;
- Voces provenientes de una casa o local pidieren socorro o anunciaren que allí se está cometiendo un delito;
- Se tuvieren sospechas fundadas que en una casa o local se encuentra la víctima de una privación ilegal de la libertad y corriere peligro inminente su vida o integridad física; el representante del Ministerio Público Fiscal deberá autorizar la medida.[84]

3.6.4 Requisitos que Debe Cumplir la Orden Judicial

El juez examinará el cumplimiento de los requisitos formales y la razonabilidad de los motivos que fundan el pedido del representante del Ministerio Público Fiscal.[85]

La orden debe ser escrita y debe contener:

- La identificación de la investigación en el marco de la cual se libra;

- La indicación detallada del lugar o lugares que habrán de ser registrados;
- La finalidad con la que se practicará el registro.

El día en que la medida deberá efectuarse y, si correspondiera, la habilitación horaria y la descripción de las cosas a secuestrar o personas a detener, así como de la autoridad que la llevará a cabo.

En casos graves y urgentes, la comunicación de la orden a quien se le encomiende el allanamiento podrá realizarse por medios electrónicos o por cualquier otro medio idóneo, con constancia fehaciente sobre el modo de comunicación utilizado y de la identificación del receptor.

Si la solicitud fuese por vía telefónica, el juez exigirá al representante del Ministerio Público Fiscal ciertos requisitos[86] y, si fueran reunidos, autorizará la medida.

3.6.5 Formalidades para el Allanamiento

La orden de allanamiento será comunicada entregándose una copia de ella al que habite o posea el lugar donde deba efectuarse o, cuando esté ausente, a su encargado o, a falta de éste, a cualquier persona mayor de edad que se hallare en el lugar, preferentemente a los familiares del primero.

El funcionario a cargo del procedimiento deberá identificarse e invitar al notificado a presenciar el registro. Cuando no se encontrare ninguna persona, ello se hará constar en el acta.

3.6.6 Recaudos para el Allanamiento

La diligencia se realizará procurando afectar lo menos posible el derecho a la intimidad.[87] El registro se circunscribirá al lugar específico sobre el que se sospecha que pudiera encontrarse el objeto de búsqueda y comprenderá exclusivamente los elementos que estén relacionados con ese fin.

Si en estricto cumplimiento de la orden de allanamiento se encontraren objetos que evidenciaren la comisión de un delito distinto al que motivó la orden, se pondrá en conocimiento del juez o representante del Ministerio Público Fiscal interviniente quien, en caso de estimarlo adecuado, ordenará su secuestro.

En un acta, que será firmada por los concurrentes, se dejará constancia explicativa sobre el lugar y la forma en que fueron hallados todos los objetos secuestrados.

3.7 Otras normativas

3.7.1 Normativa de Protección de Datos Personales

El reconocimiento del derecho de hábeas data y la protección de datos personales aparece, en primer término, y como señalamos antes, dado por la Constitución Nacional en su artículo 43. En cuanto a la protección de datos personales en la legislación argentina, esto se encuentra regulado a partir de la ley 25.326 del año 2000. La referida ley tiene como objetivo la protección integral de los datos personales que se encuentran en bases de datos, tanto públicas como privadas. Su fin es garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que tienen sobre esa información. [88] Junto con esta ley, conforman el marco de protección de datos personales el decreto que la reglamenta[89]—y sus modificaciones[90]—y la ley 26.343[91] que la modifica en uno de sus artículos.

En su artículo 2, la ley de datos personales señala que se entiende por dato personal a la "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables." Y define como dato sensible al dato personal capaz de revelar el origen racial y étnico, las opiniones políticas, las convicciones religiosas, la afiliación sindical, la información referente a la salud o a la vida sexual.

En su artículo 4, esta norma señala que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular y que deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que fueron recolectados.

Siguiendo un trabajo elaborado por ADC, el marco legal argentino, a pesar de ofrecer una fuerte protección a los datos personales presenta "debilidades estructurales." La primera de estas debilidades, dice ADC, está vinculada a una excesiva permisividad hacia el Estado en relación con el almacenamiento, tratamiento y cesión de los datos personales.[92]

La ley 25.326 establece la prohibición de tratar y de ceder datos personales sin el consentimiento de los titulares. Sin embargo, el artículo 5 que exige ese consentimiento permite evadirlo cuando estos se recaban "para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal." En otras palabras, la garantía del consentimiento es inútil cuando quien recaba información es el Estado.

El artículo 11 impide la cesión de los datos si el titular de los mismos no ha prestado su consentimiento. Pero—nuevamente—ese requisito puede ser dejado de lado cuando lo disponga una ley, cuando los datos hayan sido recabados para el ejercicio de funciones propias de los poderes del Estado o cuando la cesión se realice entre dependencias de los

órganos del Estado en forma directa en la medida del cumplimiento de sus respectivas competencias.

Como vemos, la ley de datos personales mediante estas excepciones, redactadas en términos amplios, permite al Estado evadir la prohibición de tratar o ceder datos con el consentimiento de su titular. Al hacerlo, priva a los ciudadanos de la principal herramienta de defensa de la privacidad de sus datos.[93]

El otro inconveniente del marco regulatorio argentino en materia de datos personales tiene que ver ciertos problemas de origen en cuanto a su diseño institucional de la autoridad de aplicación de esta ley. La Dirección Nacional de Protección de Datos Personales, que funciona dentro de la órbita del Ministerio de Justicia y Derechos Humanos, es un órgano de control débil y dependiente del Poder Ejecutivo.[94]

3.7.2 Sistemas de Registro y Recolección de Datos y Vigilancia

Argentina es un país pionero en materia de políticas vinculadas a la identificación de su ciudadanía a partir de técnicas biométricas,[95] entendidas como técnicas que permiten el reconocimiento automático de las personas en base a características biológicas y de comportamiento.[96] Si bien no está vinculado estrictamente a la vigilancia de las comunicaciones, es pertinente a fin de tener un panorama más amplio de la situación en Argentina, dar cuenta de cómo en los últimos años, a partir de la incorporación de nuevos sistemas digitales de recolección y registro de datos por parte de distintos organismos públicos, se ha producido una notable expansión en estas capacidades de vigilancia del Estado argentino.

Diversas organizaciones de derechos humanos vienen llamando la atención sobre el rumbo que está tomando esta recolección, almacenamiento y uso de los datos personales.[97] Estas preocupaciones tienen que ver, en gran medida, con la escasa información oficial acerca de qué hace el Estado con esos datos recabados, por cuánto tiempo los almacena, cómo los analiza, quién tiene acceso a ellos, con qué fines y qué tipo de cruces se realizan entre las distintas bases de datos de estos organismos públicos.[98]

Estos cuestionamientos se relacionan con las observaciones realizadas en secciones anteriores sobre la ley de datos personales en Argentina y dos de sus inconvenientes: (i) que el consentimiento no es necesario cuando los datos personales se recaban para el ejercicio de las funciones propias del Estado o en virtud de una obligación legal y (ii) que habilita a los distintos organismos públicos a compartir entre sí datos personales.[99]

En los últimos años se ha demostrado, además, el uso inadecuado de datos sensibles publicados sin autorización y con una finalidad distinta a la requerida, en contradicción con la normativa de datos personales.[100]

3.7.3 Documento Nacional de Identidad

En la Argentina el Documento Nacional de Identidad (de ahora en más, DNI) es el único instrumento de identificación personal. Por ley,[101] el DNI—que incluye elementos biométricos, como la fotografía y la huella digital del pulgar[102]—es obligatorio para todos los ciudadanos y residentes extranjeros.[103] En Argentina, es necesario presentar esta identificación para todo tipo de interacción: desde un trámite ante un organismo público hasta para la realización de transacciones bancarias o compras con tarjeta de crédito.

A partir del decreto 1501/2009[104] y de distintas resoluciones del Registro Nacional de las Personas (RENAPER),[105] se comenzó a expedir en 2009 un nuevo DNI, confeccionado íntegramente por el Estado argentino. El nuevo DNI incorpora tecnologías informáticas en el proceso de su producción: datos biográficos y huellas en bases de datos digitalizados, y procesos de verificación dactiloscópica mediante herramientas informáticas.[106]

El año pasado, el Ministro del Interior anunció un nuevo "DNI inteligente" que, gracias a un chip, permitirá "interactuar con todos los servicios," desde los datos del Sistema Único de Boleto Electrónico (que se explicará en el siguiente apartado), pasando por la Administración Nacional de la Seguridad Social hasta las historias clínicas de los ciudadanos argentinos.[107]

Según un trabajo de Laura Siri que recopila información oficial sobre este documento "inteligente," el Estado argentino, de esta manera, hará un uso más eficiente y tendrá un acceso más seguro a información y datos que hoy están dispersos. Siri señala que el Ministerio del Interior y Transporte, a través del RENAPER, será el organismo que tendrá a su cargo la recolección, almacenamiento, evaluación, destrucción y procesamiento de los datos del nuevo DNI.[108]

Diversos organismos de derechos humanos se manifestaron, en el último tiempo, en contra de esta iniciativa que permitiría al DNI "pasar a convertirse en una base de datos portable y digitalizada con datos biológicos, biográficos y de la rutina diaria de transporte y consumo, que podrán actualizarse y monitorearse en tiempo real."[109]

3.7.4 Sistema Único de Boleto Electrónico

Mediante una resolución de 2010,[110] se creó el Sistema Único de Boleto Electrónico (SUBE) que permite utilizar el transporte público. A partir del uso de una tarjeta que se registra con todos los datos personales,[111] este sistema genera un registro de todos los viajes que realizan los usuarios, creando así una base de datos controlada por Secretaría de Transporte de la Nación.[112]

Entre los problemas que muestra este sistema, podemos señalar que los datos personales vinculados a los viajes que realizan los usuarios son accesibles no sólo para la persona titular de la tarjeta. Por ejemplo, ingresando el número de la tarjeta en la página oficial de SUBE, y sin necesidad de ingresar ninguna contraseña, se podrá acceder a los registros de viajes que el usuario en cuestión haya realizado con la tarjeta. Esto iría en contra de lo establecido en la ley de datos personales.[113]

Asimismo, este sistema ha demostrado vulnerabilidad en cuanto al resguardo de la información personal de la ciudadanía.[114]

3.7.5 Sistema Federal de Identificación Biométrica

El Sistema Federal de Identificación Biométrica (SIBIOS) fue creado en 2011 a través de un decreto presidencial[115] sin debate público ni discusión parlamentaria. Los objetivos de SIBIOS, según el decreto que le da origen, tienen que ver con brindar una mayor seguridad y prevenir el delito.

SIBIOS, que depende del Ministerio de Seguridad, es un sistema de identificación biométrica centralizado y con cobertura nacional que permite a las agencias de seguridad hacer "referencias cruzadas" de información con datos biométricos y otros datos, inicialmente, recogidos por el RENAPER. La principal fuente de información de SIBIOS es la base de datos de este organismo, tal como lo establece el artículo 2 del decreto que crea este sistema.

SIBIOS, siguiendo lo que sostiene ADC en uno de sus trabajos, representa un cambio significativo en el Registro Nacional de las Personas. Los objetivos del documento nacional de identidad ahora pasan a ser herramientas clave en la política criminal del Estado argentino. Hasta el surgimiento de SIBIOS, sostiene ADC, la relación entre las fuerzas de seguridad y el Registro Nacional de las Personas era indirecta: si la Policía Federal quería acceder a información del RENAPER debía solicitar ese acceso. Ahora con este sistema, la base de datos de SIBIOS será accesible para las fuerzas de seguridad federales (Policía, Gendarmería, Prefectura y Policía aeroportuaria) así como la Dirección Nacional de Migraciones y el RENAPER.[116]

El artículo 3 del decreto 1176/2011 promueve que las provincias se adhieran, lo que implicaría que las fuerzas de seguridad provinciales podría acceder a una única base de datos para poder realizar "consultas biométricas en tiempo real."[117] Según analiza el periodista Claudio Savoia en un libro publicado recientemente sobre vigilancia en Argentina, en la actualidad, ya adhirieron al sistema y comparten sus bases de datos quince provincias argentinas y, hasta septiembre de 2014 fecha de los últimos datos consolidados, ya contaba con 13,2 millones de registros de huellas dactilares.[118]

SIBIOS representa, señala la ADC en uno de sus trabajos, la consolidación de bases de datos que estaban dispersas y la ampliación del acceso a las fuerzas de seguridad del Estado.[119] Este sistema, además, va en contra de la ley de datos personales, que establece que los datos no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.[120]

3.7.6 Disposiciones de la Dirección Nacional de Datos Personales

Como señalamos antes, la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente del Ministerio de Justicia y Derechos Humanos, es el organismo encargado de la aplicación de la ley de datos personales. En el último tiempo, la DNPDP ha publicado una serie de normas reglamentarias y, algunas de ellas, algunas relacionadas con el tema de vigilancia.

3.7.7 Recolección de datos personales a través de VANTs o drones

La disposición 20/2015[121] entiende, siguiendo a la ley de datos personales, que una imagen, registro fílmico o sonoro de una persona constituye un dato de carácter personal y que, por lo tanto, debe estar comprendido por ese marco regulatorio. Esta disposición regula, en particular, la actividad de los Vehículos Aéreos No Tripulados (VANTs) o drones en cuanto a su capacidad de recolectar información.[122] Esta preocupación viene despertando el interés de las organizaciones de derechos humanos en tanto su utilización puede plantear graves amenazas al derecho a la privacidad, entre otros.[123]

La disposición señala que los VANTs o drones[124] realizan "una peculiar" recolección de datos personales que "podrían implicar un importante riesgo para los derechos a la privacidad y a la autodeterminación informativa."[125]

En el Anexo I de esta disposición, se detallan las "Condiciones de licitud para la recolección de datos personales a través de drones." El primero de los artículos de este anexo, señala que la recolección de datos personales (ya sean fotográficos, fílmicos, sonoros o de cualquier otra naturaleza) a través drones será lícita en tanto se realice con el consentimiento del titular del dato, en línea con los artículos 5 y 6 de la ley de datos personales.

De todas formas, señala la disposición, no será necesario el consentimiento del titular de los datos, (i) siempre que los medios para la recolección de la información no impliquen "una intromisión desproporcionada en la privacidad," (ii) cuando los datos se recolecten en un acto público y (iii) si la recolección de los datos la realiza el Estado nacional "en el ejercicio de sus funciones." Esto último, en línea con lo que establece la Ley Nacional de Datos Personales que, como señalamos anteriormente, otorga excesivas prerrogativas al Estado en su capacidad de recolectar datos de la ciudadanía.

En el artículo 2, la disposición señala, en relación con el tratamiento de los datos recolectados por drones, que estos deben ser proporcionados, pertinentes y no excesivos respecto de la finalidad con la que fueron recabados y verificando que no afecten el derecho a la intimidad. Y agrega que los responsables del tratamiento de recolección de los datos personales a través de los drones deberán contar con un manual de tratamiento de datos personales y privacidad que indique, entre otras cosas, la finalidad de la recolección, el plazo de conservación de los datos, y los mecanismos técnicos de seguridad y confidencialidad previstos a fin de dar cumplimiento a lo que establece el marco regulatorio de datos personales.

El artículo 3 por su parte, exige la inscripción de las bases de datos generadas por la actividad de los drones o VANT ante el Registro Nacional de Datos y el artículo 5 contiene una excepción que deja fuera del ámbito de aplicación de la disposición a lo que tiene que ver con "fines recreativos."

La disposición también señala que se deberán extremar las precauciones para no recolectar datos sensibles. Por esta razón, señala la norma, deberá evitarse la captura de información personal en establecimientos de salud, lugares de culto, manifestaciones políticas o sindicales, entre otros.

3.7.8 Disposición sobre Videovigilancia

El uso de cámaras con fines de seguridad es una tendencia creciente en Argentina.[126] Según datos oficiales del primer semestre de este año, en la ciudad de Buenos Aires y los municipios del Conurbano bonaerense funcionan alrededor de 12.600 cámaras.[127] La regulación de la videovigilancia se encuentra comprendida por distinta normativa a nivel provincial. Por ejemplo, la ley 2.602 que regula la videovigilancia en la Ciudad Autónoma de Buenos Aires,[128] la ley 13.164 de Santa Fe,[129] la ley 9. 380 en Córdoba, la ley 5.984 sobre videograbaciones de seguridad de Corrientes, entre otras.

Esta disposición de la DNPDP establece, a nivel nacional, las condiciones de licitud para las actividades de recolección y tratamiento de imágenes digitales con fines de seguridad.

En su artículo 1, esta disposición sigue la línea de la normativa general de protección de datos personales al señalar que la recolección de imágenes digitales, a través de cámaras de seguridad, será lícita en la medida que cuente con el consentimiento previo e informado del titular del dato.

Nuevamente, en esta disposición encontramos excepciones para esto. La disposición establece que, siempre y cuando la recolección de las imágenes personales no implique una "intromisión desproporcionada" en la privacidad, no será necesario el consentimiento previo en un evento privado. En otras palabras, el consentimiento previo no será necesario

cuando la recolección de los datos es efectuada por parte del organizador del evento o, como venimos analizando, la recolección sea realizada por el Estado en el ejercicio de sus funciones. Tampoco será necesario el consentimiento cuando se recolecten dentro de un predio de uso propio como, por ejemplo, una propiedad privada, un espacio alquilado o concesionado.

En su artículo 2, esta disposición—al igual que la normativa que venimos analizando—señala que las imágenes no podrán ser utilizadas para una finalidad distinta o incompatible a la que motivó su captación. Y que el Estado, "sólo podrá disponer su difusión al público cuando se encuentre autorizado por ley o por decisión del funcionario competente y medie un interés general que lo justifique." Y, como en otras normas emanadas por este organismo, señala que la información recabada debe ser adecuada, pertinente y no excesiva en relación a la finalidad para la que se hubiera obtenido y deberá evitarse, especialmente, cualquier afectación a la privacidad.

La disposición señala que las imágenes captadas que atenten contra los derechos de las personas deberán ser eliminadas a pedido del titular del dato.

Los responsables de las actividades de recolección y posterior tratamiento de imágenes digitales de personas con fines de seguridad, deberán contar con una política de tratamiento de datos personales y privacidad. La política deberá determinar el tiempo por el cual resultará de utilidad el registro de las imágenes, y eliminarse, una vez vencido ese plazo.[130] También debe poner en práctica las condiciones de licitud previstas en la ley 25.326.[131]

Como en el caso de la información recabada a través de drones, las bases de datos en las que se almacenan datos personales obtenidos mediante cámaras de seguridad deberán inscribirse en el Registro Nacional de Bases de Datos.[132]

3.7.9 Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones

En este documento orientativo, la Dirección Nacional de Datos personales busca establecer pautas en relación a la protección de los datos personales sobre la aplicación de políticas de privacidad en el desarrollo de aplicaciones.[133]

El documento resalta la capacidad de las aplicaciones de recabar, usar y transferir información de carácter personal y resalta la importancia del "dato," como algo que, sin importar dónde está almacenado o cómo se esté utilizando, es propiedad de su titular. Y, señala, que el titular del dato tiene derecho a controlar los usos que se le da a su información personal.[134]

En el apartado 2 dedicado a los principios de privacidad, el documento señala que el consentimiento del titular para el uso de su información personal es la única manera en la

que el tratamiento de datos sea lícito, salvo que se trate de las excepciones antes mencionadas que contempla el marco regulatorio.

Este documento orientativo insta a los diseñadores de aplicaciones a ser claros sobre el uso de sus datos y qué tipo de usos se hará, y a poner en práctica los principios de *privacy by design* y *privacy by default*. También insta a los desarrolladores a establecer una política de privacidad.

Como en las disposiciones antes mencionadas, el documento orientativo establece que los datos recolectados sólo pueden ser utilizados de acuerdo a la finalidad por la que fueron obtenidos. Estos no deben ser excesivos en relación a la finalidad que motivaron su recolección ni obtenidos por medios desleales o fraudulentos. Finalmente, deben ser destruidos cuando hayan dejado de ser útiles.[135]

4.
Jurisprudencia

En 2009, la Corte Suprema de Justicia de la Nación se pronunció en el fallo "Halabi," la sentencia más importante en materia de vigilancia de comunicaciones.

En 2004 se promulgó una norma que modifica la Ley de Telecomunicaciones. Con el objetivo de combatir delitos, se agregaron tres artículos que obligaban a los prestadores de servicios de comunicaciones de disponer de los recursos necesarios para la 'captación y derivación de las comunicaciones para su observación remota a requerimiento del Poder Judicial o del Ministerio Público,' y de conservar esa información por diez años. Estos artículos fueron reglamentados por un decreto, que un año más tarde fue suspendido.[136] Si bien la reglamentación estaba suspendida, la ley que ordenaba la interceptación de las comunicaciones seguía vigente.

Ernesto Halabi era un abogado que inició una acción de amparo, solicitando la inconstitucionalidad de estos tres artículos, sobre la base que violaba el derecho a su privacidad e intimidad y, además, le impedía garantizar a sus clientes el secreto profesional.

El caso finalmente llegó a la Corte Suprema, que se pronunció sobre el tema. El máximo tribunal sostuvo que todo lo datos sobre las comunicaciones que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal. Estos datos sobre las comunicaciones se encuentran alcanzadas por las previsiones constitucionales que protegen la privacidad y establecen la inviolabilidad del domicilio, y lo dispuesto en la Declaración Universal de Derechos Humanos y la Convención Americana de Derechos del Hombre.[137]

Respecto de las facultades del Estado para garantizar la seguridad y mantener el orden público, citó a la Corte Interamericana de Derechos Humanos en el caso "Bulaci," en cuanto sostuvo que la actuación de los Estados está limitada por los derechos fundamentales de los individuos.[138]

La Corte Suprema entonces sostuvo que solamente podría justificarse la intromisión en la vida privada de una persona cuando la intromisión esté prevista en una ley, y siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen.[139]

La Corte citó fallos anteriores sobre los supuestos en los que podría restringirse válidamente la inviolabilidad de la correspondencia:

- que haya sido dictada una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia;
- que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión;
- que la aludida restricción resulte un medio compatible con el fin legítimo propuesto, y
- que dicho medio no sea más extenso que lo indispensable para el aludido logro. A su vez, fines y medios deberán sopesar con arreglo a la interferencia que pudieran producir en otros intereses concurrentes.[140]

Respecto de los artículos cuestionados, la Corte consideró que no respetaban los supuestos arriba citados en los que podría restringirse válidamente la inviolabilidad de la correspondencia. Los artículos no precisaba las oportunidades ni las situaciones en las que operara las interceptaciones, ni previó un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales.[141] Por todas estas razones, la Corte declaró la inconstitucionalidad de estos artículos.

5.

Marco Institucional

5.1 Organigrama de los Órganos Involucrados en la Persecución Penal

Para desarrollar esta sección, es necesario hacer una aclaración previa. Argentina adoptó para su gobierno la forma federal.[142] Un Estado federal supone la existencia de más de un centro territorial con capacidad normativa. Se equilibra la unidad de un Estado con la pluralidad y la autonomía de las provincias.[143]

La Constitución Nacional delega en el Congreso Nacional la legislación sustantiva o de fondo: Códigos Civil, Comercial, Penal, de Minería, y del Trabajo y Seguridad Social. Sin embargo, establece que la aplicación corresponderá a los tribunales federales o provinciales, según si las cosas o las personas cayeren bajo sus respectivas jurisdicciones.[144] El objetivo es mantener una unidad y coherencia en cuanto al derecho de fondo, para evitar contradicciones, y al mismo tiempo respetar la autonomía de las provincias para delinear los códigos procesales para implementar ese derecho de fondo.

Esto quiere decir que el Código Penal es sancionado por el Congreso Nacional y se aplica en todo el país. Las provincias no pueden dictar sus propios códigos penales. Mientras que la reglamentación de estos códigos de fondo como los códigos procesales deberán ser dictados por cada jurisdicción.

Por todo esto, es difícil describir con precisión el marco de actores y órganos involucrados en la persecución penal de Argentina, y realizar un diagrama del procedimiento para interceptar una comunicación, ya que ambos aspectos irán variando según la jurisdicción que se analice. En todo caso, tomaremos como modelo el Código Procesal Penal Federal, que se aplica para delitos con jurisdicción federal ya que, a su vez, muchas de las regulaciones provinciales siguen el criterio del código federal.

Órganos involucrados en la persecución penal de su país

Órganos jurisdiccionales:[145]

- Jueces con funciones de revisión;
- Jueces con funciones de juicio;
- Tribunales de Jurados;
- Jueces con funciones de garantías;
- Jueces con funciones de ejecución.

Ministerio Público Fiscal.[146]

- Las fuerzas de seguridad actúan como auxiliares de la justicia asistiendo a los órganos involucrados en la persecución penal.[147]

5.2 Diagrama de Proceso Penal Para Interceptar una Comunicación

El Código Procesal Penal Nacional establece el siguiente procedimiento para interceptar una comunicación:

- El juez podrá ordenar, a petición de parte, la interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a éste, si tal interceptación resulta útil para la comprobación del delito.[148] Se procederá de modo análogo al allanamiento.
- La intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo máximo de treinta (30) días. Este plazo puede renovarse si se expresan motivos que justifiquen la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado.[149]
- La solicitud para intervenir comunicaciones debe indicar el plazo de duración que se estime necesario según las circunstancias del caso.[150]
- El juez debe controlar la legalidad y razonabilidad del requerimiento, y resolver fundadamente.
- Aquellos funcionarios encargados de efectuar la intervención tienen un deber de confidencialidad y secreto respecto de la información obtenida por estos medios, excepto respecto de la autoridad que la haya requerido. Si se incumple este deber de confidencialidad, el funcionario incurrirá en responsabilidad penal.[151]
- Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.[152]
- Debe interrumpirse la intercepción si los elementos de convicción tenidos en

consideración para ordenar la medida desaparecieran, o una vez que hubiere transcurrido su plazo de duración o ésta hubiere alcanzado su objeto.

5.2.1 Incautación de Datos

- El juez podrá ordenar, a requerimiento de parte, y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación.[153]
- El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó.[154]
- Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos.[155]
- El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos.[156]

5.2.2 Apertura de los Efectos Interceptados

- Una vez recibida la correspondencia o los efectos interceptados, el representante del Ministerio Público Fiscal procederá a su apertura. Examinará los objetos y leerá el contenido de la correspondencia.[157]
- El representante del Ministerio Público Fiscal debe explicar, en una audiencia unilateral, los fundamentos por los cuales solicita mantener el secuestro de los objetos que tuvieran relación con el proceso. [158]
- Sobre el resto de los efectos, el juez mantendrá la reserva del contenido y dispondrá la entrega al destinatario o a sus representantes o parientes próximos, bajo constancia.[159]

Por otro lado, la Ley 25.520 de Inteligencia Nacional establece que la Agencia Federal de Inteligencia tiene la potestad de producir inteligencia criminal. Eventualmente puede solicitar la interceptación de comunicaciones referida a los delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, ciberdelitos. También puede hacerlo contra delitos atentatorios del orden económico y financiero, así como delitos contra los poderes públicos y el orden constitucional, con medios propios de obtención y reunión de información. Este proceso se desarrollará más adelante.

5.3 Organigrama de los Órganos Inteligencia

A partir de la ley 27.126 que modifica a la Ley de Inteligencia Nacional, el sistema de inteligencia en Argentina está constituido, en primer lugar por la Agencia Federal de Inteligencia (AFI).

La AFI es la autoridad máxima en materia de inteligencia en Argentina y dirige al resto de los organismos que lo integran.[160] La AFI depende, directamente, del Poder Ejecutivo Nacional—de hecho, la autoridad superior del Sistema de Inteligencia Nacional es el Presidente de la Nación y es quien tiene a su cargo la formulación de la política de Inteligencia Nacional.[161] La AFI es conducida por un Director General, con rango de ministro cuya designación está a cargo del Poder Ejecutivo con acuerdo del Senado.[162]

Según la Nueva Doctrina de Inteligencia Nacional, una normativa reciente que complementa a la ley 27.126 y da lineamientos en materia de inteligencia, las funciones de la AFI tienen que ver con:

- La producción de inteligencia nacional mediante la obtención, reunión y análisis de la información referida a los hechos, riesgos y conflictos que afecten la defensa nacional y la seguridad interior, a través de los organismos que forman parte del sistema de inteligencia nacional.
- La producción de inteligencia criminal referida a los delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, ciberdelitos, y atentatorios contra el orden económico y financiero, así como los delitos contra los poderes públicos y el orden constitucional, con medios propios de obtención y reunión de información.[163]

Los otros organismos que componen el sistema de inteligencia argentino son:

- La Dirección Nacional de Inteligencia Criminal (DINICRI), que depende del Ministerio de Seguridad.[164] La DINICRI tiene como función la producción de inteligencia criminal,[165] salvo la vinculada a delitos federales complejos o delitos contra los poderes públicos y el orden constitucional. Estas funciones fueron transferidas directamente a la AFI.[166]
- La Dirección Nacional de Inteligencia Estratégica Militar (DINIEM), dependiente del Ministerio de Defensa de la Nación.[167] La DINIEM tiene a su cargo la producción de inteligencia estratégica operacional y la inteligencia táctica necesarias para el planeamiento y conducción de operaciones militares y de la inteligencia técnica específica.[168]

5.4 Proceso de los Cuerpos de Inteligencia para Interceptar Comunicaciones

De acuerdo al artículo 4 de la ley 27.126 que modifica la Ley de Inteligencia Nacional, "las actividades de inteligencia serán ordenadas por las máximas autoridades de cada organismo." Este artículo agrega, sin embargo que, "en caso de urgencia" estas actividades "podrán ser

iniciadas, debiendo ser informadas de manera inmediata a las autoridades máximas de cada organismo de inteligencia."

A la hora de realizar interceptaciones en las comunicaciones privadas, la AFI, el organismo máximo del Sistema Nacional de Inteligencia desde la ley 27.126, debe solicitar la autorización judicial."[169] Esta autorización, señala el marco normativo, "deberá formularse por escrito y estar fundada indicando con precisión el o los números telefónicos o direcciones electrónicas o de cualquier otro medio, cuyas comunicaciones se pretenda interceptar o captar."[170]

La autorización judicial será requerida al juez federal penal con competencia jurisdiccional por el Director General de la AFI o el funcionario en quien se delegue esta facultad. La jurisdicción se establece de acuerdo al domicilio de las personas físicas o jurídicas cuyas comunicaciones van a ser interceptadas o desde la sede donde se realizarían, en caso que se trate de comunicaciones móviles o satelitales.

La autorización para la interceptación de comunicaciones será concedida por un plazo no mayor de 60 días que caducará automáticamente, salvo que, ante el pedido formal del Director de la AFI o del funcionario que esté ejerciendo esa facultad, el juez otorgue una extensión del plazo por otros 60 días como máximo (siempre que sea imprescindible para completar la investigación).[171]

Una vez que se vencen estos plazos, el juez ordenará la iniciación de la causa correspondiente o, en caso contrario, la destrucción de los elementos que permitan dar cuenta del resultado de las interceptaciones.[172]

Con la aprobación de la ley 27.126, la antes denominada Dirección de Observaciones Judiciales (DOJ), el único órgano del Estado encargado de llevar adelante interceptaciones o captaciones de comunicaciones privadas, se transfirió al ámbito de la Procuración General de la Nación del Ministerio Público, un órgano independiente con autonomía funcional y autarquía financiera. A partir de este traspaso, la DOJ pasó a denominarse Departamento de Interceptación de Captación de las Comunicaciones (Dicom).[173]

Las órdenes judiciales para la interceptación de las comunicaciones telefónicas debían ser enviadas al Dicom con instrucciones precisas para orientar dicha tarea (por ejemplo, los números a ser intervenidos). Después, el Dicom debe enviar ese pedido a la empresa de servicios telefónicos responsable de ejecutar la derivación de la comunicación.

Con estas nuevas normativas, no sólo se transfirió a la Procuración General el sistema operativo, sino también las bases de datos informáticas y los archivos documentales del

organismo anterior con el material de las intervenciones concluidas al momento del traspaso.

La normativa, asimismo, creaba una Comisión de Administración de Registros de Intervenciones Concluidas y se pondrán bajo su custodia los archivos vinculados a intervenciones de comunicaciones finalizadas antes del traspaso.

Como señalamos antes, en diciembre de 2015, el recientemente asumido presidente Macri, ordenó a través de un decreto de necesidad y urgencia el traspaso del DICOM a la esfera de la Corte Suprema de Justicia de la Nación. Según este decreto, el Ministerio Público[174] es parte principal en el proceso de investigación y persigue un interés determinado. Por este motivo, y con el fin de garantizar el debido proceso legal, la ejecución de las órdenes de intervención de las comunicaciones deberían ser llevadas a cabo por un organismo distinto al que es parte en la investigación. En este caso -establece el decreto -la Corte Suprema.[175]

La Corte decidió postergar hasta febrero de 2016 el traspaso de este organismo a su esfera.[176] Al oficializar la transferencia mediante una acordada, lo Corte renombró como Dirección de Captación de Comunicaciones del Poder Judicial de la Nación (DCCPJ).

Esta decisión de la Corte señala que las actividades de interceptación de comunicaciones se realizarán sujetandose al marco de la ley de telecomunicaciones, la Ley Federal de Inteligencia y ley Argentina Digital a las que hicimos referencia en las secciones anteriores. De acuerdo a esta decisión, la Corte Suprema retiene la autoridad para cambiar la regulación del DCCPJ.

En la misma decisión, se desarrollan los principios que, según la Corte, deben guiar la interceptación de comunicaciones:

1. Transparencia y confidencialidad: la acordada señala que se debe establecer un mecanismo de supervisión eficiente y exige una obligación de confidencialidad para los empleados que trabajan en la DCCPJ. También ordena la elaboración de un documento destinado a garantizar la "cadena de custodia" que proteja la confidencialidad de la información obtenida a través de las interceptaciones.

2. Capacitación: los responsables de las interceptaciones a las comunicaciones deben ser entrenados en el conocimiento y uso de los mecanismos y tecnologías más eficientes así como en lo que tiene que ver con evaluar la "oportunidad" y la duración de las interceptaciones. La norma establece que los miembros de la DCCPJ podrían asistir a jueces y fiscales directamente en sus oficinas o "a distancia."

3. Minería de datos: este reglamento establece la necesidad de una actualización a las prácticas de minería de datos (*data mining*) en los datos de vigilancia. En particular, indica que los intentos de hallar patrones en los "grandes volúmenes de datos" son una manera de ayudar a jueces y fiscales en los procedimientos.

4. Nuevas tecnologías: esta decisión señala que se procurará la utilización de las nuevas tecnologías y que las mejores prácticas de otras instituciones judiciales alrededor del mundo deben ser estudiadas y copiadas.

5. Relación con empresas de telecomunicaciones: la acordada establece que las autoridades del organismo acordaran protocolos de confidencialidad, auditorias compartidas, tecnologías actuales futuras con las empresas de telecomunicaciones otras que brinden servicios utilizables.[177]

La DCCJ, que mantendrá autonomía con respecto a la Corte, tendrá un Director General —un juez penal con rango de Juez de Cámara— por un periodo de un año no renovable. Asimismo, el organismo contará con un directorio aunque no da mayores precisiones de cómo sus integrantes serán seleccionados.

Junto con el traspaso de las interceptaciones al ámbito del Ministerio Público Fiscal y la creación de la DICOM se había impulsado, asimismo, la creación de una comisión asesora integrada por expertos en la materia y un consejo consultivo de instituciones y organizaciones de la sociedad civil a fin de buscar mecanismos para asegurar la transparencia y la participación.

En la acordada de la Corte que crea la DCCPJ no se hace referencia a mecanismos de participación de la sociedad civil y la academia o instancias externas de supervisión.[178] De todas formas, cabe señalar que quedan aspectos del reglamento del organismo pendientes de ser definidos por la Corte.

Según la acordada de la corte que crea esta dirección, la DCCPJ será el único órgano del Estado encargado de ejecutar las interceptaciones o captaciones privadas de cualquier tipo, "que fueran requeridas por los magistrados judiciales y los del Ministerio Público Fiscal" , en línea con los principios descriptos anteriormente. Si bien en varios de sus artículos la misma acordada señala que las interceptaciones serán a partir de la orden de la autoridad judicial competente, organizaciones de la sociedad advirtieron sobre la ambigüedad de la redacción de esta frase en tanto "podría dar lugar a la interpretación de que el Ministerio Público Fiscal tiene la potestad de solicitar directamente a la DCCJ la intervención de una determinada comunicación, sin la necesidad de obtener una orden judicial previa."[179] La Asociación por los Derechos Civiles, por ejemplo, planteó que esta redacción debería reformularse a fin de llevar a confusiones que afecten el debido proceso.

En el mismo documento, la ADC además llama la atención sobre la utilización del término minería de datos en la acordada: "La introducción del concepto de minería de datos nos resulta en este sentido muy reveladora: da cuenta de prácticas que sospechamos existen pero que no están adecuadamente reguladas en ninguna de las normas, de cualquier nivel, que regulan una actividad del Estado que por definición viola derechos de los ciudadanos."[180]

Resumiendo, a partir de estos cambios, el proceso para la interceptación de una comunicación quedaría de esta forma:

- Solicitud de la AFI
- Autorización judicial (juez federal penal con jurisdicción)
- Dirección de Captación de Comunicaciones del Poder Judicial de la Nación (DCCPJ), Corte Suprema de Justicia de la Nación

6.

Formas de Control

6.1 Entidades Autorizadas Para Intervenir Una Comunicación Privada Sin Orden Judicial

De acuerdo con la normativa penal y la normativa de actividades de inteligencia desarrolladas en secciones anteriores, no podría interceptarse una comunicación sin una orden judicial.

6.2 Obligación de Reportes de Transparencia y Supervisión Pública

En el proceso penal de interceptación de comunicaciones no se prevé una obligación de realizar reportes de transparencia. En el proceso de inteligencia, se contempla la obligación del órgano de inteligencia de elaborar informes anuales secretos de actividades de inteligencia, que debe presentar ante la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia.[181] A continuación, desarrollaremos las funciones que debe llevar a cabo esta Comisión de supervisión.

6.2.1 Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia

Este órgano de control parlamentario fue creado en 2001, cuando se promulgó la Ley de Inteligencia Nacional 25.520. Según esta ley, las funciones de la Comisión incluyen supervisar a los organismos del Sistema de Inteligencia Nacional, fiscalizar su funcionamiento para que se ajuste estrictamente a las normas constitucionales y legales, y controlar a las actividades de inteligencia.[182] Esto último abarca la consideración, análisis y evaluación de la ejecución del Plan de Inteligencia Nacional; la consideración del Informe Anual de las Actividades de Inteligencia; la elaboración y remisión en forma anual al Poder Ejecutivo Nacional y al Congreso de la Nación de un informe secreto sobre el análisis y evaluación de las actividades, funcionamiento y organización del Sistema de Inteligencia Nacional en función de la ejecución del Plan de Inteligencia Nacional, entre otras funciones.[183] La ley otorga a la Comisión "amplias facultades para controlar e investigar de oficio." Sin embargo, la ley impone una limitación, en tanto "el acceso a dicha información será autorizado en cada caso por el Presidente de la Nación o el funcionario en quien se delegue expresamente tal facultad, con las excepciones previstas en la presente ley."[184] Esta disposición supedita el control de la Comisión a la voluntad del mismo controlado.[185]

La Comisión comenzó a funcionar en 2004, cuando se le asignaron fondos para comenzar sus funciones.[186] En la práctica, se ha afirmado que funciona con un total secretismo, hasta en las cuestiones que no son, o no deberían ser secretas.[187] Por ejemplo, en su página web, no figura información sobre las reuniones de la Comisión ni su agenda de trabajo.[188]

A fines de diciembre de 2012, un grupo de organizaciones de la sociedad civil, parte de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI), presentaron un pedido de acceso a la información ante la Comisión Bicameral.[189] En ese documento, solicitaron información sobre las reuniones de la Comisión, copias de los informes realizados por la Comisión que no sean secretos, si ha realizado investigaciones de oficio en relación a presuntas irregularidades en el ejercicio de la actividad de inteligencia, entre otras cuestiones. A pesar de haber sido reiterado dos veces, el pedido no ha sido respondido hasta el cierre de este informe.[190]

En febrero de 2015 se reveló que la Comisión se reunió a puertas cerradas para analizar el proyecto de reforma a la Ley de Inteligencia.[191]

Como señalábamos antes, la resolución que daba origen al DICOM, constituía una comisión asesora integrada por expertos en la materia einstaba a la creación en el Congreso de una Comisión Bicameral del Ministerio Público que funcione como una instancia de control externo sobre el funcionamiento del DICOM.

Con el traspaso de las interceptaciones a la Corte Suprema y la creación de la DCCPJ no se establecen mecanismos independientes de supervisión pública para garantizar la transparencia y la rendición de cuentas. De todas formas, y como señalamos antes, al momento de terminar este informe quedan aspectos del reglamento del organismo pendientes de ser definidos por la misma.

6.3 Mecanismos de Notificación Diferida

Tanto el proceso penal como el procedimiento de inteligencia para interceptar comunicaciones privadas carecen de un mecanismo de notificación diferida al usuario afectado.

En el proceso penal, solamente en los casos de allanamiento, o de incautación de un sistema informático, el afectado recibe una notificación. Sin embargo, en los casos de interceptación de comunicaciones privadas, si esas comunicaciones interceptadas no terminan utilizándose en una causa penal, el afectado podría no enterarse nunca de que su comunicación fue interceptada.

7.
Aplicación de la Ley y Diseños Institucionales

A lo largo de los últimos años, han tenido lugar en Argentina distintos episodios relacionados con la vigilancia e interceptación de las comunicaciones. Espionaje a e-mails de periodistas y jueces.

Por ejemplo, en 2006 y a raíz de una investigación periodística trascendió públicamente que se habían violado correos electrónicos de periodistas y jueces.[192] Este hecho tuvo un impacto en lo que después fue la promulgación de la ley 26.388, que incorporó al Código Penal muchos de los delitos informáticos desarrollados previamente.

Si bien había habido numerosos intentos previos similares para modificar el Código para incluir estos delitos, fue este episodio específico el que aumentó el impulso de esta ley en tanto la violación de correos electrónicos, en ese entonces, no estaba tipificada. Esta situación puso en evidencia los vacíos que tenía el Código Penal en materia de delitos informáticos, y poco después se aprobó la reforma.[193]

7.1 Causa por Escuchas Ilegales en la Ciudad de Buenos Aires

Este caso reviste gravedad institucional en tanto el jefe de gobierno de la Ciudad de Buenos Aires y actual presidente del país, Mauricio Macri, está procesado desde 2010 en esta causa por ser "partícipe necesario de una asociación ilícita" dedicada al espionaje ilegal.[194]

En la decisión del tribunal se responsabiliza al jefe de gobierno porteño por participar del armado de una “estructura de inteligencia subterránea" en la Ciudad de Buenos Aires y se lo imputa por escuchas telefónicas ilegales denunciadas, entre otros, por su ex cuñado y dirigentes de familiares de víctimas de la AMIA opositores al gobierno porteño.[195] En la misma causa, está procesado y aguardando juicio, entre otros, un ex jefe de la Policía Metropolitana de la Ciudad de Buenos Aires.

7.2 Proyecto X

Uno de los escándalos más grandes del último tiempo en materia de vigilancia. El denominado “Proyecto X,” implementando desde 2005 y descubierto en 2012, comprendía actividades de recolección y sistematización de información de inteligencia llevadas adelante por la Gendarmería Nacional. Actividades que, a contramano del marco legal analizado en

secciones anteriores, no estaban enmarcadas en ninguna causa judicial, ni autorizadas por un juez ni se rindió cuenta de ellas ante la Comisión Bicameral encargada de auditar las actividades de inteligencia.

Proyecto X, cuya existencia fue reconocida por la entonces ministra de Seguridad de la Nación como por el jefe de gendarmería, consistía en una base de datos con información sobre organizaciones sociales, ambientalistas, familiares de víctimas de la represión, movimientos sociales, sindicatos y organismos de derechos humanos.[196]

Proyecto X consistía en tareas de espionaje en las que efectivos de Gendarmería que se infiltraban en manifestaciones y en protestas de organizaciones opuestas al Gobierno.[197] A raíz de estas protestas, se realizaban denuncias judiciales contra los manifestantes, basadas en la información aportada por los agentes infiltrados.

El que, según la ex ministra de Seguridad no era espionaje sino, en realidad, "sólo un software"[198] iba en contra, por ejemplo, de la prohibición establecida por la ley de Inteligencia Nacional, antes analizada, que impide a las fuerzas de seguridad la producción de inteligencia o el almacenamiento de datos sobre las personas por su opinión política o por su adhesión o pertenencia a organizaciones sociales, sindicales, partidarias, comunitarias, etc. Asimismo, Proyecto X contradecía el marco jurídico establecido por la ley de protección de datos personales que impide recoger datos "por medios desleales, fraudulentos;"[199] almacenar "datos sensibles"[200] como los que revelan "opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical."[201]

En la actualidad, existe una causa en trámite vinculada a esta iniciativa en la que se investiga si la tarea ejercida por Gendarmería fue o no ilegal. El expediente se encuentra en la etapa de instrucción y, hasta el momento, no se ha indagado a nadie.

7.3 Compra de Equipamiento para Vigilancia de las Comunicaciones

A raíz de un pedido de información realizado por parlamentarios alemanes, trascendió que Argentina compró a ese país equipamiento para vigilancia electrónica. Este caso da cuenta de la falta de transparencia en relación a las actividades de vigilancia en tanto, hasta ahora, las características, los fines de este equipamiento o qué organismo habría sido su destinatario se mantienen en secreto.[202]

Asimismo, en las recientes filtraciones de WikiLeaks[203] trascendió que existieron contactos con Hacking Team para la posible compra de software de espionaje. De este material se desprende que hubo presentaciones de los productos de la empresa italiana ante organismos públicos argentinos dedicados a tareas de inteligencia. Como en el caso de las compras de

equipamiento, hasta el momento no existe información más concreta ni una declaración oficial al respecto.

7.4 La Muerte del Fiscal Nisman y la Reforma al Sistema de Inteligencia

Sin embargo, el caso más reciente ha sido la muerte en enero de 2015 de Alberto Nisman,[204] el fiscal a cargo de la causa por el atentado contra la Asociación Mutual Israelita Argentina (AMIA) en 1994. Nisman, la noche antes de presentarse ante el Congreso para presentar su denuncia contra la Presidenta por encubrimiento en la causa, fue encontrado muerto en su departamento.

Una investigación del experto en seguridad del portal *The Intercept*, Morgan Marquis-Boire, señaló que Nisman fue atacado por un software espía (*malware*) descargado en su teléfono celular poco antes de su misteriosa muerte.[205] Marquis-Boire explica que el malware fue ocultado bajo un documento .PDF que decía confidencial y tenía la intención de infectar un ordenador con Windows. Sin embargo, Nisman abrió el archivo desde su teléfono Android por lo cual no llegó a infectarse.[206] Según el diario, The Intercept, se desconoce si Nisman abrió el archivo desde su computadora. Agrega Marquis-Boire, que el ataque no fue un hecho aislado y que las persona o personas que aparecen detrás del intento de vigilancia también han ejecutado otras operaciones desde distintos lugares de América del Sur a otros objetivos como el periodista Jorge Lanata.

Una de las consecuencias de la muerte del fiscal fue poner en la mira y en el debate público el funcionamiento de los servicios de inteligencia en Argentina.[207] Poco tiempo después de la muerte del fiscal y en medio de declaraciones de distintos sectores de la política argentina, que asociaban a los servicios de inteligencia con el hecho,[208] la Presidenta presentó, a través de una cadena nacional, un proyecto para reformar el sistema de inteligencia, en tanto "no ha servido a los intereses nacionales."

Este proyecto dio lugar a los cambios desarrollados en este informe en materia de inteligencia: la disolución de la Secretaría de Inteligencia, la creación de una Agencia Federal de Inteligencia, la transferencia de las escuchas telefónicas a la Procuración Nacional, entre otros.

8.

¿Respeta Argentina los Estándares Internacionales de Derechos Humanos Frente a la Vigilancia Estatal?

Legalidad

> *Este principio requiere que cualquier limitación a los derechos humanos deba ser prescrita por ley, que deberá ser precisa y clara, para asegurar que las personas la conozcan por adelantado.*

Las interceptaciones a las telecomunicaciones en el régimen penal y de inteligencia deben realizarse conforme a la Constitución Nacional, los tratados de derechos humanos suscriptos por la Argentina y las disposiciones previstas en leyes y códigos. Ambos cuerpos normativos detallan el procedimiento para ordenar la interceptación de una comunicación y qué funcionarios pueden autorizarlas. En este sentido, cumplen con el requisito de legalidad.

Sin embargo, cuestiones que aparecen en el marco regulatorio en materia de inteligencia podrían derivar en acciones discrecionales por parte del Estado. Por ejemplo, la ley de inteligencia nacional establece que son las "autoridades máximas" de cada organismo del sistema de inteligencia las que ordenan estas actividades. De todas formas, señala que "en caso de urgencia" estas actividades podrán iniciarse, debiendo ser informadas de manera inmediata a esas máximas autoridades.[209] Consideramos que el hecho de no definir taxativamente qué se entiende por "caso de urgencia" podría derivar en acciones que vulneren derechos fundamentales.

La misma amplitud y falta de precisión en ciertas definiciones aplica para la nueva doctrina en materia de inteligencia. La nueva doctrina emana de un decreto del Poder Ejecutivo y, por lo tanto, no fue discutido en el Congreso ni hubo debate público al respecto. La nueva doctrina amplía los denominados atentados contra el orden constitucional lo que podría ser problemático en términos de legalidad en tanto no están definidos claramente. La misma falta de precisión se le puede objetar cuando se refiere a las actividades de inteligencia en la investigación por el uso fraudulento y la difusión ilegal de contenidos, por ejemplo.

La actual regulación sobre telecomunicaciones también incluye cuestiones vagas y amplias que podrían ser peligrosas y podrían abrir la puerta a prácticas de vigilancia en las comunicaciones.

La ley "Argentina Digital" establece, por un lado, el marco general en materia de Tecnologías de la Información y Comunicación (TIC). Por otro lado, establece la inviolabilidad de las comunicaciones realizadas a través de las redes y servicios de telecomunicaciones. Y señala que la interceptación de las comunicaciones, así como su posterior registro y análisis, sólo podrá realizarse mediante el requerimiento de un juez competente.[210] Hasta aquí cumple con el principio de legalidad.

Pero, en otro de sus artículos, establece obligaciones para los usuarios de los denominados servicios TIC que podrían ir contra de esa premisa y del principio de legalidad. Como analizamos antes, establece como una obligación que los usuarios deberán permitir el acceso del personal de las empresas que proveen servicios TIC y del ENACOM (ex AFTIC) "a los efectos de realizar todo tipo de trabajo o verificación necesaria."[211]

La resolución podría representar un problema para este principio de legalidad en tanto contiene cuestiones muy amplias. Por ejemplo, los prestadores de servicios de telecomunicaciones deberán garantizar "el libre acceso a sus redes y a su información" al organismo público encargado de aplicar el marco de telecomunicaciones, y deberán brindar toda la información que les sea requerida y que este organismo "estime pertinente."[212]

Lo mismo se puede aplicar a la Ley 25.891 de Servicios de Comunicaciones Móviles. Esta ley obliga a los prestadores de conexión móvil a recolectar, retener y divulgar datos personales sin establecer de manera clara los límites ni las finalidades de la recolección, ni qué tipo de datos se están recolectando. Simplemente obliga a compartir "toda la información sobre clientes y usuarios."

Por lo menos, cabe señalar que estas normativas no son claras, son amplias, carecen de precisión y podrían avalar procedimientos discrecionales por parte de la autoridad contrarios a los estándares internacionales en materia de privacidad.

Objetivo Legítimo

> *Las interceptaciones a las comunicaciones deben estar justificadas de forma que cumplan un objetivo legítimo que corresponda a un interés jurídico preponderante, importante y necesario en una sociedad democrática. Las normas que permiten la vigilancia de las comunicaciones no pueden basarse sobre condiciones como raza, sexo, idioma, religión, opinión política, nacionalidad, entre otros.*

En principio, el régimen legal argentino que prevé interceptaciones a las comunicaciones cumple con este requisito, en tanto establece que las interceptaciones serán realizadas de forma excepcional, con el objetivo de comprobar delitos complejos o de asegurar la defensa nacional y la seguridad interior.

De todas formas, como analizamos antes, el nuevo marco que regula las actividades de inteligencia en Argentina amplía los actos que pueden ser considerados contra el orden institucional y el sistema democrático y que serían objeto de actividades de inteligencia. Como dijimos, esta ampliación podría incentivar nuevas prácticas estatales que podrían ser peligrosas en términos de vigilancia y ejercicio de derechos humanos y pondría en cuestión este principio de objetivo legítimo.

En cuanto al marco de telecomunicaciones, las obligaciones de retención de información por los prestadores de servicios no se encuentran debidamente justificados. Solo esgrimen motivos como el cálculo de indicadores de calidad y permiten a la autoridad de aplicación conservarlos "por el lapso que considere conveniente."[213] Tampoco justifica debidamente con qué fines más allá de los antes mencionados estándares de calidad del servicio.

En materia de telecomunicaciones tampoco se cumple con este principio. Esta norma obliga a los usuarios a permitir el acceso de la autoridad de aplicación a los fines de realizar "todo tipo de trabajo o verificación necesaria" sin dar precisiones sobre qué tipo de trabajo, qué tipo de verificación y con qué fines;[214] También obliga a los prestadores de servicios de conexión móviles a informar a la autoridad sobre "toda información" sobre usuarios y clientes del servicio sin dar cuenta cabalmente en el texto de la ley de cuáles serían los fines que justifican este tipo de medidas.[215]

Los nuevos sistemas de recolección de datos analizados en este documento como SUBE, SIBIOS y el DNI, surgidos de normativas que tampoco fueron discutidas públicamente tampoco se ajustan a este principio en tanto no están debidamente justificados sus objetivos. Bajo la muy amplia idea de brindar mayor seguridad, prevenir el delito o simplificar y mejorar los trámites[216] se están recabando y tratando datos biológicos, biográficos y de la rutina diaria de transporte y consumo de la ciudadanía sin mayor transparencia.

Y, más allá que la normativa de datos personales y la de inteligencia prohíben obtener información, producir inteligencia y almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, y opiniones y actividades políticas. Existen ejemplos como el Proyecto X que dan cuenta que esas prácticas sí se implementan por parte de las fuerzas de seguridad en Argentina, a contramano de lo establecido en el marco legal.

Necesidad

> *Las interceptaciones a comunicaciones privadas deben realizarse de forma estricta y limitarse a lo necesario para alcanzar dicho objetivo legítimo. Esto significa que la vigilancia debe ser el único medio para alcanzar ese objetivo, o el que menos vulnere derechos humanos.*

En el procedimiento penal para la interceptación de comunicaciones se establece la excepcionalidad de la interceptación de comunicaciones, y el deber del juez de analizar que el requerimiento de interceptación cumpla con la legalidad y la razonabilidad.

El marco legal sobre inteligencia nacional señala que cuando en el desarrollo de las actividades de inteligencia sea "necesario" realizar una interceptación de comunicaciones esta deberá ser solicitada a una autoridad judicial.[217] Pero, en tanto no da más especificaciones sobre cuándo se consideraría "necesario" recurrir a este procedimiento, ni que solicitaron interceptaciones en tanto no existan otros medios que —permitiendo alcanzar los mismos fines— sean menos lesivos para los derechos humanos. En este sentido no se ajustaría a este principio.

De todas formas, el marco de inteligencia establece cuestiones vinculadas a este principio en tanto solo se podrá realizar una interceptación de una comunicación mediante una orden judicial que debe estar formulada por escrito y debe indicar con precisión los números telefónicos o direcciones electrónicas que se pretendan interceptar o captar.[218] La ley de inteligencia nacional también establece que sus actividades se enmarcarán "inexcusablemente" dentro de lo que establece el marco regulatorio de protección de datos personales en Argentina[219] y establece un plazo máximo para la autorización a interceptar una comunicación.[220]

El marco legal en materia de telecomunicaciones reafirma la idea de inviolabilidad de las comunicaciones y que cualquier interceptación deberá realizarse solo con una orden judicial[221] ajustándose a este principio de necesidad, pero normativas que componen el cuerpo legislativo en la materia contradicen este principio en tanto establecen que los prestadores de servicios deberán entregar datos de los usuarios a pedido de la autoridad de aplicación y por el tiempo que esta considere necesario.[222]

Adecuación

> *La vigilancia de las comunicaciones prevista en la ley debe ser apropiada e idónea para cumplir el objetivo legítimo específico identificado.*

El régimen de interceptación de comunicaciones en una causa penal prevé la necesidad de que la interceptación sea útil para comprobar un delito.

Por su parte, la regulación de inteligencia se ajusta a este principio al establecer que los datos recabados por medio de las actividades de inteligencia que no sirvan para los fines establecidos por ese marco regulatorio —es decir, la producción de información tendiente a prevenir los riesgos para la seguridad interior y la defensa nacional; y lo que tiene que ver con sus funciones de investigación e inteligencia criminal vinculada a delitos federales complejos— serán destruidos. La ley de inteligencia señala, asimismo que no se debe almacenar información por motivos de raza, creencias religiosas, acciones privadas, actividades políticas, pertenencia a organizaciones sociales, entre otras.[223]

En materia de telecomunicaciones, como venimos señalando, parte de la legislación que integra el marco normativo no se ajusta por completo a este principio en tanto, no establece un plazo máximo de retención de datos personales.[224] A contramano de lo que sí aparece en la ley de datos personales que, en su artículo 4, señala que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular y que deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que fueron recolectados.

Proporcionalidad

> *Para que la vigilancia de comunicaciones privadas sea proporcional, es necesario que el Estado deba demostrar a una autoridad judicial competente, a los fines de llevar a cabo vigilancia de comunicaciones, ciertos requisitos:*
>
> 1. *Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo, y;*
>
> *En el ámbito penal este requisito no se cumple en tanto se requiere únicamente que la interceptación resulte útil para la comprobación de un delito, sin especificar si éste debe ser grave.*

En lo que tiene que ver con actividades de inteligencia, se pueden solicitar a una autoridad judicial interceptaciones a las comunicaciones dentro del amplio marco de facultades del organismo de inteligencia nacional—desde lo que tiene que ver riesgos para la seguridad interior y la defensa nacional hasta la investigación de delitos federales complejos como narcotráfico hasta corridas bancarias.

> 2. *Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la Información Protegida, y;*

Este requisito no se cumple en el proceso penal ni en el marco que regula las actividades de inteligencia. En el proceso penal, solamente se exige que la información sea útil, y no que haya sólidos indicios que se accederá a evidencia pertinente. Como señalamos antes, se puede solicitar la captación de comunicaciones en el marco del desarrollo de las actividades de inteligencia. También mencionamos que es muy amplio el abanico de actividades de inteligencia comprendidas, lo que puede resultar problemático.

> 3. *Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica. Y;*

Si bien en el ámbito penal se especifica que la interceptación de comunicaciones debe ser excepcional, no se menciona específicamente que haya que agotar otras técnicas de investigación previamente. En cuanto al marco regulatorio en materia de inteligencia, éste tampoco señala que hay que agotar otras técnicas menos lesivas para los derechos humanos.

> 4. *La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza específica al fin legítimo alegado; y*

En el ámbito penal, la interceptación de comunicaciones se remite a las normas para allanamiento de morada, que prevén limitar el registro exclusivamente a los elementos que estén relacionados con el objeto que se busca. Este principio se cumple en lo que tiene que ver con la regulación de las actividades de inteligencia.

> 5. *Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud; y*

El régimen penal prevé el deber de confidencialidad y secreto en las interceptaciones de comunicaciones, y en el caso de incautación de datos prevé la devolución de aquellos componentes que no tengan relación con el proceso. La regulación en materia de inteligencia establece un plazo máximo para la interceptación de las comunicaciones y que los datos recabados que no sirvan para los fines establecidos por el marco que regula esta actividad, serán destruidos.[225]

> 6. *La información será accesada solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y*

La normativa penal contempla estos requisitos, en tanto prevé la devolución de los datos incautados y la interrupción de la interceptación una vez cumplido el plazo o cumplido el objetivo.

La normativa de inteligencia se ajusta a este principio en tanto establece que el personal afectado a las actividades de inteligencia, la documentación y los bancos de datos de los organismos de inteligencia "llevarán la clasificación de seguridad que corresponda en interés de la seguridad interior, la defensa nacional y las relaciones exteriores de la Nación. El acceso a dicha información será autorizado en cada caso por el Presidente de la Nación o el funcionario en quien se delegue expresamente tal facultad", con las excepciones que prevé esa ley."[226]

Asimismo, se ajusta a este principio en tanto señala que no se deberá almacenar información por motivos de raza, creencias religiosas, acciones privadas, actividades políticas, pertenencia a organizaciones sociales, entre otras.[227]

7. *Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.*

La normativa penal prevé la protección de la privacidad y la intimidad al imponer un deber de confidencialidad a los funcionarios que realizan las intervenciones respecto de la información obtenida, bajo posible responsabilidad penal si lo incumple.

La ley de inteligencia nacional, como se explicó anteriormente, establece sanciones penales para aquellos integrantes de los servicios de inteligencia que indebidamente intercepten, capten o desvíen comunicaciones que no le estuvieran dirigidas.[228]

Por su parte, como vimos, en la normativa de telecomunicaciones, en cuanto a retención de datos incluye cuestiones amplias que pueden derivar en un proceder discrecional por parte de la autoridad de aplicación del marco de Tecnologías de la Información y Comunicación en Argentina. Por ejemplo, normativas que no establecen un plazo máximo de retención de datos personales, permiten un uso distinto de la finalidad con la que fueron recolectados, habilita la cesión de los mismos, entre otros.

Autoridad Judicial Competente

Este principio establece la necesidad de que las decisiones sobre vigilancia de comunicaciones sean tomadas por una autoridad judicial competente imparcial e independiente. Ésta debe estar separada y ser independiente de las autoridades encargadas de llevar a cabo la vigilancia, debe estar capacitada y ser competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las

> *comunicaciones, y tener recursos adecuados para el ejercicio de las funciones que se asignen.*

Este requisito se cumple, tanto en el ámbito penal como en el de actividades de inteligencia. Por su parte, en la ley Argentina Digital también se ajusta a este principio en su artículo 5 cuando señala que la interceptación de las comunicaciones sólo podrá tener lugar a requerimiento de un juez competente.

Sin embargo, como se señaló antes este principio no se cumple en artículos de otras leyes que componen el marco regulatorio en materia de telecomunicaciones. Por ejemplo, los reglamentos de calidad del servicio de telecomunicaciones y la ley de servicios de comunicaciones móviles antes mencionados.

Debido Proceso

> *Este requisito exige que los Estados respeten y garanticen el ejercicio de los derechos humanos de las personas. Deben asegurar que los procedimientos legales que rigen cualquier interferencia con derechos humanos garanticen una audiencia pública y justa, realizada dentro de un plazo razonable por un tribunal independiente, competente e imparcial. Sólo podría permitirse prescindir de una orden judicial cuando exista un riesgo inminente para la vida humana, y debe subsanarse de forma posterior.*

El régimen penal argentino garantiza, en líneas generales, el debido proceso. Sin embargo, en el caso de un allanamiento, se prevé la posibilidad de realizarlo sin orden judicial en ciertos casos. Estos incluyen casos de amenaza para la vida –caso acorde con este principio- pero además lo permite cuando "una o más personas han sido vistas mientras se introducían en una casa o local con indicios manifiestos de comisión de un delito." Esta excepción no es del todo precisa y permitiría desnaturalizar el requisito de autorización judicial.

La interceptación de las comunicaciones en el marco de las actividades de inteligencia prevén el debido proceso en tanto sólo pueden realizarse mediante una autorización judicial. Cabe recordar, de todas formas, que el marco regulatorio habilita que se inicien actividades de inteligencia en casos de "urgencia" —que, de todas formas, deberían ser informados de manera inmediata. Esto, consideramos, podría abrir una puerta a la vulneración de derechos en el marco de las actividades de inteligencia.

El marco de inteligencia, asimismo, establece un plazo máximo para la autorización de interceptación de comunicaciones. La autorización se podrá extender por otros 60 días como máximo, siempre que sea imprescindible para completar la investigación.[229]

La retención de datos, siguiendo alguna de las leyes y resoluciones que componen el marco de regulación de las telecomunicaciones no se ajusta del todo a este principio. Si bien, como mencionamos antes, la ley Argentina Digital señala que toda interceptación de las comunicaciones se realizará mediante una orden judicial y en el marco de una investigación, otras normas habilitan a un organismo del Poder Ejecutivo a acceder a datos personales, solicitar información sobre los usuarios y, entre otras cosas, alojarla por el tiempo que considere necesario. Todas estas cuestiones vulneran este principio.

Notificación del Usuario

> *Este principio establece la obligación de notificar al individuo cuyas comunicaciones sean interceptadas, con el tiempo suficiente para impugnar la decisión o buscar otras soluciones. Solamente podría retrasarse la notificación si esto pusiera en serio peligro la finalidad para la que se autoriza la vigilancia, o representa un riesgo inminente de peligro para la vida humana, la autorización para retrasar la notificación es otorgada por la autoridad judicial competente cuando se autoriza la vigilancia, y si se notifica al usuario tan pronto como el riesgo desaparece.*

Este requisito no se cumple en Argentina, ya que no está previsto en el marco normativo penal, ni en el régimen de actividades de inteligencia. No hay una obligación de informar al individuo, ni siquiera una vez concluida la interceptación.

Si de dicha interceptación surjan elementos relevantes para una investigación penal o de inteligencia, el sujeto podría eventualmente enterarse, si dichos elementos son presentados como prueba en un proceso penal. Sin embargo, podría ocurrir que de la interceptación no surgieran elementos relevantes o útiles para la investigación, en cuyo caso el individuo jamás se enteraría que sus comunicaciones fueron vigiladas.

Transparencia

> *Para cumplir con el requisito de transparencia respecto del alcance y la implementación de las leyes de vigilancia de las comunicaciones, los Estados deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.*

Este principio tampoco se cumple en el ordenamiento argentino. Si bien los organismos de inteligencia deben elaborar informes para la posterior fiscalización de la Comisión Bicameral, dichos informes no son públicos. Por lo tanto, no hay datos oficiales públicos sobre actividades de interceptación de comunicaciones.

Supervisión Pública

> *Este principio implica que los Estados deben establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones. Estos mecanismos de supervisión deben contar con facultades amplias para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado en cuanto a la vigilancia de comunicaciones. Deben establecerse, además, otros mecanismos de supervisión independientes adicionales a los existentes a través de otra rama del gobierno.*

Es positivo que exista una Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia cuyas amplias facultades de fiscalización permiten asegurar que los órganos que llevan a cabo actividades de inteligencia cumplan con normas constitucionales y respeten derechos humanos. Sin embargo, ésta Comisión ha sido criticada por organizaciones de la sociedad civil por operar con opacidad y secretismo. A pesar de que se han realizado pedidos de información sobre cuestiones de funcionamiento de la Bicameral, éstos no han sido respondidos.

No obstante el reglamento del organismo todavía está pendiente de ser determinado por la Corte, la acordada que crea la Dirección de Captación de Comunicaciones del Poder Judicial no establece mecanismos de supervisión externos. (Solo hace referencia a que existirá un organismo de auditoría a cargo de la corte, pero no brinda mayores detalles al respecto).

Más allá de esto, no se contempla, ningún mecanismo adicional independiente para la supervisión de actividades de inteligencia.

Integridad de las Comunicaciones y Sistemas

> *Para garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado.*

Nunca debe exigirse a priori a los proveedores de servicios la retención o la recopilación de datos. La mencionada Resolución que establece el Reglamento de Calidad de los Servicios de Telecomunicaciones, elaborado por la Secretaría de Comunicaciones, podría representar un problema para este principio.

Este reglamento señala que los prestadores de telecomunicaciones deben conservar, en archivos electrónicos y por un plazo mínimo de tres años, los datos recogidos por sus

sistemas que sirvieran de base para el cálculo de los indicadores de calidad establecidos por esta normativa. La autoridad de aplicación podrá luego requerir la entrega de tales datos. Si bien los datos recolectados serán utilizados solamente para los cálculos de indicadores de calidad, y el reglamento contempla el deber de respetar los datos personales, consideramos que esta facultad podría ser contraria a este principio.

Por otro lado, la guía de buenas prácticas en privacidad para el desarrollo de aplicaciones, si bien es orientativa y no es vinculante de la Dirección Nacional de Datos Personales (DNDP) es un paso positivo con vistas al cumplimiento de este principio en tanto insta a los diseñadores de aplicaciones a ser claros sobre el uso de sus datos y qué tipo de usos se hará y a poner en práctica los principios de *privacy by design* y *privacy by default*.

Garantías para la Cooperación Internacional

> *Este principio requiere que los acuerdos de cooperación internacional celebrados por los Estados garanticen que, cuando pueda aplicarse la legislación de más de un Estado, se adopten los estándares más protectores para las personas. Dichos acuerdos deben incluir también el principio de doble incriminación.*

Si bien debe analizarse cada acuerdo en particular, ante la falta de un acuerdo de cooperación específico, la ley de cooperación internacional en materia penal dispone el requisito de doble incriminación para que proceda la extradición de una persona.

Garantías contra el Acceso Ilegítimo

> *Este principio prevé que los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "whistleblowers" y medios de reparación a las personas afectadas.*
>
> *Además, las leyes deben establecer que después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados.*

Consideramos positivo que en el ámbito penal y en el de actividades de inteligencia se prevé la pena para la interceptación ilegal de comunicaciones o realización ilegal de actividades de inteligencia, con penas agravadas en caso de funcionarios públicos.

Respecto de la protección a los informantes o "whistleblowers", la normativa penal que criminaliza la publicación de comunicaciones privadas prevé una excepción para quienes hubieran obrado con "el propósito inequívoco de proteger un interés público."[230]

Por su parte, la Ley 25.520 de Inteligencia Nacional incorporó este año disposiciones penales para castigar a quien, participando en forma permanente o transitoria de las tareas reguladas en dicha ley, "indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos."[231]

Esta ley también tipifica el delito de quien, con orden judicial y estando obligado a hacerlo, "omitiere destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones."[232] Siguiendo lo que establece esta normativa, se castiga también a todo funcionario o empleado público que realice acciones de inteligencia prohibidas por las leyes.[233]

Por otra parte, en la normativa de inteligencia nacional no hay incentivos para que los agentes de inteligencia den a conocer públicamente información sobre prácticas que vulneran derechos fundamentales.[234]

9.
Recomendaciones

En cuanto a la legalidad

- El marco que regula las actividades de inteligencia debería precisar y acotar ciertas definiciones en lo que tiene que ver con atentados contra el orden constitucional a fin de no infringir este principio y que esto derive en prácticas de vigilancia contrarias a los estándares internacionales.
- En cuanto al ámbito de las telecomunicaciones, deben ser revisadas normativas y artículos de la ley Argentina Digital que permitirían un uso de los datos personales de los usuarios contrario al marco de protección de los mismos.

En cuanto a la proporcionalidad

- Es necesario que la vigilancia de las comunicaciones se limite, como lo establece el principio de proporcionalidad, a delitos graves y prever, expresamente, que primero deben agotarse otras técnicas de investigación menos invasivas.

En cuanto al debido proceso

- Es parece necesario acotar más las situaciones en las que se puede realizar un allanamiento sin autorización judicial. Las excepciones tan amplias desnaturalizan el debido proceso.

En cuanto a notificación del usuario

- Una de las reformas más necesarias es la incorporación de notificación al usuario cuyas comunicaciones son interceptadas.

En cuanto a la transparencia

- No hay datos oficiales públicos sobre actividades de interceptación de comunicaciones. Es necesario que el Estado publique reportes con, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.
- A los fines de este propósito, es clave que se pongan en funcionamiento las instancias de supervisión y control previstas en el marco normativo de las actividades de inteligencia.

- Si bien excede lo que tiene que ver con vigilancia de las comunicaciones, es imprescindible transparentar lo que tiene que ver con los sistemas de recolección de datos como SIBIOS, SUBE y el DNI, entre otros. Hasta el momento, es prácticamente nula la información oficial acerca de qué hace el Estado con esos datos recabados, quién tiene acceso a ellos, con qué fines, de qué manera esos datos se están cruzando, por cuánto tiempo se los almacena, etc.[235]
- Estos cuestionamientos se relacionan con las observaciones realizadas en secciones anteriores sobre la ley de datos personales en Argentina y dos de sus inconvenientes: que el consentimiento no es necesario cuando los datos personales se recaban para el ejercicio de las funciones propias del Estado o en virtud de una obligación legal y que habilita a los distintos organismos públicos a compartir entre sí datos personales.[236]

En cuanto a la supervisión pública

- Es necesario que la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia actúe con más transparencia respecto de las cuestiones que no son secretas y, además, deben contemplarse otros mecanismos de supervisión independientes adicionales.

En cuanto a garantías contra el acceso ilegítimo

- A la luz de casos como las revelaciones de Edward Snowden, sería clave que la normativa de inteligencia nacional incorpore incentivos y medidas de protección para los agentes de inteligencia den a conocer públicamente información sobre prácticas que vulneran derechos fundamentales.[237]

10.

Nuevos desarrollos adoptados por el presidente Macri

Agosto de 2016

El reporte original sobre Argentina fue terminado en octubre de 2015. Desde entonces, ocurrieron muchos cambios. Hacia finales de ese mes, se llevó a cabo la primera vuelta de las elecciones presidenciales. Dos fueron los candidatos más votados: Daniel Scioli, gobernador de la provincia de Buenos Aires y miembro del oficialismo, y Mauricio Macri, jefe de gobierno de la Ciudad Autónoma de Buenos Aires y líder de la coalición opositora. El 22 de noviembre de 2015, Mauricio Macri fue electo presidente con el 51 por ciento de los votos. Una versión actualizada del informe de Argentina, así como la presente adición, fue completado en agosto de 2016.

Asumió el cargo el 10 de diciembre de 2015, momento en que el Congreso estaba en receso de verano.[238] Durante las primeras semanas de su mandato, Macri tomó varias decisiones ejecutivas—la mayoría a través de decretos presidenciales—que modificaron el marco normativo descrito en el reporte de Argentina. Esta breve adenda presenta y, cuando resulta pertinente, analiza estos cambios en relación con los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[239]

Suspensión del nuevo Código Procesal Penal

El Congreso adoptó el nuevo Código Procesal Penal el 9 de noviembre de 2014. La Ley 27.150 estableció en junio de 2015 un proceso de implementación gradual y escalonada, que debía completarse para el 1 de marzo de 2016. El presidente Macri suspendió la implementación del Código alegando que "no se cumplieron" las condiciones para su completa aplicación. En lugar de establecer una nueva fecha para su implementación, Macri decidió—mediante un decreto de necesidad y urgencia—que una Comisión Bicameral del Congreso decidiría cuándo entraría en efecto el nuevo Código, con el consentimiento del Ministerio de Justicia.[240]

Consecuentemente, el análisis brindado en la sección 3.6 del reporte ahora carece de relevancia. Esa sección cubre las maneras en las que se deben realizar los registros y allanamientos (3.6.1 y 3.6.2), y los casos en los que no se requiere una orden judicial (3.6.3). También incluye las formalidades que debe cumplir una orden judicial (3.6.4) y las formalidades por seguir para la ejecución de allanamientos (3.6.5 y 3.6.6). Debido a que el

nuevo Código Procesal Penal no ha entrado en vigencia, las regulaciones de hoy en día se encontrarán en el Código Procesal Penal anterior, el de 1991. La manera en que estos dos códigos abordan los allanamientos e incautaciones no cambia de manera significativa.

En el Código Procesal Penal de 1991, los jueces están a cargo de realizar las investigaciones penales. Sin embargo, pueden delegar los allanamientos y registros a fiscales si así lo eligen.[241] Tanto la orden de allanamiento como el procedimiento deben estar descritos en un documento oficial (un acta), el cual debe cumplir ciertos requisitos formales.[242]

A pesar de que se requiere una orden judicial, el Código establece que no es necesario contar con una en casos de incendio, explosión o inundación en los que la vida de los residentes de una propiedad pueda estar en peligro (artículo 227.1). Tampoco se necesitará una orden cuando se hayan visto "personas extrañas" en una propiedad y haya indicios de que se pueda cometer un delito (227.2). Asimismo, no se requerirá una orden cuando un imputado a quien se persigue entre a una construcción (227.3) o cuando alguien pida socorro desde una casa o local (227.4). Finalmente, no se necesitará una orden cuando haya sospechas de que una víctima de trata de personas se encuentra dentro de una casa o local que debe allanarse (227.5). Se deberá notificar de inmediato a los residentes de la propiedad al momento de la orden de allanamiento y del procedimiento. Si no se encontraren los residentes al momento del allanamiento, se deberá asentar dicha ausencia en el acta.

La sección 5.2 también debe ser reexaminada; actualmente describe cómo se desarrolla el proceso de interceptación de las comunicaciones. En ese sentido, el Código de 1991 en vigencia limita las interceptaciones a la "correspondencia postal o telegráfica".[243] Se puede encontrar una disposición más precisa en la antigua Ley de Telecomunicaciones de 1972 (No. 19.798), la cual fue derogada por la Ley Argentina Digital solo con respecto a aquellos artículos en contradicción con la nueva regulación.[244] En consecuencia, la Ley No. 19.798 todavía controla el proceso por el cual se pueden interceptar las telecomunicaciones. Los artículos del 18 al 21 establecen la necesidad de contar con una orden judicial (artículo 18) e indican que aquellos que trabajen en los servicios de telecomunicaciones deben mantener la confidencialidad de las comunicaciones (artículo 20), obligación que se extiende a "cualquier individuo" que conozca el contenido de estas (artículo 21).

El nuevo Código Procesal Penal, que se encuentra ahora en suspensión, incluía un artículo (144) que permitía el registro de computadoras con el fin de incautar los datos contenidos en ellas. Las reglas para el procedimiento del registro son las mismas que se aplican a la inspección de domicilios personales. Sin embargo, esta regulación también incluía una disposición que garantizaba que los datos que no fueran relevantes para la investigación debían ser devueltos a sus dueños y que cualquier copia de estos en manos del estado debía ser destruida.

Desde la perspectiva de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, la regulación en vigencia actualmente también presenta problemas con respecto a la precisión del uso del lenguaje.[245] En ese sentido, el régimen legal actual también da lugar a registros sin órdenes judiciales bajo circunstancias excepcionales, inclusive algunas—como la de haber visto a personas entrando al domicilio de otro individuo—que son extremadamente generales y propensas al uso abusivo.

Traspaso de la atribución para interceptar comunicaciones

La Ley de Inteligencia Nacional de 2001 (No. 25.520) es el marco legal más importante para las actividades de vigilancia del Estado. Esta ley fue reformada por la Ley No. 27.126 el 5 de marzo de 2015. Además de cambiar el nombre de la principal agencia de inteligencia (de Secretaría de Inteligencia pasó a llamarse Agencia Federal de Inteligencia [AFI]), la ley introdujo una reforma sustantiva: trasladó el organismo a cargo de interceptar comunicaciones (DICOM) desde la esfera del Poder Ejecutivo hacia el Ministerio Público, entidad que es independiente desde 1994.[246] El DICOM es el departamento a cargo de interceptar comunicaciones a petición o con la autorización de un juez.[247] Podría asegurarse que el traslado de este organismo al Ministerio Público fue una decisión que incrementó la transparencia e independencia: habitualmente, el DICOM era percibido como el responsable de una afianzada práctica de espionaje político a voluntad del presidente.[248]

El 24 de diciembre de 2015, mediante el decreto 256/2015, Macri decidió trasladar el DICOM del Ministerio Público a la Corte Suprema.[249] El decreto que hizo que esto se cumpla sostenía que el Ministerio Público no era la entidad institucional correcta para que el DICOM funcionara de manera apropiada, ya que es la parte principal en los procesos penales donde las interceptaciones se usan como evidencia. Por lo tanto, el poder de interceptar comunicaciones yace—según el decreto—en un organismo "distinto al que es parte de la investigación".

Cabe mencionar que tanto la Ley No. 27.126 como el decreto 256/2015 son bastante imprecisos en lo que respecta al poder del DICOM. De conformidad con la Ley de Inteligencia Nacional, todas las interceptaciones de las comunicaciones corresponden al ámbito del DICOM y requieren autorización judicial, es decir, aquellas realizadas para investigaciones penales y las que se llevan a cabo con propósitos de inteligencia, incluida la inteligencia extranjera. Sin embargo, la Ley No. 27.126 y el decreto No. 256/2015 usan un lenguaje que sugiere que el DICOM solo interviene en investigaciones penales. Ese no es el caso, ya que también se encuentra a cargo de interceptaciones relacionadas con la recopilación de inteligencia, incluida la inteligencia extranjera.

El decreto No. 256/2015 afirma que la Corte Suprema establecerá un reglamento interno para la dirección del DICOM, que estará a cargo de un juez con rango de juez de cámara,

quien será designado por sorteo y ejercerá el cargo por el plazo de un año. No obstante, la Corte Suprema se rehusó a tomar esta nueva responsabilidad de inmediato. En un fallo del 29 de diciembre de 2015, la Corte, de manera unánime, decidió que, con el objetivo de recibir al DICOM, debía crear una estructura burocrática que en ese momento no existía.[250] Por lo tanto, se prorrogó la recepción del DICOM hasta el 15 de febrero de 2016. En esa fecha, la Corte publicó la Acordada No. 2/2016 mediante la cual se creó la Dirección de Captación de Comunicaciones del Poder Judicial de la Nación (DCCPJ).[251] Esta regulación aclaró el marco regulatorio que controla la interceptación de las comunicaciones: hace mención de la Ley de Telecomunicaciones de 1972 (No. 19.798), la Ley de Inteligencia Nacional de 2001 y la Ley Argentina Digital de 2015.

Esta nueva Dirección tendrá autonomía de gestión respecto de la Corte Suprema, y estará a cargo de un juez federal. La Corte Suprema, sin embargo, mantiene la facultad de cambiar la regulación de la DCCPJ cuando lo disponga. La Acordada expone unos cuantos principios, los cuales deben guiar la interceptación de las comunicaciones:

- Transparencia y confidencialidad: Establece "fijar" un sistema de control eficiente y ordena reserva absoluta por parte del personal de trabajo de la DCCPJ. También estipula redactar un documento que garantice una "cadena de custodia" que proteja la confidencialidad de la información recopilada mediante las interceptaciones.
- Capacitación: La Corte estableció que aquellos que estén a cargo de interceptar comunicaciones deben estar capacitados para poder tomar decisiones sensatas con respecto a los mecanismos y tecnologías más eficientes para interceptar y evaluar la "oportunidad" y duración de las intervenciones. Es importante mencionar que la regulación establece que los miembros de la DCCPJ pueden asistir a los jueces y fiscales directamente en las dependencias o "en forma remota".
- Minería de datos: Se ordena buscar una actualización para la práctica de minería de datos. Particularmente, señala que se debe intentar encontrar información en "grandes volúmenes de conjuntos de datos" para que esto sea útil para los jueces y fiscales.
- Nuevas tecnologías: Establece que deben buscarse nuevas tecnologías y que deben estudiarse y copiarse las mejores prácticas de los poderes judiciales de otros países.
- Relación con las compañías de telecomunicaciones: La Acordada indica que se firmarán acuerdos de confidencialidad con las compañías de telecomunicaciones, así como también con otras que brinden "servicios utilizables".

La DCCPJ estará integrada por un director general, que será un juez penal, y estará en esa posición por el periodo de un año. Además, la DCCPJ contará con un directorio de cinco directores, pero la Acordada no especifica la manera en la que se elegirán los miembros de este directorio.

Las organizaciones de la sociedad civil que han estado trabajando en este asunto de la reforma de inteligencia durante estos últimos años expresaron su preocupación acerca de la nueva regulación. La Asociación por los Derechos Civiles (ADC) le recordó al público que muchos dudaron de la constitucionalidad de trasladar el DICOM al Poder Judicial.[252] Además, la ADC advirtió sobre el uso de lenguaje impreciso que no aclara completamente cuándo y cómo se realizarán las intervenciones ni quién puede solicitarlas. Con respecto a la sección sobre minería de datos de la Acordada, la ADC cuestionó la existencia de una base de datos que pueda ser minada.

> *"Si el órgano encargado de interceptar comunicaciones ha generado una base de datos que puede ser "minada" los ciudadanos deberían conocer detalles de la misma. ¿En qué consiste? ¿Qué tipo de información almacena? ¿Cómo es la misma recabada? ¿Existen procedimientos de depuración de información que evalúe la legalidad de su retención? ¿Existen garantías en línea con lo que establece la Ley Nacional de Protección de Datos Personales? La introducción del concepto de minería de datos nos resulta en este sentido muy reveladora: da cuenta de prácticas que sospechamos existen pero que no están adecuadamente reguladas en ninguna de las normas, de cualquier nivel, que regulan una actividad del Estado que por definición viola derechos de los ciudadanos".*[253]

Desde el punto de vista de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, el traslado del DICOM hacia el poder de la Corte Suprema también carece de medidas adicionales de supervisión y rendición de cuentas.[254] En efecto, mientras que el DICOM bajo el mando del Ministerio Público carecía de un mecanismo independiente de supervisión, se puede decir lo mismo del DICOM bajo el mando de la Corte Suprema, a pesar de que aún no se han establecido las reglas internas.

Cambios en las autoridades de telecomunicaciones

El reporte menciona la Ley Argentina Digital de 2014, modificada parcialmente por el decreto 267/2015 del 29 de diciembre de 2015. Este decreto no modifica sustancialmente la ley, mas sí unifica su autoridad administrativa (AFTIC) con la autoridad de radiodifusión (AFSCA) establecida por la Ley 26.522 de 2013. Los cambios que se incorporaron en el decreto no aluden a las regulaciones que se tuvieron en cuenta en el reporte de Argentina. Sin embargo, cambia radicalmente las reglas contra la propiedad cruzada de los medios; autoriza a las compañías de telecomunicaciones a acceder y brindar servicios de radiodifusión; y elimina tanto las autoridades de radiodifusión como las de telecomunicaciones para crear una nueva y más abarcativa: el ENACOM.

Conclusión

La suspensión del nuevo Código Procesal Penal se llevó a cabo principalmente debido a que

proponía un cambio controvertido: trasladaría el poder de realizar investigaciones penales, inicialmente de los jueces, hacia los fiscales. Esta es la reforma más importante, que por el momento se encuentra en espera. Con respecto a las reglas que realmente controlan la investigación de crímenes, los cambios que se presentaron entre el Nuevo Código y el Código de 1991 no fueron tan radicales, como hemos visto en la descripción general—y como se puede ver en el cuadro comparativo. La ley permaneció prácticamente igual, aunque algunas actualizaciones propuestas en el Nuevo Código—como la de incluir de manera explícita las comunicaciones electrónicas y la captura de datos electrónicos—todavía no se encuentran dentro de los libros de derecho.

Por otro lado, debe interpretarse que el traslado del departamento a cargo de interceptar las comunicaciones, que antes se encontraba en el Ministerio Público, hacia la Corte Suprema fue motivado por las mismas razones que yacen detrás de la suspensión del nuevo Código Procesal Penal. La máxima autoridad del Ministerio Público es una figura controvertida, que el partido gobernante consideraba demasiado cercana al gobierno anterior. Por ende, el traslado del DICOM a la Corte Suprema se puede interpretar como un esfuerzo para mantenerlo independiente, pero, al mismo tiempo, restringe los poderes del Ministerio Público. De todas formas, la regulación que propone la Corte Suprema parece realmente problemática. Tal y como señaló la ADC, muchos de los detalles son conflictivos, como la directiva de aumentar las capacidades de minería de datos. Asimismo, el DICOM—tanto bajo el mando del Ministerio Público como del de la Corte Suprema—aún carece de un mecanismo de control independiente. Queda por ver si, dentro del nuevo panorama político, el mecanismo de control legislativo establecido en la Ley de Inteligencia Nacional de 2001 funciona como debería o si, como ha pasado durante la última década, es incapaz de controlar de manera efectiva las actividades de inteligencia (ADC, 2015).

Cuadro 1

Marco anterior: Nuevo Código, ahora suspendido	Reglas actuales (Código de 1991)
En el nuevo Código (actualmente en suspensión), los fiscales estaban a cargo de realizar allanamientos y requisas o inspecciones, y—en general—de dirigir las investigaciones penales (artículo 132 del nuevo Código).	El antiguo Código (actualmente vigente) señala que los jueces son quienes realizarán los allanamientos, a pesar de que pueden—si así lo deciden—delegar la diligencia a un fiscal (artículo 224 del Código de 1991).
El nuevo Código, ahora suspendido, indica que el nombre del fiscal a cargo del allanamiento debe quedar asentado en el acta de allanamiento (artículo 132 del nuevo Código).	El Código de 1991 no incluye ese requerimiento (artículo 224).
El nuevo Código (actualmente en suspensión) prevé la interceptación de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación (artículo 143).	El antiguo Código (actualmente vigente) solo menciona la correspondencia postal y las comunicaciones telegráficas (artículo 234).
El nuevo Código (actualmente en suspensión) contiene algunas regulaciones en cuanto a cómo se incautarán los datos recopilados durante el allanamiento. En ese sentido, un juez podría emitir una orden para registrar una computadora, con el objetico de quedarse con los datos. Las mismas reglas aplican para el registro e incautación de documentos. Todos los elementos que no estén relacionados con la investigación penal serán devueltos a sus dueños, quienes pueden exigir la destrucción de los datos que no tengan relación con la investigación (artículo 144).	No existe una regla análoga en el antiguo Código (actualmente vigente). Sin embargo, cabe mencionar que la Corte Suprema consideraba como "documento" a los metadatos a fines constitucionales, y que el Estado únicamente puede recopilarlos bajo las mismas condiciones que aplican para el registro e incautación de un documento. Por ende, la recopilación de metadatos en Argentina no requiere orden judicial.
El DICOM, el organismo a cargo de interceptar comunicaciones, estaba bajo el mando del Ministerio Público.	El presidente Mauricio Macri trasladó al DICOM a la Corte Suprema, la cual le cambió el nombre a lo que ahora llamamos DCCPJ.
En el gobierno anterior, la AFSCA era la autoridad de radiodifusión y la AFTIC, la de telecomunicaciones.	Macri unificó a estas dos autoridades, que fueron eliminadas para poder crear una nueva agencia, más abarcativa, llamada ENACOM.

1 Corte Suprema de Justicia de la Nación, “Ekmekdjian, Miguel Ángel c. Sofovich, Gerardo y otros”, 7 de julio de 1992.

2 El artículo 75 inciso 22 incluye a los siguientes tratados de derechos humanos, ratificados antes de 1994: Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo; la Convención sobre la Prevención y la Sanción del Delito de Genocidio; la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial; la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer; la Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes; la Convención sobre los Derechos del Niño. El artículo contempla un procedimiento en el Congreso para incorporar a los tratados que se firmen con posterioridad.

3 Ley No. 24.767 de Cooperación Internacional en Materia Penal, B.O. del 16/01/1997, artículo 6.

4 Ley No. 25.304, B.O. del 07/09/2000.

5 *Ibíd.*, artículo 2.1.

6 Ley No. 25.911, B.O. del 13/09/1996.

7 Conforme a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, el término “comunicaciones” abarca las actividades, interacciones y transacciones transmitidas por medios electrónicos, tales como el contenido, la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP, momento y duración de las comunicaciones, e identificadores de los equipos utilizados, y “vigilancia de las Comunicaciones” en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, conservar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas.

8 Constitución Nacional, artículo 19.

9 *Ibíd.*, artículo 18.

10 CSJN, "Halabi, Ernesto c/ PEN ley 25.873 y decreto 1563/04 s/ amparo”, sentencia del 24 de febrero de 2009. Disponible en: http://www.cij.gov.ar/nota-615-La-Corte-reconoce-accion-colectiva-y-da-alcance-general-a-un-fallo.html

11 Constitución Nacional, artículo 43.

12 Ibíd.

13 Aprobado por Ley No. 27.063, promulgada el 9 de diciembre de 2014. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239340/norma.htm

14 La ley No. 27150, promulgada el 17 de junio de 2015, establece un procedimiento gradual de entrada en vigor. A partir de marzo de 2016, el Código iba a entrar en vigor en el ámbito de la justicia nacional. En el ámbito de la justicia federal, estaba pactado que entre en vigor de conformidad con un cronograma de implementación progresiva establecido por una Comisión Bicameral de Monitoreo e Implementación del Nuevo Código Procesal Penal de la Nación. Ver página web de la Comisión Bicameral. Disponible en: http://www.senado.gov.ar/parlamentario/comisiones/info/379

15 Decreto 257/2015. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=257347

16 En tanto el nuevo Código Procesal Penal no ha sido derogado, a lo largo del informe nos referiremos a este cuerpo normativo. En el Anexo XXX, incluimos un cuadro comparativo entre el antiguo Código Procesal Penal (vigente al momento de elaborar este informe) y el nuevo marco normativo, por el momento suspendido, en lo vinculado a la interpretación de las comunicaciones.

17 Artículo 13. El subrayado es nuestro.

18 Código Penal, artículo 153.

19 *Ibíd.*, artículo 153 bis.

20 *Ibíd.*, artículo 155.

21 *Ibíd.*, artículo 157 bis.

22 Ley No. 25.520 de Inteligencia Nacional, B.O. del 6/12/2001, artículo 42. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm

23 *Ibíd.*, artículo 43.

24 *Ibíd.*, artículo 43 ter.

25 Ley No. 25.520 de Inteligencia Nacional, supra nota 19.

26 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, B.O. del 05/03/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

27 Decreto No. 337/2015 que promulga la Ley No. 27.126, B.O. del 3/3/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243822/norma.htm

28 Decreto No. 950/2002, B.O. del 06/6/2002. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/74896/norma.htm

29 Decreto 1311/15, B.O. del 6/07/ 2015. Disponible en: http://www.infoleg.ov.ar/infolegInternet/verNorma.do?id=248914

30 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 1.

31 *Ibíd.*, artículo 2.

32 Ley No. 23.554 de Defensa Nacional, B.O. del 13/04/1988. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

33 Ley No. 24.059 de Seguridad Interior, B.O. del 17/01/1992. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/458/texact.htm

34 Asociación por los Derechos Civiles, "Quién vigila a quienes vigilan. Estudio comparativo sobre sistemas de control de los organismos de inteligencia", 2014, p. 5 y 6.

35 Ley No. 23.554 de Defensa Nacional, artículo 15.

36 Ley No. 24.059 de Seguridad Interior, artículo 8, punto 2.

37 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 3.

38 Durante el proceso de discusión que se mantenga este aspecto ha sido criticado por organizaciones de derechos humanos. Por ejemplo, el Centro de Estudios Legales y Sociales (CELS) ha señalado: "Este artículo habilitó que durante todos estos años se cuele la actuación de la Secretaría de Inteligencia en cualquier causa judicial como auxiliar de la justicia, lo que alimentó la relación promiscua con sectores importantes de la justicia federal. Si se sostiene esta posibilidad, fracasarán los objetivos de la reforma". Ver más en Centro de Estudios Legales y Sociales, "Ley de Inteligencia: las reformas al proyecto no solucionan problemas de fondo", 7 de febrero de 2015. Disponible en: http://cels.org.ar/comunicacion/?info=detalleDoc&ids=4&lang=es&ss=46&idc=1896

39 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 4.

40 *Ibíd.*, artículo 5 bis.

41 *Ibíd.*, artículo 18.

42 *Ibíd.*

43 *Ibíd.*, artículo 41.

44 Decreto 256/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm

45 Ley No. 25.326 de Protección de los Datos Personales. B.O. del 13/04/1988. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

46 Ley No. 25.520, *supra* nota 19, artículo 16 quáter., incorporado por el artículo 13 de la ley No. 27.126.

47 *Ibíd.*, artículo 16 quinquies, incorporado por el artículo 14 de la ley No. 27.126.

48 Ley No. 25.520, *supra* nota 19, artículo 16 sexies, incorporado por el artículo 15 de la ley No. 27.126.

49 *Ibíd.*, artículo 42.

50 Decreto No. 1311/15, B.O. del 6/07/2015. Disponible en: http://www.infojus.gob.ar/descarga-archivo?guid=noprstuv-wnov-edad-esde-c13112015pdf&name=dec13112015.pdf

51 *Ibíd.*

52 Según la nueva doctrina de inteligencia nacional, la "información de inteligencia" es la que comprende "el conjunto de observaciones y mediciones obtenido o reunido de fuentes públicas o reservadas referido a un evento o problemática relevante del ámbito de la defensa nacional o la seguridad interior o que tiene incidencia en esas esferas".

53 *Ibíd.*

54 Decreto No. 15, supra nota 46, Anexo I. Disponible en: http://www.boletinoficial.gov.ar/Displaypdf.aspx?s=A&tid=49218111&i=1

55 *Ibíd.*

56 *Ibíd.*

57 Asociación por los Derechos Civiles, "Observaciones al decreto 1311/15", 9 de julio de 2015, p. 2. Disponible en: http://www.adc.org.ar/wp-content/uploads/2015/07/Apuntes-sobre-el-decreto-1311-15.pdf

58 Decreto No. 1311/15, *supra* nota 46, Anexo I.

59 Cabe señalar que Argentina cuenta con un marco regulatorio muy restrictivo en cuanto a derechos de autor dado por la Ley de Propiedad Intelectual No. 11.723 del año 1933 que tuvo posteriores modificaciones siempre en sentido más restrictivo.

60 Ley No. 27.078 Argentina Digital, B.O. del 19/12/2014. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/235000-239999/239771/norma.htm

61 Ver más en Fontanals, Gustavo, "La política detrás de AFTIC", *Bastión Digital*, 13 de julio de 2015. Disponible en: http://ar.bastiondigital.com/notas/la-politica-detras-de-aftic y Massare, Bruno y Pautasio, Leticia, "Argentina Digital en detalle: qué cambios plantea la nueva ley de telecomunicaciones", *Infotechnology*, 8 de mayo de 2015. Disponible en: http://www.infotechnology.com/internet/Argentina-Digital-en-detalle-que-cambios-plantea-la-nueva-ley-de-telecomunicaciones-20150508-0008.html#sthash.UuPMbB3U.dpuf

62 La ley Argentina Digital en su artículo 89 señala que la Ley No. 19.798 y sus modificatorias sólo subsistirán "respecto de aquellas disposiciones que no se opongan a las previsiones de la presente ley".

63 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 5.

64 A través de otro decreto presidencial, el 267/2015, se fusionaron los organismos públicos encargados de los medios audiovisuales (Autoridad Federal de Servicios de Comunicación Audiovisual, AFSCA) y de telecomunicaciones (Autoridad Federal de Tecnologías de la Información y la Comunicación, AFTIC) en un nuevo organismo denominado Ente Nacional de las Comunicaciones, ENACOM). Más allá de esta dimensión, este decreto no altera el marco de telecomunicaciones en lo vinculado a los aspectos analizados en este informe.

65 *Ibíd.*, artículo 60, punto d.

66 Asociación por los Derechos Civiles, "Alerta de la ADC sobre el proyecto de ley Argentina Digital", 16 de noviembre de 2014. Disponible en: http://www.adc.org.ar/alerta-de-la-adc-sobre-el-proyecto-de-ley-argentina-digital/

67 Secretaria de Comunicaciones, Resolución No. 5/2013, 1/7/2013. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

68 Ley No. 27.078 Argentina Digital, supra nota 56, artículo 87.

69 Ley No. 25.891 de Servicios de Comunicaciones Móviles, B.O. del 28/04/ 2004. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/95000-99999/95221/norma.htm

70 Portal Nacional de Usuarios de Telecomunicaciones. Autoridad Federal de Tecnologías de la Información y las Comunicaciones. Disponible en: http://www.quenosecorte.gob.ar/

71 Ley No. 25.891 de Servicios de Comunicaciones Móviles, Art. 3.

72 Vargas, Paula, "Vigilancia masiva de las comunicaciones: inconstitucionalidad de la Ley 25.891", *Blog Derecho de Internet y Tecnología de las Comunicaciones*, 12 de agosto de 2015. Disponible en: http://www.ditc.com.ar/2015/08/12/397/

73 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaria de Comunicaciones, Resolución No. 5/2013, 1/7/2013. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

74 *Ibíd.*, artículo 2.

75 *Ibíd.*, artículo 3.

76 *Ibíd.*, artículo 5, punto 2.

77 *Ibíd.*

78 Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), "Internet en Argentina: ¿cómo estamos hoy?", p. 18. Disponible en: http://www.palermo.edu/cele/pdf/investigaciones/Mapping-ARG-CELE.pdf

79 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaria de Comunicaciones, Resolución No. 5/2013, 1/7/2013, artículo 8.

80 Código Procesal Penal de la Nación. Artículo 132.

81 *Ibíd.*

82 Código Procesal Penal de la Nación, artículo 133.

83 *Ibíd.*

84 *Ibíd.*, artículo 135.

85 *Ibíd.*, artículo 137.

86 Requisitos establecidos en el artículo 136: a) La determinación concreta del lugar o los lugares que deberán ser registrados; b) La finalidad del registro, mencionando los objetos a secuestrar o las personas a detener; c) El nombre del representante del Ministerio Público Fiscal responsable del control o de la ejecución de la medida, los motivos que fundan su necesidad y cuáles son las evidencias disponibles que, prima facie, la justifican; d) En su caso, los motivos que fundamentan la necesidad de efectuar la diligencia fuera del horario diurno; e) La firma del representante del Ministerio Público Fiscal que requiere la autorización.

87 Código Procesal Penal de la Nación, artículo 139.

88 Ley No. 25.326 de Protección de los Datos Personales, *supra* nota 41, artículo 1.

89 Decreto No. 1558/2001, B.O. del 29/11/2001. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

90 Decreto No. 1160/10, B.O. del 11/08/2010. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/170000-174999/170508/norma.htm

91 Ley No. 26.343, B.O. del 09/01/2008. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/135000-139999/136483/norma.htm

92 Asociación por los Derechos Civiles, "El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos", 2014, p. 3.

93 *Ibíd.*, p. 3 y 4.

94 *Ibíd.*, p. 3 y Torres, Natalia, *Acceso a la información y datos personales: una vieja tensión, nuevos desafíos*, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Universidad de Palermo. Disponible en: http://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf

95 *Véase*, Asociación por los Derechos Civiles, "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina", mayo de 2015, p. 5. Disponible en: http://www.adc.org.ar/wp-content/uploads/2015/05/InformeBiometriaADC2015.pdf y Fascendini, Flavia y Roveri, Florencia, "Tu software, mi biología. Sistemas de vigilancia masiva en Argentina", *GISWatch Report*, 2014. Disponible en: http://www.giswatch.org/node/4951

96 Savoia, Claudio, *Espiados*, Buenos Aires, Editorial Planeta, 2015, p. 333.

97 Madres de Plaza de Mayo Línea Fundadora, Fundación Vía Libre, Liga por los Derechos del Hombre y otros, "Los DNI electrónicos violan nuestros derechos", 06 de octubre de 2014. Disponible en: http://www.pensamientopenal.org.ar/dni/

98 Siri, Laura, "El Documento Nacional de Identidad Argentino: una "caja negra" y una política de veridicción", III Simposio Internacional LAVITS Vigilancia, Tecno Políticas y Territorios 13-15, mayo 2015. Río de Janeiro, Brasil. Red de Estudios Latinoamericanos sobre Vigilancia, Tecnología y Sociedad (LAVITS), p. 3.

99 *Ibíd.*

100 *Véase también*, Villa, Emiliano y Álvarez Ugarte, Ramiro, "Las fotos de los argentinos, al mejor postor", Boletín *Digital Rights*, 22 de noviembre de 2013. Disponible en: http://www.digitalrightslac.net/es/las-fotos-de-los-argentinos-al-mejor-postor/

101 Ley No. 17.671 de Identificación, registro y clasificación del potencial humano nacional, BO del 29/02/1968. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

102 Siri, Laura, *supra* nota 94, p. 2.

103 ADC, *supra* nota 91, p. 8.

104 Decreto No. 1501/2009, B.O. del 20/10/2009. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

105 RENAPER, Resoluciones No. 585/2012 y No. 797/2012.

106 ADC, *supra* nota 74, p. 9.

107 "Randazzo anunció nuevo DNI inteligente que incorpora un chip", Audiovisual Télam, 27 de junio de 2014. Disponible en: http://www.telam.com.ar/multimedia/video/5091-randazzo-anuncio-nuevo-dni-inteligente-que-incorpora-un-chip/

108 Siri, Laura, *supra* nota 77, p. 5.

109 Madres de Plaza de Mayo Línea Fundadora y otros, *supra* nota 76.

110 Secretaría de Transporte, Resolución 162/2010, del 27/10/2010. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/170000-174999/170118/norma.htm

111 Es posible usar la tarjeta sin registrarse pero, en caso de no hacerlo, no hay modo de reclamar el saldo no usado si la tarjeta, por ejemplo, se extravía. Asimismo, el uso de esta tarjeta no es obligatorio pero, de no hacerlo, el costo de los viajes es mayor.

112 Fundación Vía Libre, "Con SUBE sí vas a pagar más caro: el fin de la privacidad". Disponible en: http://www.vialibre.org.ar/2012/01/27/con-sube-si-vas-a-pagar-mas-caro-el-fin-de-la-privacidad/

113 Ley No. 25.326 de Protección de los Datos Personales, *supra* nota 41, artículo 9.

114 "Exponen en la Red los registros de viajes de la tarjeta SUBE", *La Nación*, 30 de enero de 2012. Disponible en: http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube y "Anonymous SUBE viajes", *Página 12*, 31 de enero de 2012. Disponible en: http://www.pagina12.com.ar/diario/cdigital/31-186566-2012-01-31.html

115 Decreto No. 1766/2011.

116 ADC, "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina", 2015, p. 18.

117 Decreto No. 1176/2011, artículo 4.

118 Savoia, Claudio, *supra* nota 92, p. 335 y 336.

119 ADC, 2015, "Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina", p. 17 y 18.

120 Tordini, Ximena, "El triunfo final sobre el anonimato", Revista Crisis, Número 8, febrero-marzo de 2012. Disponible en: http://www.revistacrisis.com.ar/el-triunfo-final-sobre-el.html

121 Dirección Nacional de Protección de Datos Personales, Disposición No. 20/2015, B.O. 27/05/2015.

122 La Administración Nacional de Aviación Civil emitió regulación general sobre los vehículos no tripulados. *Véase*, ANAC, Resolución N° 527/2015, Reglamento Provisional de los Vehículos Aéreos no Tripulados. Disponible en: http://www.anac.gov.ar/anac/web/index.php/1/1196/noticias-y-novedades/reglamento-provisional-de-los-vehiculos-aereos-no-tripulados-vant

123 Por ejemplo, organizaciones de la región expusieron sobre el uso de drones y su impacto en los derechos humanos en las Américas en una audiencia ante la Comisión Interamericana de Derechos Humanos en 2013.

124 La disposición define, en su Anexo II, al VANT o drone como un artefacto "equipado con cámaras, micrófonos, gps, o cualquier otro tipo de sensor, tiene la capacidad para recolectar datos de personas, como pueden ser imágenes, videos, conversaciones, geolocalización, entre otros. A ello se le suma su capacidad de vuelo, que le permite acceder a lugares a los que el ojo humano no llega; y la posibilidad de operar sin ser detectados".

125 Dirección Nacional de Protección de Datos Personales, Disposición No. 20/2015, B.O. 27/05/2015. Disponible en: http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf

126 Ministerio de Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales, Disposición 10/2015, Bs. As., 24/2/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243335/norma.htm

127 Savoia, Claudio, *supra* nota 92, p. 318.

128 Ley No. 2.602, 06/12/ 2007.

129 Ley No. 13.164.

130 *Ibíd.*, artículo 3.

131 *Ibíd.*, artículo 7.

132 *Ibíd.*, artículo 6.

133 Ministerio de Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales, Disposición 18/2015, Bs. As., 10/4/2015. Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/245000-249999/245973/norma.htm

134 *Ibíd.*, Introducción.

135 *Ibíd.*, Anexo 1, Punto 3.

136 El Decreto No.357/2005 suspendió la aplicación del Decreto No. 1563.

137 Halabi, considerando 23.

138 *Ibíd.*, considerando 24.

139 Halabi, considerando 24.

140 *Ibíd.*, considerando 25.

141 *Ibíd.*, considerando 26.

142 Constitución Nacional, artículo 1.

143 Gelli.

144 Constitución Nacional, artículo 75, inciso 12.

145 Código Procesal Penal Nacional, artículo 52.

146 Código Procesal Penal Nacional, artículo 88.

147 Código Procesal Penal Nacional, artículo 90.

148 Código Procesal Penal Nacional, artículo 143.

149 *Ibíd.*

150 *Ibíd.*

151 *Ibíd.*

152 *Ibíd.*

153 Código Procesal Penal Nacional, artículo 144.

154 *Ibíd.*

155 *Ibíd.*

156 *Ibíd.*

157 Código Procesal Penal Nacional, artículo 145.

158 *Ibíd.*, artículo 145.

159 *Ibíd.*

160 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, *supra* nota 23, artículo 7.

161 Decreto No. 1311/15, *supra* nota 46, Anexo I, Capítulo III.

162 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, *supra* nota 23, artículo 8.

163 *Ibíd.*

164 Presidencia de la Nación de Argentina. Ministerio de la Seguridad. Disponible en: http://www.minseg.gob.ar/

165 Decreto No.1311/15, *supra* nota 46, Anexo I, Capítulo III, folio 27.

166 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, *supra* nota 23, artículo 7.

167 *Ibíd.*

168 Decreto No. 1311/15, *supra* nota 46, Anexo I, Capítulo III, folio 28.

169 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 18.

170 *Ibíd.*

171 *Ibíd.*, artículo 19.

172 *Ibíd.*, artículo 20.

173 Ministerio Público Fiscal, Resolución, PGN No. 2067/15, 07 de julio de 2015.

174 El Ministerio Público Fiscal es parte fundamental en la administración de justicia, compuesta por el Poder Judicial y los Ministerios Públicos: Fiscal y de la Defensa. En su conjunto, conforman las tres partes fundamentales en un proceso judicial. Asimismo, el Ministerio Público Fiscal es un órgano independiente dentro del sistema de administración de justicia. Se encuentra a cargo del Procurador o de la Procuradora General, que es propuesto o propuesta por el Poder Ejecutivo y aprobado por el Congreso de la Nación. Es independiente incluso del Poder Judicial (encabezado por la Corte Suprema de Justicia). Esa independencia tiene sus orígenes en la Reforma Constitucional de 1994, que estableció la autonomía del Ministerio Público. En relación con la parte penal, el Procurador o la Procuradora a cargo del Ministerio tienen la facultad de definir cómo se persiguen determinados delitos que pueden tener una relevancia mayor en la defensa de los intereses generales de la sociedad. Por ejemplo, aquellos que atentan contra la vida, contra la humanidad, los vinculados al narcotráfico, a la violencia institucional, o al lavado de dinero, por mencionar algunos. Por eso es que en la estructura del MPF se conformaron unidades especializadas, que tienen como fin mejorar el desempeño en el trabajo. El Ministerio Público Fiscal de la Nación, es según la ley que le da origen, un órgano autónomo e independiente del Poder Ejecutivo. *Véase también*, Ley No. 27.148 Orgánica del Ministerio Público Fiscal, junio de 2015. Disponible en: http://www.infojus.gob.ar/27148-nacional-ley-organica-ministerio-publico-fiscal-lns0006116-2015-06-10/123456789-0abc-

defg-g61-16000scanyel

175 Decreto 256/2015. Disponible en http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm

176 Corte Suprema de Justicia de la Nación, Acordada 45/2015, 29 de diciembre de 2015. Disponible en: http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=96663

177 Corte Suprema de Justicia, Acordada No. 2/16, 15 de febrero de 2016. Disponible en http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=96793

178 Ver más en Asociación por los Derechos Civiles, "Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones"19 de febrero 2016. Disponible: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

179 Ídem.

180 Ídem.

181 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 13.9.

182 *Ibíd.*, artículo 32.

183 *Ibíd.*, artículo 33.

184 *Ibíd.*, artículo 16.

185 Asociación por los Derechos Civiles, "Quién vigila a los que vigilan", p. 15.

186 *Ibíd.*, p. 14.

187 Di Santi, Matías, "Marcelo Fuentes: 'Las funciones de la Comisión están claras y su trabajo también'", *Chequeado.com*, 3 de febrero de 2015. Disponible en: http://chequeado.com/ultimas-noticias/marcelo-fuentes-las-funciones-de-la-comision-estan-claras-y-su-trabajo-tambien

188 Ver página web de la Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia -Ley 25.520. Disponible en: http://www.senado.gov.ar/parlamentario/comisiones/proyectos/104

189 "Cuestionan a la Comisión Bicameral de Inteligencia", *La Nación*, 25 de febrero de 2014. Disponible en: http://www.lanacion.com.ar/1667003-cuestionan-a-la-comision-bicameral-de-inteligencia

190 Iniciativa Ciudadana para el Control del Sistema de Inteligencia.

191 Sued, Gabriel, "Se reúne la bicameral de Inteligencia", *La Nación*, 3 de febrero de 2015. Disponible en: http://www.lanacion.com.ar/1765255-se-reune-la-bicameral-de-inteligencia y "A puertas cerradas y con la presencia de Parrilli, la bicameral de fiscalización de organismos de inteligencia analiza el proyecto oficial", *Télam*, 5 de febrero de 2015. Disponible en: http://www.telam.com.ar/notas/201502/94130-proyecto-sistema-de-inteligencia-bicameral-fiscalizacion.html

192 "Espían y roban correos electrónicos de un juez y de un periodista de Clarín", *Clarín*, 11 de mayo de 2006 y Sued, Gabriel, "Espían e-mails de políticos y periodistas", *La Nación*, 23 de mayo de 2006. Disponible en: http://www.lanacion.com.ar/808286-espian-e-mails-de-politicos-y-periodistas

193 Palazzi, Pablo, *Los delitos informáticos en el Código Penal. Análisis de la ley No. 26.388*, Abeledo Perrot, 2012, pp. 20-22.

194 *Véase también*, Smink, Veronica, "Procesan al alcalde de Buenos Aires por caso de espionaje", *BBC Mundo*, disponible en: http://www.bbc.com/mundo/america_latina/2010/05/100514_2318_macri_proceso_buenos_aires_jg.shtml y Hauser, Irina y Kollmann, Raúl, "El día que Macri quedó Procesado", *Página 12*, 15 de mayo de 2010. Disponible en: http://www.pagina12.com.ar/diario/elpais/1-145731-2010-05-15.html

195 "Escuchas ilegales: la Cámara Federal confirmó el procesamiento de Macri", *Perfil*, 15/07/2010. Disponible en: http://www.perfil.com/politica/Escuchas-ilegales-la-Camara-Federal-confirmo-el-procesamiento-de-Macri-20100715-0019.html

196 Véase, "Una denuncia contra la Gendarmería", *Página 12*, 22 de noviembre de 2011. Disponible en: http://www.pagina12.com.ar/diario/elpais/1-181754-2011-11-22.html; Thieberger, Mariano, "Proyecto X: Cómo espió la Gendarmería a más de mil organizaciones", *Clarín*, 10 de octubre de 2013. Disponible en: http://www.clarin.com/zona/espio-Gendarmeria-mil-organizaciones_0_880112088.html; Riera, Ariel y Tarricone, Manuel, "CFK: "Quisieron montar (...) que había una suerte de espionaje de la Gendarmería, Proyecto X, inexistente". Disponible en: https://eff.org/r.ktax; "Un escándalo que reveló la cara oculta de la política de seguridad", *Clarín*, 10 de octubre de 2013. Disponible en: http://www.clarin.com/zona/escandalo-revelo-oculta-politica-seguridad_0_880112093.html

197 Se puede tomar dimensión del alcance de Proyecto X viendo la lista completa de las organizaciones en todo el país que fueron objeto de las actividades de inteligencia de la Gendarmería Nacional. *Véase*, Savoia, Claudio, *supra* nota 92, p. 341-383.

198 "No admitimos espionaje", *Página 12*, 18 de febrero de 2012. Disponible en: http://www.pagina12.com.ar/diario/elpais/1-187848-2012-02-18.html

199 Ley de datos personales, artículo 4.

200 *Ibíd.*, artículo 7.

201 *Ibíd.*, artículo 2.

202 Entrevista a Beatriz Busaniche de la Fundación Vía Libre, "Acá se vigila a quienes interpelan al poder", *Perfil*, 02 de enero de 2015. Disponible en: http://www.perfil.com/elobservador/Aca-se-vigila-a-quienes-interpelan-al-poder-20150102-0062.html, Santoro, Daniel, "El Gobierno compró equipos para espiar mails y llamados", *Clarín*, 15 de noviembre de 2014. Disponible en: http://www.clarin.com/politica/Organismos_de_inteligencia-vigilancia-SIDE-espionaje_0_1249075526.html y Savoia, Claudio, *supra* nota 92, p. 220.

203 "Hacking Team", 8 de julio de 2015. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/4517

204 Ver más en "Hallan muerto al fiscal Alberto Nisman en su departamento de Puerto Madero", *La Nación*, 19 de enero de 2015. Disponible en: http://www.lanacion.com.ar/1761270-hallan-muerto-al-fiscal-alberto-nisman-en-su-departamento-de-puerto-madero y "AMIA Special Prosecutor Alberto Nisman found dead in his Puerto Madero home", *Buenos Aires Herald*, 19 de enero de 2015. Disponible en: http://www.buenosairesherald.com/article/179900/amia-special-prosecutor-alberto-nisman-found-dead-in-his-puerto-madero-home

205 Marquis-Boire, Morgan, "Dentro de la campaña de spyware contra alborotadores argentinos" [*Inside the Spyware Campaign Against Argentine Troublemakers*], *The Intercept*, 21 de Abril del 2015. Disponible en: https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/

206 En este mismo sentido, los peritos locales afirmaron que el software encontrado "sólo tiene efecto en computadoras". Ver más en: Hauser, Irina, "Una lupa sobre el celular y la notebook", *Página 12*, 8 de junio de 2015. Disponible en: http://www.pagina12.com.ar/diario/elpais/1-274433-2015-06-08.html y "Peritos dictaminaron que el virus en el celular del fiscal no sirve para espiar", *Perfil*, 26 de agosto de 2015. Disponible en: https://eff.org/r.8rvv

207 *Véase*, O'Donnell, Santiago, "Caso Nisman. Pruebas y sospechas", *Revista Anfibia*. Disponible en: http://www.revistaanfibia.com/ensayo/pruebas-y-sospechas/ y Budassi, Sonia y Fidanza, Andrés, "El rompecabezas Nisman", *Revista Anfibia*. Disponible en: http://www.revistaanfibia.com/cronica/el-rompecabezas-nisman/

208 *Véase*, Smink, Verónica, "Por qué Argentina tiene un problema con sus servicios de inteligencia", *BBC Mundo*, 27 enero 2015. Disponible en: http://www.bbc.com/mundo/noticias/2015/01/150126_argentina_nisman_espias_vs y "Macri reclamó que la muerte de Nisman sea 'un antes y un después'", *Clarín*, 19 de enero de 2015. Disponible en: http://www.clarin.com/politica/Macri-reclamo-muerte-Nisman-bisagra_0_1288071426.html

209 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 5 bis.

210 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 5.

211 *Ibíd.*, artículo 60, punto d.

212 *Ibíd.*, artículo 5, punto 2.

213 Secretaría de Comunicaciones, *supra* nota 62, artículo 8.

214 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 60, punto d.

215 Ley No. 25.891 de Servicios de Comunicaciones Móviles, *supra* nota 64, artículo 8.

216 *La Nación*, "Florencio Randazzo anunció un nuevo DNI, con chip inteligente", 27 de junio de 2014. Disponible en: http://www.lanacion.com.ar/1705106-florencio-randazzo-anuncio-un-nuevo-dni-con-un-chip-inteligente.

217 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 18.

218 *Ibíd.*, Título VI, artículo 18.

219 Ley de Protección de los Datos Personales No. 25.326.

220 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 19.

221 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 5.

222 Secretaría de Comunicaciones, *supra* nota 62, artículo 8.

223 Ley 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 16 sexies.

224 *Véase*, Secretaría de Comunicaciones, *supra* nota 62 y ley de servicios de comunicación móviles, *supra* nota 64.

225 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 20.

226 *Ibíd.*, artículo 16.

227 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 16 sexies.

228 *Ibíd.*, artículo 42.

229 *Ibíd.*, artículo 19.

230 Código Penal, artículo 155.

231 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 42.

232 *Ibíd.*, artículo 43.

233 *Ibíd.*

234 *Véase*, Bertoni, Eduardo, "Ley de inteligencia, oportunidad perdida", Bastión Digital, 19 de febrero de 2015. Disponible en: http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgJU.dpuf

235 Siri, Laura, *supra* nota 77, p. 3.

236 *Ibíd.*

237 *Véase*, Bertoni, Eduardo, "Ley de inteligencia, oportunidad perdida", Bastión Digital, 19 de febrero de 2015. Disponible en: http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgJU.dpuf

238 En Argentina, el Congreso mantiene sesiones ordinarias entre el 1 de marzo y el 30 de noviembre. La Constitución Nacional argentina permite al presidente solicitar una prórroga para las sesiones ordinarias o convocar al Congreso a sesiones extraordinarias (artículo 99.9). El presidente Macri decidió no ejercer este poder durante la primera semana de su mandato. En febrero de 2016, sí convocó al Congreso para debatir un conjunto determinado de cuestiones, en las que no se incluyeron ninguna de las decisiones o decretos que desarrollaremos en este documento.

239 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://en.necessaryandproportionate.org/text.

240 Decreto 257/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257347/norma.htm. Este poder presidencial no existe en otras democracias presidenciales, como por ejemplo, Estados Unidos. Esta facultad se incorporó en la Constitución de 1994, cuando se la reformó. El artículo 99.3 le concede este poder al presidente de la siguiente manera:

"El Presidente de la Nación tiene las siguientes atribuciones: ...3. Participa de la formación de las leyes con arreglo a la Constitución, las promulga y hace publicar. El Poder Ejecutivo no podrá en ningún caso bajo pena de nulidad absoluta e insanable, emitir disposiciones de carácter legislativo. Solamente cuando circunstancias excepcionales hicieran imposible seguir los trámites ordinarios previstos por esta Constitución para la sanción de las leyes, y no se trate de normas que regulen materia penal, tributaria, electoral o de régimen de los partidos políticos, podrá dictar decretos por razones de necesidad y urgencia, los que serán decididos en acuerdo general de ministros que deberán refrendarlos, conjuntamente con el jefe de gabinete de ministros. El jefe de gabinete de ministros personalmente y dentro de los diez días someterá la medida a consideración de la Comisión Bicameral Permanente, cuya composición deberá respetar la proporción de las representaciones políticas de cada Cámara. Esta comisión elevará su despacho en un plazo de diez días al plenario de cada Cámara para su expreso tratamiento, el que de inmediato considerarán las Cámaras. Una ley especial sancionada con la mayoría absoluta de la totalidad de los miembros de

cada Cámara regulará el trámite y los alcances de la intervención del Congreso".

241 Código Procesal Penal de 1991, artículo 224.

242 Código Procesal Penal de 1991, artículos 224, 138 y 139.

243 Código Procesal Penal de 1991, artículo 234.

244 *Véase* Ley Argentina Digital, artículo 89.

245 *Vea el análisis en el reporte, subsección sobre Debido Proceso.*

246 El artículo 120 de la Constitución argentina establece lo siguiente:
"El Ministerio Público es un órgano independiente con autonomía funcional y autarquía financiera que tiene por función promover la actuación de la justicia en defensa de la legalidad de los intereses generales de la sociedad en coordinación con las demás autoridades de la República. Está integrado por un procurador general de la Nación y un defensor general de la Nación y los demás miembros que la ley establezca. Sus miembros gozan de inmunidades funcionales e intangibilidad de remuneraciones".

247 Al respecto, *vea* ADC, "¿Quién vigila a quienes vigilan? Estudio comparativo sobre sistemas de control de los organismos de inteligencia", Policy Paper (Buenos Aires: Asociación por los Derechos Civiles, mayo de 2014) y ADC, "El (des)control democrático de los organismos de inteligencia en la Argentina", Reporte. (Buenos Aires: Asociación por los Derechos Civiles, enero de 2015).

248 *Véase* ADC, 2015, p. 7.

249 Decreto 256/2015. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm.

250 Vea la Acordada No. 45/2015, Corte Suprema de Justicia de la Nación, 29 de diciembre de 2015.

251 Vea la Acordada No. 2/2016, Corte Suprema de Justicia de la Nación, 15 de febrero de 2016.

252 Asociación por los Derechos Civiles. Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones. 19 de febrero de 2016. Disponible en: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/.

253 Ídem.

254 Vea el análisis en el reporte, subsección sobre Supervisión Pública.