VIGILANCIA ESTATAL PERSONALIZADA Y DERECHO A LA INTIMIDAD. LA CARA OBSCURA DE LA DEMOCRACIA ARGENTINA

Vladimir CHORNY [1]

La vigilancia estatal es un problema enorme para quienes nos preocupamos por el respeto a los derechos humanos, en particular el de la privacidad (y otros relacionados con éste como la inviolabilidad de las comunicaciones privadas y la libertad de expresión). Aquí analizo el fenómeno concreto de la vigilancia personalizada o el espionaje estatal, diferenciándola de la vigilancia masiva y la ciberseguridad (los tres podrían entrar en una definición amplia de vigilancia estatal), a la luz de las protecciones legales de la Ciudad de Buenos Aires, el marco argentino en general y los estándares internacionales y regionales en materia de derechos humanos y vigilancia. En cinco apartados mostraré la incompatibilidad de la vigilancia personalizada con la democracia argentina (siendo "su cara obscura"): I. una introducción sobre la vigilancia estatal y sus implicancias para la vida de las personas en las sociedades democráticas modernas; II. el marco internacional y nacional de protección y controles democráticos a la vigilancia estatal; III. la estructura actual de los sistemas de inteligencia y las autoridades relacionadas con las acciones de vigilancia estatal; IV. el contexto argentino sobre la intervención de las comunicaciones privadas; y V. las conclusiones sobre por qué el espionaje estatal sin controles es democráticamente inaceptable.

I. Introducción

La vigilancia estatal personalizada o dirigida es parte del concepto más amplio de vigilancia estatal de las comunicaciones [2], donde

1 Investigador asociado de la Red en Defensa de los Derechos Digitales (R3D). Doctorante en Filosofía Política en la Universidad de Buenos Aires (UBA). Profesor de Teoría General del Derecho en la UBA.

2 La vigilancia estatal en general se entiende como las acciones que los Estados realizan para recolectar, almacenar, monitorear y analizar in-

se incluye la vigilancia masiva (retención de datos, por ejemplo) y, en algunos casos, la ciberseguridad [3].

Me concentro sólo en la primera separándola de la vigilancia masiva y de la ciberseguridad y mantengo la relación con los otros dos conceptos (vigilancia masiva y ciberseguridad) cuando éstos son utilizados para ampliar las facultades de vigilancia de los Estados [4]. Creo que proceder de esta forma es útil para entender los límites y alcances particulares de cada tema, para establecer después las formas en que éstos pueden ser compatibles con el derecho a la intimidad y la privacidad en general [5].

---

formación que utilizan en tareas de inteligencia o de investigación criminal, y éstas pueden ir desde acciones de infiltración de grupos sociales o políticos y las medidas de retención de datos, hasta el uso de nuevas tecnologías para utilizar *software* invasivo de la privacidad de las personas a través de sus dispositivos electrónicos. Red en Defensa de los Derechos Digitales (R3D), *El Estado de la Vigilancia. Fuera de Control*, México, Noviembre de 2016, p. 6. Aquí estudio sólo el último tipo de acciones, denominándolas "espionaje estatal" o "vigilancia personalizada", y dejando la denominación de "vigilancia estatal" o "vigilancia de las comunicaciones" para el concepto más amplio que no estudio aquí.

3 Esta última entendida de forma acotada (como hace la Comisión Interamericana de Derechos Humanos), entendida como el resguardo de los sistemas y datos informáticos, donde es central la protección de las redes interdependientes y la infraestructura de la información. Comisión Interamericana de Derechos Humanos (CIDH). *Libertad de expresión e Internet*. 31 de diciembre de 2013. Como ejemplos sobre ciberseguridad están la infraestructura estatal y militar, la infraestructura de la información, el combate al cibercrimen, etc. Asociación de Derechos Civiles (ADC): *Ciberseguridad en la era de la Vigilancia Masiva. Descubriendo la agenda de ciberseguridad de América Latina: El caso de Argentina*, Mayo 2016, pp. 19-22.

4 ADC: *Ciberseguridad*… op. cit., p. 37. En Argentina, por ejemplo, esta relación se define por la nueva doctrina de inteligencia estatal establecida en 2015, donde se señala que parte de las problemáticas que quedan dentro del ámbito de la Seguridad Interior están las acciones que atentan contra la seguridad cibernética, los delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos o parte de ellos, el uso fraudulento y la difusión ilegal de contenidos.

5 La relación vigilancia-ciberseguridad se delinea de la nueva Doctrina de Inteligencia Nacional. La segunda es un fenómeno delictivo complejo que la Agencia Federal de Inteligencia encara produciendo inteligencia criminal para ayudar a combatir ciertos tipos de delitos y apoyar en investigaciones (en

Por esta razón no estudio temas como la retención y la minería de datos y la protección de datos personales, sino que sólo los señalo para explicar el marco general de la inteligencia estatal en relación con la vigilancia estatal personalizada. No analizo legislaciones y casos judiciales que son relevantes para el tema de la vigilancia estatal en general ya que la profundidad de ese tema rebasa el alcance de este trabajo [6].

Lo primero a señalar de la vigilancia estatal en general es que se trata de una práctica estatal que está en tensión con los principios más básicos de las sociedades democráticas [7]. En el mundo actual las Tecnologías de la Información y la Comunicación (TIC) permiten recolectar información de formas que colisionan con el derecho a la privacidad, y -en teoría- los Estados deben ajustar sus acciones para protegerlo en el entorno digital, y para ello deben establecer una prohibición general para la vigilancia. La intimidad y la privacidad pueden limitarse cuando la ley establece los casos excepcionales en que se permite vigilar para proteger ciertos objetivos legítimos,

---

relación con el crimen organizado, por ejemplo). Al respecto ver: ADC: *Ciberseguridad*…op. cit., pp. 49-52.

6 En este sentido, decisiones relevantes como el caso "Halabi", legislación como la ley 25.891 y reglamentación como el Reglamento de Calidad de los Servicios de Telecomunicaciones, quedan fuera del estudio central de este trabajo. Sucede lo mismo, también, con la Ley de Datos Personales y los poderes excesivos de almacenamiento, tratamiento y cesión que tiene el Estado sobre la misma, y que han sido criticados en otros lugares. Para ver un análisis más completo al respecto ver: ADC, *El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos*, 2014; y Ferrari, Verónica y Schnidrig, Daniela, *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina*, EFF-CELE, agosto de 2016.

7 Naciones Unidas. 2014. A/RES/68/167, 21 de enero de 2014, "Resolución 68/167: El derecho a la privacidad en la era digital". Disponible en: http://www.un.org/es/comun/docs/?symbol=A/RES/68/167. En sentido similar: "La utilización de artificios tecnológicos para conocer conversaciones, información o comunicaciones de otros en general es una forma de injerencia no autorizada en la intimidad de las personas", en Ipohorski, José, "El Derecho a la Intimidad", en Gargarella, Roberto y Guidi, Sebastián (Coords.), Coment*arios de la Constitución de la Nación Argentina. Jurisprudencia y doctrina: una mirada igualitaria*, Buenos Aires, La Ley, Tomo II, 2016, p. 505.

como por ejemplo, los del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) [8].

La vigilancia estatal suele justificarse en el discurso de aumento a la seguridad, donde la privacidad es un costo que vale la pena pagar aun cuando ésta sea necesaria para que las personas ejerzan su gama más amplia de derechos [9]. Pero este discurso tiene muchos problemas. El primero, es que dar un cheque en blanco al Estado para vigilar sin controles implica un riesgo no sólo para la privacidad sino para la propia seguridad, integridad, vida y patrimonio de las personas vigiladas. Cuando el poder coercitivo y el aparato estatal se despliegan en secreto, sin contrapesos ni controles democráticos, el Estado se convierte en un peligro real para todas las personas [10].

Un segundo problema del discurso de *seguridad vs. privacidad* es que la normalización de las acciones de inteligencia (sin controles) se plantea como la única forma de realizarlas efectivamente y esto no es así. Un enfoque de derechos humanos permite armonizar la vigilancia estatal con éstos, estableciéndolos como condición para que los Estados mantengan su legitimidad política. Un ejemplo (que desarrollo en el punto II. son los controles de transparencia para saber el volumen y alcance de las medidas de vigilancia; la transparencia es necesaria y viable, además de que favorece la deliberación pública de este tema y protege indirectamente a la privacidad [11].

---

8 Comité de Derechos Humanos, Comentario General No. 16 (1988), Derecho a la Intimidad (artículo 17). Disponible en: http://hrlibrary.umn.edu/hrcommittee/Sgencom16.html. Así: "Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones".

9 Brito, Carlos y Narváez Herrasti, Santiago, "Medir y acotar la vigilancia estatal para no perder derechos", en Bianchi, Matías (Comp.), *Recuperar la Política. Agendas de Innovación Política en América Latina*, Buenos Aires, Argentina, Asuntos del Sur-Democracia en Red, 2017, p. 298; B. Rule, James. *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, New York, Oxford University Press, 2007, p. 3.

10 Brito, Carlos y Narváez Herrasti, Santiago, "Medir y acotar la vigilancia estatal…" p. 299.

11 Brito, Carlos y Narváez Herrasti, Santiago, "Medir y acotar la vigilancia estatal…", p. 309.

Sacrificar la privacidad para contar con servicios de inteligencia sin controles es una idea autoritaria. Su origen está en los regímenes militares del siglo pasado y sus resultados son bastante claros en toda la región (exploro esto en el apartado IV). Por eso durante años la sociedad civil, la academia y otros grupos han trabajado en la construcción de alternativas que democraticen a los servicios de inteligencia. Esto es así porque la vigilancia también tiene efectos directos en la vida diaria.

Saberse vigilado lleva muchas veces a inhibir la actividad política y el disenso, generando una espiral del silencio que es incompatible con los derechos (no es poco que el Estado sepa qué hacemos, con quién hablamos y qué intercambiamos en nuestras redes sociales) [12]. La vigilancia estatal genera que las personas "se encierren en sí mismas", reservándose de realizar acciones y comunicaciones que normalmente harían si no se supieran vigiladas. La intimidación que resulta de ello puede llevar a que la gente se abstenga de exigir al gobierno que rinda cuentas, de protestar ante injusticias, etc., y también puede aumentar la brecha entre los gobernantes y gobernados, sirviendo como caldo de cultivo para la corrupción y la impunidad [13].

Evitar esto sólo es posible conociendo el alcance, la naturaleza y la forma de aplicación de las medidas de vigilancia, y esto sólo puede pasar si se interviene adecuadamente en los órganos encargados de

12 Brito, Carlos y Narváez Herrasti, Santiago, "Medir y acotar la vigilancia estatal…", p. 299; en el mismo sentido: Stoycheff, Elizabeth, "Under Surveillance: Examing Facebooks Spiral of Silence in Wake of NSA Internet Monitoring", Journalism & Mass Communication Quarterly, 2016, p. 305. Disponible en http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255, y PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, 2013, p. 3. Disponible en: https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

13 Elster, Jon, *La explicación del comportamiento social*, trad. Horacio Pons, Barcelona, Gedisa, 2010, p. 378; así, "[… la intromisión sistemática en la intimidad de opositores y críticos es la práctica a la que recurren determinadas facciones en su circunstancial ejercicio del poder estatal para consolidarse y así evitar, no sólo las críticas a su actuación, sino también toda alternancia en el manejo estatal que podría poner en riesgo su consolidación hegemónica, la que generalmente lleva a abusos, corrupción y mala gestión de asuntos públicos y por ende, pérdida de bienestar en la mayoría de la población", en: Ipohorski, José, op. cit. *supra* en nota 7, p. 513.

ella. No es una cuestión de todo o nada, los Estados necesitan realizar labores de inteligencia para enfrentar realidades como el crimen organizado, el narcotráfico y el terrorismo; pero también necesitan la legitimidad democrática que da el respeto a los derechos humanos, donde la privacidad es central.

Ésta es una tarea difícil particularmente en el espionaje estatal, ya que su práctica es difícilmente detectable y requiere de herramientas de investigación altamente especializadas y de un estudio multidisciplinario (donde participen las víctimas del espionaje, especialistas en TIC, políticos y sociedad civil interesada en el tema). Esto es porque el *malware* (o *software malicioso*) que se utiliza para infiltrar, por ejemplo, los teléfonos celulares de las víctimas de espionaje, se disfraza de mensajes encubiertos que aparentan ser legítimos pero que infectan el dispositivo una vez que son abiertos (con *links* o supuestos documentos *pdf* que al abrirse activan el programa que toma el control del dispositivo) [14], por lo que contar con las personas que sufrieron los intentos de infección, las que investigan-analizan los mensajes y las interesadas en proteger, difundir y establecer los controles para evitar esta práctica es indispensable.

El caso de Argentina es interesante ya que sus servicios de inteligencia están vinculados a violaciones de derechos humanos desde hace décadas [15]: las dictaduras espiaron sistemáticamente a los grupos que les criticaban y se les oponían [16]. Esto llevó a intentar "desmilitarizar la seguridad interior" a través de la transformación institucional post dictadura cívico-militar, que implicó que las tareas

14 Brito, Carlos y Narváez Herrasti, Santiago, "Medir y acotar la vigilancia estatal…", pp. 325-326.

15 En este sentido es interesante recordar lo que hace décadas fue señalado por Carlos Nino, quien reconoció que "…en la sociedad argentina todo el mundo sospecha que su derecho a la intimidad es recurrentemente violado por intercepciones telefónicas y de correspondencia […] (sobre todo de los distintos servicios de inteligencia) […]", Nino, Carlos S., "Proyecto de Constitución del Centro de Estudios Institucionales", en *Una teoría de la justicia para la democracia*, Buenos Aires, Siglo XXI, 2013.

16 Asociación de Derechos Civiles, *Quién vigila a quienes vigilan. Estudio comparativo sobre sistemas de control de los organismos de inteligencia*. Argentina, mayo de 2014, pp. 1-2.

de inteligencia abandonaran la lógica intervencionista relacionada con la doctrina de la seguridad nacional (en la que las dictaduras militares del cono sur se apoyaron para actuar) [17], para que las tareas de combate al terrorismo y al narcotráfico quedaran fuera de la jurisdicción del Ejército [18].

A la pregunta de dónde estamos en el estado de la vigilancia y el respeto de los derechos, la respuesta es poco alentadora. La vulneración constante del derecho a la intimidad resulta probablemente de que los gobiernos democráticos post-dictadura vieron en los sistemas de inteligencia un círculo de poder para utilizar en su favor (ya no un coto de poder negociado con el Ejército, resultado de una transición negociada para salir de la dictadura) [19]. Esto muestra una situación que parece cada vez más homogénea en los gobiernos formalmente democráticos en la región: el uso político antidemocrático de la vigilancia estatal para fines personales de los gobiernos en turno.

Pero para entender los cambios institucionales y el panorama político y social alrededor del tema del espionaje y del rol de los servicios de inteligencia es necesario pasar por su andamiaje legal y hacer un breve paso por su desarrollo histórico, particularmente durante las últimas cuatro décadas.

17 Desde los primeros años del regreso de la democracia, se intentó tener esta ruptura con el foro castrense a través de dos leyes: la ley de Defensa Nacional (1988) y la ley de Seguridad Interior (1992). A partir de ellas se inició la separación de la doctrina de seguridad nacional que permitió el uso del aparato represivo del Estado en la última dictadura. Con ellas se intentó marcar una diferencia clara entre las actividades de defensa nacional (amenazas externas a la soberanía) y las de seguridad nacional (situaciones internas como el narcotráfico y el terrorismo). ADC: *El (des)control democrático de los organismos de inteligencia en Argentina*, Argentina, Enero de 2015, pp. 12-13.

18 *Ibid*, pp. 5-6. Ver también Marcelo Fabián Saín, "Las 'nuevas amenazas' y las Fuerzas Armadas en la Argentina de los '90", en XXIII International Congress Latin American Studies Association (LASA), Washington, DC, United States 6-8 de septiembre de 2001.

19 ADC, *El (des)control democrático,* op. cit., pp. 6-7.

II. El marco jurídico internacional y nacional de protección y controles democráticos a la vigilancia estatal

a. Los estándares internacionales y regionales sobre vigilancia estatal

La vigilancia estatal es compatible con una sociedad democrática siempre que se mantenga dentro de un marco de controles que sirven como protección a los derechos a la privacidad, la inviolabilidad de las comunicaciones privadas y la libertad de expresión: i) que los alcances de la vigilancia se regulen en leyes claras y detalladas; ii) que los límites a la privacidad sean necesarios y proporcionales; iii) que exista el control judicial de la intervención de comunicaciones; y iv) que existan mecanismos de fiscalización y rendición de cuentas que aseguren la transparencia de esta práctica estatal [20].

• *Los alcances y límites de la vigilancia estatal -la justificación para realizar las medidas de vigilancia, su naturaleza, alcance y duración, las razones para ordenarla, las autoridades facultadas para llevarlas a cabo y los medios legales de impugnación- deben estar contenidos en leyes que no sean vagas ni ambiguas*

La regulación de la vigilancia estatal no debe ser vaga ni ambigua, debe ser redactada de manera clara y precisa **en una ley formal y materialmente**. Esto permite que las personas sepan de qué va la vigilancia y entiendan en qué situaciones podrían ser vigiladas [21]. Dado que la vigilancia estatal es generalmente encubierta (por su secrecía), las leyes deben plantearse de modo que las

20 R3D, *El Estado de la Vigilancia...* op. cit. *supra* en nota 2, pp. 8-14. Como se muestra en este apartado, este *set* de controles es resultado del marco internacional y regional del derecho a la privacidad, las decisiones de organismos especializados al respecto y el desarrollo de los estándares de protección sobre este derecho desde distintos sectores (sociedad civil, gobiernos, academia, empresas, etc.).

21 *Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Declaración Conjunta sobre Programas de Vigilancia y su Impacto para la Libertad de Expresión*, 21 de junio de 2013, ¶12. *Disponible en http://ow.ly/N3jS30dSuuq*.

personas sepan las circunstancias y casos en que las autoridades competentes pueden actuar [22]. La jurisprudencia internacional ha señalado que en estos casos las leyes deben ser particularmente precisas por el riesgo que todos los sistemas de vigilancia implican por sí mismos [23].

Esto es un problema grave en Argentina porque muchas de las normas sobre vigilancia no han sido establecidas por la vía legislativa sino por decretos presidenciales. Esto refleja el problema profundo (además de contravenir los estándares de derechos humanos que el gobierno dice respetar), de que pareciera que a la clase política le importa poco o nada llevar a cabo una deliberación seria sobre la vigilancia estatal, las responsabilidades por sus abusos y la mejor manera de reglamentarla para que sirva a los intereses de las personas y no a los de los grupos en el poder.

• *Las medidas de vigilancia estatal que limiten la privacidad deben ser necesarias y proporcionales*

Aunque una medida sea útil para lograr el objetivo que persigue (por ejemplo, combatir la criminalidad), eso no la vuelve *legítima per se*. Para que las autoridades puedan utilizarla, debe ser la alternativa menos lesiva al derecho para lograr el objetivo legítimo (necesidad), y la lesión que causa no debe ser desmedida frente a sus ventajas (proporcionalidad). Esto obliga a ponderar las ventajas de la medida con sus costos para asegurarse que los derechos no sean afectados de manera desproporcional [24].

Por esto la vigilancia *masiva* es incompatible con el derecho a la privacidad, ya que lesiona indiscriminadamente los derechos de muchas personas. **Sucede lo mismo con el espionaje estatal**; utilizar *malware* (*software* malicioso) para intentar infectar dispositivos de personas es en principio un método ilegítimo de interferen-

22 R3D, *El Estado de la Vigilancia*… op. cit., p. 9.

23 TEDH. Caso de Uzun vs. Alemania. Aplicación No. 35623/05. Sentencia de 2 de septiembre de 2010, párr. 61; Weber y Sarabia vs. Alemania. Aplicación No. 54934/00. Decisión de 29 de Junio de 2006. párr. 93; Caso de Valenzuela Contreras vs. España. Aplicación No. 58/1997/842/1048. Sentencia de 30 de Julio de 1998, párr. 46.

24 R3D, *El Estado de la Vigilancia*… op. cit., pp. 9-10.

cia en la privacidad. El control de los dispositivos una vez que son infectados es enorme y controlar su abuso es realmente difícil. Por un lado se obtiene información sin límites (desde recolectar los datos hasta activar la cámara y grabar o implantar archivos); por otro lado, lo sofisticado de esta práctica y el que no requiera de un tercero para realizar la infección la hace muy difícil de detectar. En el mejor de los casos, debería estar limitada solamente para las circunstancias más extremas y **sí y sólo sí** se contare con los controles de la revisión judicial, la transparencia y la supervisión independiente [25].

Además, esta práctica difícilmente resiste un *test* de necesidad y proporcionalidad (tal como exigen los estándares internacionales y regionales de derechos humanos). Esto debe ser siempre contrastado con el uso del espionaje estatal en la práctica; cuando sucede que, tal como pasa en el caso argentino, el Estado utiliza las acciones de vigilancia para realizar espionaje civil o político, el aparato de inteligencia se utiliza con fines no democráticos [26].

• *Como regla general, toda interferencia con el derecho a la privacidad debe ser autorizada previamente por una jueza o juez competente que evalúe la legitimidad de la medida solicitada*

Para sujetar la vigilancia al mínimo indispensable de evaluación y control, es necesario que un tercero intervenga en su práctica, ya que en caso contrario todas las medidas se mantendrían en secreto y las personas vigiladas no tendrían conocimiento de ello [27]. La vigilancia sin control judicial representa la ausencia de supervisión de este tipo de acciones estatales, dejando al arbitrio de las autoridades facultadas para realizarla el comportarse respetando los derechos de las personas o el abusar de dicho poder.

Las autoridades judiciales deben ser independientes y deben asegurarse que la medida de vigilancia es idónea para lograr los fines

25 R3D, *El Estado de la Vigilancia…* op. cit. *supra* en nota 2, p. 11.

26 Thomas C. Bruneau y Steven C. Boraz, "Intelligence reform: Balancing democracy and effectiveness", en Thomas C. Bruneau y Steven C. Boraz, editores, *Reforming Intelligence. Obstacles to Democratic Control and Effectiveness*, páginas 1-24. University of Texas Press, Austin, 2007. Citado en Ibid, p. 10.

27 R3D, *El Estado de la Vigilancia…* op. cit. *supra* en nota 2, p. 11.

que persigue, además de que cumpla los criterios de necesidad y proporcionalidad. Esto hace que la revisión judicial de las acciones de vigilancia estatal sea una condición necesaria de su legitimidad y que, en sentido contrario, la ausencia de controles judiciales sobre estas acciones sea ilegítima e injustificable desde un enfoque de derechos humanos [28].

Esto no significa que la autorización judicial sea absoluta, sino que como regla general no debe desplazarse. En casos de extrema urgencia, como cuando se encuentre en riesgo la vida de una persona o en casos de secuestro donde se necesite actuar de manera expedita, es viable -y acorde a los estándares internacionales en la materia- contar con un mecanismo de emergencia en que se autorice una medida de intervención de comunicaciones sin que medie una orden judicial, siempre que esta acción sea simultáneamente notificada a una autoridad judicial y que esta última tenga que revisarla dentro de un plazo razonable y expedito (dentro de las 24 horas de realizada la intervención, por ejemplo) para determinar su legitimidad o para ponerle fin [29]. Este mecanismo de control judicial simultáneo permitiría actuar en emergencias para proteger valo-

28 CIDH, *Libertad de Expresión e Internet*, op. cit. *supra* en nota 3, párr. 165. Ver también el principio de "Autoridad Judicial Competente", de los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. En el caso argentino, esto podría ser un problema dado que el órgano que actualmente se encarga de la autorizar la intervención de comunicaciones privadas pertenece al Poder Judicial. Me ocupo de esto en las conclusiones.

29 "De esta manera, la autorización judicial posterior tendría efectos retroactivos, o en su defecto, la negativa de dicha autorización debería conducir a la subsanación de los defectos de la solicitud o a la destrucción de los datos obtenidos y, en su caso, la imposición de sanciones por la utilización abusiva del mecanismo de emergencia". R3D, *El Estado de la Vigilancia…* op. cit., p. 12; sucede lo mismo con el principio de "Debido Proceso" de los *Principios Internacionales sobre Vigilancia*: "[…] al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo".

res fundamentales como la seguridad, la integridad o la vida y, al mismo tiempo, mantener bajo controles democráticos el poder de la vigilancia estatal.

• *La vigilancia estatal debe estar acompañada de mecanismos que aseguren su transparencia y rendición de cuentas; la supervisión independiente y el derecho de notificación son fundamentales*

La Asamblea General de la ONU ha recomendado contar con mecanismos de supervisión independientes y efectivos que permitan lograr transparencia y rendición de cuentas en las acciones de vigilancia estatal [30]. La exigencia de mecanismos para analizar la legalidad y legitimidad de las acciones de vigilancia es receptada en el principio 10 de los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (en adelante *Principios Internacionales sobre Vigilancia*). Dichos organismos deberían tener facultades para poder revisar la información confidencial o reservada, realizar informes públicos y poder investigar y denunciar los abusos en la vigilancia estatal [31].

Esto subraya la obligación estatal de publicar informes de solicitudes de intercepciones de comunicaciones aprobadas y rechazadas, su desagregación por proveedor de servicios y por investigación y propósito [32]. Para lograrlo, esta garantía debe contenerse en leyes que la habiliten y permitan al público entender los alcances de la vigilancia [33]. La oposición que comúnmente se hace a la exigencia de publicidad se ampara en una versión anacrónica de la Seguridad

30 Naciones Unidas, "El derecho a la privacidad en la era digital"… op. cit. *supra* en nota 7.

31 R3D, *El Estado de la Vigilancia. Fuera de Control*, México, Noviembre de 2016, p. 14.

32 ONU. Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de abril de 2013. A/HRC/23/40. Disponible en inglés en http://ow.ly/zfLo30dSu8C. En el mismo sentido: CIDH, *Libertad de Expresión e Internet*, op. cit. *supra* en nota 3.

33 *Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Declaración Conjunta sobre Programas de Vigilancia y su*

Nacional, que dice que los servicios y actividades de inteligencia deben permanecer obscuros y lejos del escrutinio público y el control porque en caso contrario las labores de seguridad no pueden realizarse.

Pero la transparencia y el respeto a la privacidad son compatibles con la Seguridad Nacional. Parte de los esfuerzos para salir de la lógica de seguridad sostenida por los gobiernos militares del siglo pasado está contenida en los instrumentos que armonizan las necesidades de seguridad nacional de los Estados con los derechos humanos. Los *Principios de Tshwane* establecen que la información sobre la vigilancia estatal se considera como una categoría sobre la que existe un fuerte interés a favor de su divulgación, y que esto trae la obligación de dar a conocer las leyes y reglamentaciones de todas las formas de vigilancia secreta, las medidas de vigilancia permitidas, su duración, las entidades facultadas para realizarlas, la información estadística de las autorizaciones de intercepción, los casos conocidos de vigilancia ilegal, entre otras [34].

Esta idea es sostenida también por grupos de sociedad civil, expertos y expertas internacionales en materia de vigilancia estatal y grupos de la industria relacionada, quienes han reconocido la necesidad de la transparencia en las acciones de vigilancia a través de los *Principios Internacionales sobre Vigilancia* [35].

Estas disposiciones muestran que es posible tener mecanismos para evaluar cómo se realiza la vigilancia estatal (si se hace o no de manera legal), su efectividad y el cumplimiento de los estándares mínimos necesarios (contar con controles y cerciorarse de su efectividad) para su ejercicio de manera democrática (y para controlar y sancionar los abusos de esta práctica). Las únicas doctrinas de la Seguridad Nacional que son incompatibles con estos estándares son aquellas que parten de una lógica totalitaria que pone en el centro al Ejército frente a los poderes públi-

---

Impacto para la Libertad de Expresión, 21 de junio de 2013, ¶12. *Disponible en http://ow.ly/N3jS30dSuuq*.

34 Principios Globales sobre Seguridad Nacional y el Derecho a la Información ("Principios de Tshwane"), Tshwane, Sudáfrica, 12 de junio de 2013. Disponibles en http://ow.ly/eC6B30dSNrG.

35 *Principios Internacionales sobre Vigilancia*. Principio de TRANSPARENCIA.

cos y a la democracia. En su carácter antidemocrático radica su ilegitimidad y esto es suficiente para descartarlas como opciones razonables en una democracia. Como menciono en los apartados I. y IV., salir de esta lógica es precisamente lo que la sociedad argentina y sus gobiernos civiles se han propuesto en las últimas cuatro décadas.

El espionaje estatal es mucho más complicado que la vigilancia estatal en general porque no requiere de la participación o colaboración de las empresas de telecomunicaciones (evitando por completo la transparencia), y esto genera un obstáculo extra (al de la secrecía con la que funcionan los servicios de inteligencia y la intervención de comunicaciones en general) para la detección de las personas espiadas (en este caso de la infección de los dispositivos por las que son espiadas). La exigencia de una auditoría independiente y seria aumenta por dos razones complementarias a las ya expuestas: i) que por sus características, el espionaje estatal puede eludir el control judicial (por su difícil detección) y, ii) que puede ser una puerta abierta para realizar actos de corrupción (por los costos elevados de recursos que implica, la opacidad de los procesos de adquisición de los *software maliciosos -malware-* y la práctica con la que los gobiernos se acercan a las empresas que los proporcionan) [36].

Finalmente, este problema ha llevado a reconocer la salvaguarda del **derecho de notificación** a las personas que fueron blanco de vigilancia estatal (en todas sus formas). Esto obliga a que: i) se notifique a la persona que sus comunicaciones fueron intervenidas, ii) tan pronto como cuando dicha notificación no ponga en riesgo la efectividad de la vigilancia (lo más pronto posible), y iii) exista la posibilidad de exigir la reparación por el uso incorrecto de las medidas de vigilancia [37]. Esto permite pensar en mecanismos de notificación diferida en los que las personas son informadas que fueron vigiladas cuando la medida de vigilancia no está en riesgo, para que acuda "**a los mecanismos jurídicos que considere pertinentes para**

36 Brito, Carlos y Narváez Herrasti, Santiago, "Medir y acotar la vigilancia estatal…", op. cit., pp. 320-321.

37 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de abril de 2013. A/HRC/23/40.

remediar posibles abusos sin que se obstaculice de forma alguna la actividad legítima de alguna autoridad" [38].

b. El marco jurídico argentino sobre la vigilancia estatal

1. La Constitución Nacional y el marco legal de la Ciudad Autónoma de Buenos Aires

La Constitución argentina protege el derecho a la intimidad y el derecho a la privacidad de manera articulada. Aunque ambos términos suelen tomarse de manera indistinta, en el caso argentino es útil adaptar la delimitación metodológica establecida por Carlos Nino, en la que el ámbito de la privacidad (entendido como la protección de la autonomía personal y el plan de vida, libre de intervención del Estado) se encuentra en el artículo 19 constitucional, mientras que el ámbito de la intimidad (entendido como la protección de la esfera personal exenta del conocimiento de las demás personas, donde el Estado puede intervenir en casos excepcionales) está en el artículo 18, particularmente en cuanto a las comunicaciones privadas [39]. Esto es lo que provoca que se hable de la idea amplia de la privacidad (relacionada con la autonomía) y su complemento con una visión concreta de la intimidad [40].

38 R3D, *El Estado de la Vigilancia…* op. cit., p. 14. El Tribunal Europeo de Derechos Humanos reconoció el estándar de la notificación diferida en el menor tiempo posible en "Elimdzhiev vs. Bulgaria".

39 Nino, Carlos Santiago, *Fundamentos de derecho constitucional,* Buenos Aires, Astrea, 2000, pp. 304, 327, 333. Estos artículos establecen que: "Artículo 18. […] *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…* (*Énfasis mío*) […]; Artículo 19. 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".

40 Esto porque decir que la privacidad está libre de la interferencia estatal se refiere a las acciones que permiten a las personas desarrollar su vida y tomar sus decisiones, mientras que en el caso de la intimidad su análisis se complementa con la idea del daño a terceros, lo que justifica la intervención del Estado: como ejemplo, el Estado no puede sancionar las relaciones homosexuales consensuadas, pero sí intervenir en casos de violencia de género en el

La lectura de ambos artículos se debe hacer a la luz del marco internacional de protección de derechos humanos puesto que éstos son reconocidos a nivel constitucional en virtud del artículo 75.22 (tales como la CADH en su artículo 11.2, la Convención Europea de Derechos Humanos en su artículo 8.1 y el PIDCP en su artículo 17.1). A partir de este marco (y en concordancia también con una interpretación de la legislación nacional vigente), se derivan ciertas prohibiciones claras sobre la vigilancia estatal: i) ninguna actividad de inteligencia sobre investigación criminal puede realizarse sin una orden judicial que la autorice; ii) el espionaje civil o político está expresamente prohibido; iii) la divulgación de información (sobre espionaje que se presupone legítimo) sin orden judicial que la autorice no está permitida [41].

La protección constitucional y legal sobre la privacidad ha sido respaldada por la Corte Suprema argentina en el caso "Halabi", donde -de manera acorde a los estándares interamericanos en la materia- se reconoció que la protección de la inviolabilidad a las comunicaciones privadas alcanzaba a los *metadatos* de éstas (la información sobre las comunicaciones electrónicas incluida Internet, no su contenido). Así, la ley No. 25.873 en materia de retención de datos, que permitía la recolección y almacenamiento de datos sin orden judicial y de forma completamente abierta (que obligaba a las empresas prestadoras de servicios de Internet -ISP- a almacenar por 10 años y a responder a cualquier solicitud de la entonces Dirección de Observaciones Judiciales -DOJ- sin que medie una orden judicial), fue declarada inconstitucional. Aun así esta legislación permanece vigente dado que el fallo se dirigía a un caso concreto y la ley nunca fue expresamente derogada. Si bien este fallo corresponde a la vigilancia estatal en general y no al espionaje estatal, importa señalar el reconocimiento de la Corte Suprema al

hogar. Sin embargo, no debe obviarse que esta distinción metodológica entre intimidad y privacidad no borra los puntos que los hacen interdependientes (y que por ello hace que en otros países y en el ámbito internacional se les conciba bajo la idea amplia del derecho a la privacidad). Al respecto ver: IPOHORSKI, José, "El Derecho a la Intimidad"… cit., pp.481-82, 486; GARGARELLA, Roberto, "Constitucionalismo y privacidad", en *Teoría y crítica del derecho constitucional*, Abeledo-Perrot, Buenos Aires, 2008, pp. 788 y 793.

41 ADC. *El (des)control democrático*… cit., pp. 14-16.

derecho a la privacidad y a los estándares internacionales relacionados [42].

La Corte fue clara al establecer que las acciones de los Estados, incluso las de vigilancia, encuentran sus límites en los derechos fundamentales, tales como los de la privacidad y las comunicaciones privadas, por lo que fijó los requisitos para que la intervención de las comunicaciones estuviera de acuerdo a los estándares interamericanos, a decir: que la intromisión sea contemplada por una ley que esté orientada por un objetivo legítimo o un interés superior (para que esté justificada), que la restricción sea compatible con el fin legítimo y que el medio o acción de interferencia no sea más extenso que lo indispensable para alcanzar el fin particular [43].

La Constitución de la Ciudad Autónoma de Buenos Aires (CABA) emula a la nacional al garantizar el derecho a la privacidad, la intimidad y confidencialidad como partes de la dignidad de todas las personas (artículo 12.3). La intimidad se protege por los funcionarios estatales mediante **el requisito de autorización judicial** en los casos en que se busque allanar el domicilio, realizar escuchas telefónicas o secuestrar papeles y correspondencia o información almacenada (artículo 13.8).

Esto es correspondido en el **Código Procesal Penal de la CABA** (Ley No. 2303/07, del 29 de marzo de 2007), que en su artículo 93 obliga a que los actos de investigación relacionados con allanamientos, requisas o intercepción de comunicaciones se lleven a cabo con una orden judicial previa y, en su artículo 115, establece que la intervención de correspondencia deberá ser autorizada por la autoridad judicial a pedido del o la Fiscal competente (reconociendo que en "casos de urgencia" el Ministerio Público Fiscal puede autorizar la intercepción de comunicaciones). Por su parte, el artículo

42 Como menciona José Ipohorski, la relevancia fundamental de dicho fallo radica también en que se reconoció que todas las comunicaciones reguladas por la ley de Telecomunicaciones, incluidas las que se hacen por Internet o que utilizan aplicaciones de comunicación en teléfonos celulares (como *whatsapp*), son protegidas por el derecho a la intimidad y la privacidad contenidos en los artículos 18 y 19 de la Constitución. Ipohorski, José, "El Derecho a la Intimidad"… cit., p. 493. En el mismo sentido Nino, op. cit. *supra* en nota 15, pp. 500-01.

43 Ferrari, Verónica y Schnidrig, Daniela, *Vigilancia Estatal…* op. cit. *supra* en nota 6, pp. 27-28.

117 subraya que la intercepción de comunicaciones es de carácter excepcional y que puede realizarse solamente durante un periodo de 30 días (renovable solamente por 15 días más una sola vez, en casos justificados ante autoridad judicial).

Dado que la intervención de las comunicaciones privadas se encuentra centralizada en Argentina (por lo que tanto los servidores y servidoras públicas del Ministerio Público Fiscal de la CABA como los de la Nación deben solicitar a un mismo organismo la intercepción de las comunicaciones, como explico en el apartado siguiente), es importante hacer un repaso de la legislación a nivel nacional, puesto que es esclarecedora de la forma en que funciona el entramado de vigilancia estatal.

2. La legislación nacional

El marco legal nacional sobre vigilancia estatal y comunicaciones privadas se distribuye en una red compleja de ordenamientos jurídicos: i) por un lado en la legislación procesal penal, donde se tiene la particularidad de que en la actualidad "existen" dos códigos procesales penales, puesto que el "nuevo Código Procesal Penal" que debería haber entrado en vigor está suspendido por un decreto presidencial que se emitió a finales de 2015 (lo que hace que permanezca vigente el Código Procesal Penal anterior); ii) por otra parte, en la legislación específica sobre inteligencia nacional, a partir de las leyes 25.520 y 27.126 y sus decretos respectivos [44]; y iii) finalmente, en el marco de la regulación sobre telecomunicaciones de la ley "Ar-

44 El nuevo código fue aprobado en noviembre de 2014, y estaba reglamentado que entrara en vigencia el mes de marzo de 2016 (de acuerdo a la ley 27.150, del 17 de junio de 2015). Sin embargo, el decreto 257/2015 pospuso la entrada en vigor, y estableció que fuera una comisión bicameral quien estableciera el nuevo cronograma de su entrada en vigor. Al respecto ver: Ferrari, Verónica y Schnidrig, Daniela, *Vigilancia Estatal…* op. cit. *supra* en nota 6, pp. 8-9.

Por otro lado, la ley de Inteligencia Nacional 25.520 es complementada por la 27.126, quien reforma distintos de sus artículos y modifica algunos de los organismos que la primera establecía. Sin embargo, la estructura de los servicios de inteligencia en la actualidad tampoco corresponde al texto de la ley 27.126, ya que por decreto presidencial éstos pasaron a la órbita del Poder Judicial (decreto 256/2015). Para ver todas las normas que modifican y/o completan a la Ley de Inteligencia Nacional 25.520 ir a: http://servicios.infoleg.gob.ar/infole-

gentina Digital". Como explico más abajo, la articulación compleja de disposiciones lleva muchas veces a que exista vaguedad en las normas relacionadas con la vigilancia estatal y a que no se sepa con certeza cuáles son los límites de esta práctica.

La legislación penal

Para diferenciar ambas legislaciones, primero mencionaré la forma en que el Código Procesal Penal Nacional vigente (en adelante CPPNv) se articula, para después señalar las diferencias con el nuevo Código Procesal Penal Nacional (suspendido por el decreto presidencial, en adelante nCPPN), dado que al momento en que este trabajo fue entregado el primero aún tenía validez y el segundo se mantenía suspendido. En la actualidad el CPPNv protege más el derecho a la intimidad, mientras que el nCPPN contiene problemas de vaguedad y abre distintos riesgos a este derecho.

Si bien es cierto que la forma en que ambos códigos regulan la intervención de las comunicaciones privadas no es tan distinta, y muchas cosas permanecen de la misma manera [45], un par de cambios y modificaciones merecen ser destacadas, particularmente tomando en cuenta que la suspensión del nCPPN eventualmente cesara y éste entrara en vigor.

El CPPNv (Ley N° 23.984, promulgado el 4 de septiembre de 1991), establece en su artículo 236 las reglas correspondientes a la intervención de las comunicaciones privadas, señalando por un lado la exigencia de una orden judicial para la intervención y, por otra parte, un mecanismo excepcional para los casos de secuestro y extorsión (artículos 142 bis y 170 del Código Penal de la Nación): "cuando existiese peligro en la demora, debidamente justificado", donde el representante del Ministerio Público Fiscal podrá realizar el pedido de intervención de las comunicaciones "mediante auto fundado, con inmediata comunicación al Juez, quien deberá convalidarla en el término improrrogable de veinticuatro horas, bajo pena de nulidad del acto y consecuente ineficacia de la prueba introducida a partir

gInternet/verVinculos.do;jsessionid=AF5E3F08B1E49F4706097C5367492432?modo=2&id=70496.

45 Privacy International, *The Right to Privacy in Argentina*, Stake holder Report, Universal Periodic Review, 28th sesión, March 2017, p. 61.

de él". Esta disposición protege el derecho a la privacidad porque mantiene un carácter excepcional que es proporcional al bien que se protege (la libertad y/o la vida) y que es controlado judicialmente en un tiempo razonable para evitar el uso arbitrario de la figura.

Del mismo modo, la requisa domiciliaria o allanamiento y los registros se pueden delegar a los fiscales si la jueza en cuestión así lo decide, en los casos en que "hubiere motivo para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito, o que allí puede efectuarse la detención del imputado o de alguna persona evadida o sospechada de criminalidad" (artículo 224) [46]. Como complemento a esto, el artículo 227 establece todos los casos en que la orden judicial es innecesaria, y en este caso el inciso 5 es particularmente relevante ya que regla que esto es así cuando "Se tenga sospechas fundadas de que en una casa o local se encuentra la víctima de una privación ilegal de la libertad y corra peligro inminente su vida o integridad física", habilitando a un "representante del Ministerio Público Fiscal". Haciendo una interpretación de estos artículos -aunque no refieren específicamente a las comunicaciones digitales o a posibles medidas de espionaje estatal en casos excepcionales-, ambos podrían utilizarse para habilitar la intervención a las comunicaciones, aunque deberían ser posteriormente notificadas a una jueza o juez para que las validara o rechazara (utilizando el mecanismo de urgencia).

El nCPPN, por su parte, reconoce en su artículo 13 la protección al derecho a la intimidad y la privacidad, así como a las comunicaciones privadas, estableciendo el requisito de la autorización judicial para realizar intervenciones.

En su artículo 143 establece las reglas generales para la intercepción de comunicaciones: el control judicial es condición necesaria (a pedido, en este caso, del Ministerio Público Fiscal), la intervención debe ser por tiempo definido (máximo 30 días renovables si hay motivos que justifiquen la extensión) y su solicitud debe especificar el tiempo que se solicita y justificarlo, además de señalarse que la autoridad facultada para interceptar las comunicaciones incurre en responsabilidad penal si falta a su deber de confidencialidad y secreto, así como que las empresas de telecomunicaciones están obligadas a cumplir con la orden so apercibimiento de responsabilidad pe-

46 Ibid, p. 57.

nal. Sin embargo, el párrafo 2º dice que deberá procederse de forma análoga al allanamiento (en particular en relación al artículo 135, inciso e), que establece los casos en que no se requiere de orden judicial para realizarse [47]. Esto es problemático porque, primero, abre la puerta a que sea la policía o cualquier "otra fuerza de seguridad" quien actúe sin orden judicial, generando una excepción extremadamente amplia y vaga.

En los casos de urgencia, no es irrazonable que las autoridades actúen sin orden judicial, siempre que se basen "en pautas objetivas que posibiliten el control judicial posterior de la legitimidad de la medida"; es decir, que en casos excepcionales se puede actuar para salvaguardar -por ejemplo- la integridad o la vida de una persona, pero todas las decisiones de las autoridades -incluso éstas- deben ser revisadas posteriormente por una jueza o juez competente para que no sean ilegítimas. El ejemplo más claro del ordenamiento argentino corresponde al allanamiento en casos de secuestros para liberar a la víctima, donde puede entenderse la razonabilidad de la acción de las autoridades sin orden judicial previa, y exigirse posteriormente la revisión de la constitucionalidad de la medida por dichas autoridades [48].

Sumado a esto, en septiembre de 2016 se presentó una propuesta de reforma legislativa al nCPPN, que incluye -como métodos de investigación común- la vigilancia remota de equipos electrónicos, la vigilancia por medio de localización y monitoreo y, en particular, el *hackeo* como un método legal de investigación (sin definir concretamente qué se entiende por esta figura, aludiendo sólo al uso de *software* que permite facilitar el acceso remoto a dispositivos electrónicos), abriendo esta práctica a la discrecionalidad de dichas

47 Así, la disposición en cuestión establece, en particular en su inciso e), que:

"Artículo 135.- *Allanamiento sin orden judicial.* No obstante lo dispuesto en los artículos anteriores de este Título, la policía u otra fuerza de seguridad podrán proceder al allanamiento sin previa orden judicial si:

[…]

e) Se tuvieren sospechas fundadas de 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".

48 Ipohorski, José, "El Derecho a la Intimidad"… op. cit., pp. 497-98.

autoridades (y con el problema particular de no especificar cuáles serían las autoridades relevantes que podrían realizar el acceso remoto o *hackeo*) [49].

La legislación sobre Inteligencia Nacional

La ley 25.520 reconoce en su artículo 1º que la vigilancia estatal debe ser acorde a lo establecido en los Tratados internacionales suscriptos por Argentina. La garantía de orden judicial está en los artículos 4, 5, 18 y 19 de la ley de Inteligencia Nacional. Este requisito es reconocido como la mejor garantía en contra de abusos de las autoridades, ya no sólo en los estándares internacionales sino por la propia doctrina argentina, donde se recuerda que la intromisión del Estado en la intimidad de las personas debe estar justificada por una jueza o un juez [50].

Las disposiciones de la Ley de Inteligencia Nacional establecen que toda intervención de comunicaciones privadas, de cualquier tipo, debe hacerse mediando la intervención judicial federal, donde la Agencia Federal de Investigación (anteriormente Secretaría de Inteligencia) vía el Secretario de Inteligencia o un funcionario expresamente facultado, debe solicitar la autorización ante un juez federal penal con competencia, y cuya autorización debe darse por escrito, con instrucciones precisas y detalladas sobre la intervención (números a intervenir, especificidades del medio electrónico, etc.) [51]. Dicha autorización no puede exceder los 60 días y sólo puede repe-

49 Esto en el Título VI "Medidas especiales de investigación", Capítulo 3 "Vigilancia", artículo 175 decies, undecies, duodecies, terdecies. El texto completo de la propuesta puede consultarse en: https://www.justicia2020.gob.ar/wp-content/uploads/2016/09/texto-final-del-proyecto-reforma-CPP.pdf. Al respecto ver: Privacy International, *The Right to Privacy in Argentina*… op. cit. *supra* en nota 45, p. 8.

50 Ipohorski, José, "El Derecho a la Intimidad"… op. cit., p. 493. En el mismo sentido Nino en su "Proyecto de Constitución del Centro de Estudios Institucionales", op. cit., p. 246.

51 ADC. *El (des)control democrático*… pp. 17-19. Efectivamente, la AFI puede solicitar a un juez una intervención en casos de producción de inteligencia criminal (sobre delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, ciberdelitos, delitos contra el orden económico y financiero, contra los poderes públicos y el orden constitucional. Al

tirse por otros 60 cuando sea imprescindible para la investigación (artículo 19).

En cuanto a la transparencia, la ley contempla en su artículo 13.9 una obligación que queda lejos de ser efectiva: la ahora AFI debería "Elaborar el informe anual de actividades de inteligencia a los efectos de su presentación ante la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia del Congreso de la Nación. A tales efectos, los organismos del Sistema de Inteligencia Nacional le deberán brindar toda la información correspondiente", para que dicha Comisión los revise. No obstante, dado el candado que existe en su artículo 16 (que condiciona el acceso a la información por el Presidente de la Nación o el funcionario en que se delegue esa facultad), en la práctica la regla general es la secrecía. Esto hace que el organismo funcione en sentido contrario a una lógica de protección a la privacidad.

El marco jurídico de protección parece mantenerse también después del complemento de la ley 27.126 y los decretos posteriores (mencionados más arriba). Sin embargo, con el paso de este organismo al Poder Judicial por medio del decreto de necesidad y urgencia 256/2015, se abrió una ventana de vaguedad para el control judicial tal como se encontraba anteriormente (desarrollo el punto del diseño institucional actual de la vigilancia estatal en el apartado siguiente).

La Acordada 2/2016 de la Corte Suprema (del 15 de febrero de 2016) reconoce como su marco jurídico las disposiciones jurídicas contenidas en la Ley de Telecomunicaciones 19.798 (su artículo 45 bis), la ley 25.520 (explicada arriba) y la Ley de Tecnologías de la Información y las Comunicaciones (ley "Argentina Digital") 27.078 (en su artículo 62). Así creó la Dirección de Captación de Comunicaciones del Poder Judicial de la Nación (DCC), quien tendría autonomía de gestión frente a la Corte aunque ésta podría modificar su estructura y revocar el mandato de sus autoridades por "incumplimientos graves" (artículo 1º).

La principal crítica desde un enfoque de derechos humanos se encuentra en la ambigüedad en su artículo 2º, donde establece que actuará ante los requerimientos de intercepción tanto de "magistra-

---

respecto ver: Privacy International. *The Right to Privacy in Argentina*… pp. 31 *et seq*.

dos judiciales" como de "los del Ministerio Público Fiscal" [52]. Esto abre una zona gris que puede permitir interpretaciones contrarias al derecho a la privacidad, tal como la que resultaría de conceder que el MPF pueda activar las acciones de intercepción sin pasar por un control judicial. Esto sería inconsistente con el resto de la legislación relacionada con la protección a la privacidad y con el propio principio de "Transparencia y Confidencialidad" reconocido en la Acordada, donde se establece que "En todos los casos se ajustará estrictamente a las normas legales vigentes **y a las órdenes judiciales**" (*énfasis mío*).

Como preocupación adicional está el reconocimiento de la "minería de datos" para "descubrir patrones en grandes volúmenes de conjuntos de datos" para su uso en "colaboración con los operadores jurídicos". Esta disposición es vaga (¿qué operadores? ¿bajo qué parámetros? ¿con qué garantías de privacidad?) pero también es un problema por la invasión desproporcional a información que puede ser sensible. Otro espacio de vaguedad es el principio de "Nuevas tecnologías de investigación", al señalar que "Se procurará la actualización de la tecnología disponible y la incorporación de métodos alternativos de intervención referidos a los nuevos modos de comunicación en estrategias delictivas". Esto, en relación con el 2º párrafo del principio de transparencia (que pareciera contradictorio con el primero) que dice: "Establecer una reserva absoluta de la información y, respecto del personal, evaluar la realización de contratos de confidencialidad respecto de la información y de los métodos de trabajo y colaboración con los operadores jurídicos", puede ser una caja negra donde se utilicen tecnologías de espionaje contrarias al derecho a la privacidad, sin poder advertirlo.

Meses después, a través de otra Acordada (30/2016), la estructura y facultades fueron modificadas nuevamente. La DCC fue sustituida por la Dirección de Asistencia Judicial en Delitos Complejos Crimen Organizado del Poder Judicial de la Nación (DAJDCCO), quien tendría las mismas competencias, más las que se sumaron en esta nueva Acordada. En ella se mantiene el riesgo de una interpretación contraria al derecho a la privacidad, ya que en la intervención a comunicaciones privadas, "la Dirección intervendrá siempre a requerimiento de los jueces fiscales de todo el país" (reabriendo

52 Privacy International… op. cit. nota 45 *supra*, p. 35.

la discusión sobre la exigencia de la orden judicial para el MPF) (considerando 5). Pasa lo mismo con la vaguedad sobre las TIC para combatir la criminalidad, al reconocerse que se utilizarán "nuevas herramientas tecnológicas fin de alcanzar procesos judiciales ágiles resultados eficaces en los casos" (considerando 4, inciso d), y que se brindarán "nuevas herramientas en materia de intervención captación de las comunicaciones que permitan acceder tecnologías que faciliten el acceso nuevos modos de comunicación en estrategias delictivas" (considerando 4, inciso f).

La legislación en materia de telecomunicaciones

En el caso de la regulación sobre telecomunicaciones, la ley 27.078 (aprobada en diciembre de 2014) reconoce que las comunicaciones privadas son inviolables (artículo 5º), incluidas aquellas que se realicen a través de las redes y servicios de telecomunicaciones, estableciendo el requisito de contar con autorización judicial para intervenirlas. No obstante, aunque incorpora esta protección, establece de forma vaga y ambigua que los usuarios de telecomunicaciones deben permitir el acceso de los prestadores de servicios de telecomunicaciones y del Ente Nacional de Comunicaciones (ENACOM) para "los efectos de realizar todo tipo de trabajo o verificación necesaria", lo que ha sido criticado desde la academia y las organizaciones de la sociedad civil [53]. El problema principal aquí es que el marco legal existente no parece cumplirse y que las intercepciones no se hacen solamente por autorización judicial.

53 Ferrari, Verónica y Schnidrig, Daniela, *Vigilancia Estatal,* op. cit. en nota 6 *supra*, pp. 8-9; ADC: "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/.

Por otro lado, la ley de Inteligencia Nacional 25.520 es complementada por la 27.126, que reforma distintos de sus artículos y modifica algunos de los organismos que la primera establecía. Sin embargo, la estructura de los servicios de inteligencia en la actualidad tampoco corresponde al texto de la ley 27.126, ya que por decreto presidencial éstos pasaron a la órbita del Poder Judicial (decreto 256/2015). Para ver todas las normas que modifican y/o completan a la Ley de Inteligencia Nacional 25.520 ir a: http://servicios.infoleg.gob.ar/infolegInternet/verVinculos.do;jsessionid=AF5E3F08B1E49F4706097C5367492432?modo=2&id=70496.

III. La estructura actual de los sistemas de inteligencia y la vigilancia estatal

Para explicar la forma en que la vigilancia estatal *funciona* en Argentina se tiene que empezar desde el final, para luego diagramar la forma en que los organismos de inteligencia se fueron transformando hasta la actualidad. Lo primero a mencionar es que su organización es compleja y que tiene traslapado su marco normativo entre la legislación en la materia y los decretos presidenciales que se han emitido para modificarla. Esto abre un primer problema frente a los estándares internacionales, como mencioné anteriormente, pues establecen que la vigilancia estatal debe materializarse en leyes formales y materiales que sean claras y precisas.

Es importante tener dos cosas en cuenta al revisar la estructura del sistema de inteligencia argentino. Primero, que tras décadas de un servicio de inteligencia vinculado directamente al poder presidencial, en el año 2015 se realizó un cambio estructural para dividir esa unión a través de una reforma legislativa. Segundo, que poco tiempo después (finales de 2015) se realizó otra modificación importante aparentemente en la misma dirección de separar estos servicios del Poder Ejecutivo, pero ésta fue por medio de un decreto presidencial, generando críticas sobre su legitimidad [54].

En febrero de 2015, la reforma al sistema de inteligencia prometida por el gobierno saliente de la presidenta Kirchner (a raíz de la muerte del Fiscal Nisman) se materializó en la ley 27.126, que vino a modificar la Ley de Inteligencia Nacional 25.520 (aún en vigor, modificada por esta reforma). Con ella se cambió la estructura del sistema de inteligencia y, poco tiempo después, por la vía de decretos se estableció una "nueva doctrina de inteligencia" (primero con el 1311/2015 y luego con el 2415/2015) [55]. Este cambio creó la actual

54 ADC: *El cambio que no llega. Un análisis sobre los recientes acontecimientos en el sistema de inteligencia en Argentina*, abril de 2017, p.10.

55 La nueva doctrina buscaba profesionalizar y regularizar al personal de inteligencia para volver los servicios más efectivos. Sin embargo, incorporaba las figuras de "atentados contra el orden constitucional y la vida democrática" y las "acciones que atenten contra la ciberseguridad" dentro del marco de su campo de acción. Ninguna de éstas estaban previamente reconocidas ni en la ley ni en la Constitución. El decreto fue problemático no sólo por la intervención innecesaria del Poder Ejecutivo y el momento político e institucional (en ple-

AFI y reemplazó a la Secretaría de Inteligencia (denominada así desde el año 2005, y anteriormente denominada Secretaría de Inteligencia de Estado, desde la última dictadura hasta 2005). Además del cambio de nombre, se trasladó el órgano facultado para intervenir las comunicaciones privadas de las personas.

Previo a la reforma de la ley 27.126, quien se encargaba de esta labor era la Dirección de Observaciones judiciales (conocida como la "*Ojota*"), y con el cambio legislativo este órgano se sacó de la esfera de los servicios de inteligencia para trasladarse al Ministerio Público Fiscal de la Nación [56], estableciéndose como el Departamento de Intercepción y Captación de las Comunicaciones (DICOM) [57]. Esta nueva estructura mantendría los controles formales

---

no tránsito y modificación de los sistemas de inteligencia de manera posterior a la muerte del fiscal Nisman), sino porque su contenido era al menos vago y eso ponía en riesgo los derechos relacionados con las acciones de vigilancia estatal. Al respecto ver: ADC. *Educar para vigilar,* Argentina, diciembre de 2015, pp. 5-6, 9-11; AFI, Presidencia de la Nación, julio de 2015. Disponible en (PDF): http://www.casarosada.gob.ar/pdf/AFI.pdf; ADC: "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.

Estos cambios duraron poco tiempo, ya que en mayo de 2016 un nuevo decreto emitido por el presidente (decreto 656/16) echó atrás la mayoría de los cambios positivos al establecer un nuevo estatuto para el personal de la AFI. Con esto, la información relacionada con la estructura orgánica y el régimen de administración de fondos volvió a ser reservada (inaccesible a las personas), se eliminó la restricción de que las acciones de inteligencia se hicieran solamente en relación al combate al delito complejo (criminalidad) o la defensa de la nación (al eliminar la metodología de "inteligencia por problema"), se derogó el régimen de administración de fondos que permitía la distinción entre fondos públicos y reservados (regresando la secrecía presupuestaria total), y se suprimió el mecanismo de coordinación entre la AFI y el MPFN y las provincias, abriendo a mayor discrecionalidad el ámbito de acción de estos servicios.

56 El DICOM dependía de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP). Sacar el DICOM de la órbita de la AFI tenía como objetivo darle una mayor independencia de los servicios de inteligencia.

57 Ley 27.126, artículo 17: "Transfiérase al ámbito de la Procuración General de la Nación del Ministerio Público, órgano independiente con autonomía funcional y autarquía financiera previsto en la Sección Cuarta de la Constitución Nacional, la Dirección de Observaciones Judiciales y sus delegaciones, que será el único órgano del Estado encargado de ejecutar las interceptaciones o

que ya existían [58], centralizando en un organismo las facultades de intervención de las comunicaciones y la obligación de que éstas fueran autorizadas previamente por un juez federal [59].

Fue entonces que, a finales del año 2015 (el 24 de diciembre), la nueva estructura fue finalmente modificada por el decreto presidencial 256/2015, que transfirió el DICOM de la Procuración General de la Nación a la Corte Suprema de Justicia de la Nación, quien lo sustituyó por la Dirección de Captación de Comunicacio-

---

captaciones de cualquier tipo autorizadas u ordenadas por la autoridad judicial competente".

58 Esto hacía que no importara qué organismo realizaba una investigación (la Policía Federal o la Policía Metropolitana, por ejemplo) ni cuál jurisdicción estaba involucrada, dado que en todos los casos -sin excepción- los organismos tenían que pedir al DICOM que realice la intervención de comunicaciones (todos los demás carecen de facultades para hacerlo). La Policía Federal Argentina y la Policía Metropolitana (para la Ciudad Autónoma de Buenos Aires), estaban obligadas formalmente entonces a pasar por un control judicial y por la acción centralizada del DICOM. Sucede lo mismo en el caso de la Gendarmería, la Prefectura, la Policía de Seguridad Aeroportuaria y las policías provinciales. ADC, *Educar para vigilar,* Argentina, diciembre de 2015, pp. 15-17, 22-23. En estos casos, recibida la autorización judicial el DICOM se comunicaba con la empresa de telecomunicaciones para grabar las comunicaciones en discos compactos que enviaban después al juzgado. Sólo tratándose de secuestros extorsivos o privación ilegal de la libertad, el DICOM podía hacer directamente las escuchas telefónicas o revisar las comunicaciones digitales, siempre que así hubiera sido indicado por el juez o la jueza competentes (pp. 22-23).

59 No obstante estos controles formales, la sociedad civil criticó que no eran respetados muchas veces y que el control a los servicios de inteligencia no era suficiente. Al respecto ver: ADC, *Educar para vigilar,* cit., pp. 5-6, 21-22. Aunque esto se relaciona principalmente con las intercepciones telefónicas, de las propias palabras del Fiscal General a cargo de la Unidad Fiscal en Ciberdelincuencia (UFECI) del MPF, Horacio Azzolín, aunque las regulaciones en cuanto a intervenciones telefónicas son claras, existirían dudas de si otro tipo de intervenciones como la vigilancia estatal particular (el espionaje) por medio de *malware* especializado debía centralizarse o no en el DICOM. Esto muestra un problema para el derecho a la privacidad. En palabras del fiscal, la legislación en ese momento no era suficiente para clarificar, por ejemplo, si la retención de los datos de tráfico requerían orden judicial o si ésta era necesaria en caso de ser revelados (en p. 20). En el caso de las provincias, su aproximación a la intervención de comunicaciones parecería lejana o nula, salvo en el caso del Ministerio Público de Córdoba, que cuenta con un área de cibercrimen, aunque no se tenga información formal al respecto (pp. 21-22).

nes (DCC). La modificación estructural fue criticada por provenir de un decreto del Poder Ejecutivo y por considerar que el texto de la acordada judicial que estableció el órgano (2/2016) era ambiguo y permitía interpretaciones que libran al Ministerio Público Fiscal de solicitar una orden judicial para la intervención de las comunicaciones privadas (aunque el decreto por el que se trasladó esta facultad al Poder Judicial sí reconocía la necesidad de que dicha intercepción se hiciera con el control judicial correspondiente) [60]. Además, se señaló lo inoportuno de la modificación frente a los avances que se estaban llevando a cabo y se cuestionó la constitucionalidad de la medida [61].

Meses después (en septiembre de 2016), la propia Corte modificó la estructura de inteligencia al crear la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado del Poder Judicial de la Nación, encargada de combatir causas complejas y del crimen organizado (trata de personas, terrorismo, tráfico de drogas, lavado de activos, etc.). En esta dirección se creó internamente la Oficina de Captación de Comunicaciones (OCC), para reemplazar a la DCC, contando con las mismas competencias y agregando otras en su "rol de órgano auxiliar en la investigación de delitos complejos y de crimen organizado". Este organismo puede, además, "desarrollar nuevas herramientas tecnológicas, brindar nuevas herramientas en materia de intervención y captación de las comunicaciones que permitan acceder a tecnologías que faciliten el acceso a nuevos modos de comunicación en estrategias delictivas" [62].

60 ADC: Ciberseguridad…op. cit., pp. 49-52; ADCI: *Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones*, 19 de febrero de 2016.

61 ADC: *El cambio que no llega*…op. cit., pp. 6-8; Comunicado de la Iniciativa para el Control Ciudadano del Sistema de Inteligencia (ICCSI) "¿Nuevo traspaso de las escuchas telefónicas? Ni urgente, ni razonable, ni legal", 24/12/15 disponible en http://www.iccsi.com.ar/nuevo-traspaso-de-las-escuchas-telefonicas-ni-urgente-ni-razonable-ni-legal/. Efectivamente, se criticó que no existiera una situación de urgencia que justificara dictar un Decreto de Necesidad y Urgencia de acuerdo al artículo 99 constitucional, así como que los avances en transparencia y trabajo con organizaciones de la sociedad civil que se venían realizando con la DICOM iban a ser simplemente desplazados.

62 Al respecto ver la Acordada 30/2016 de la Corte Suprema, disponible en: http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=100091.

El tránsito a esta nueva oficina -entre críticas de la sociedad civil por el alejamiento del objetivo de contar con un órgano autónomo encargado de la inteligencia estatal- no fue sencillo. En los primeros meses, existió una apertura a actuar con transparencia rindiendo informes estadísticos que realizaría mensualmente, y estableciendo un reglamento interno que mostraría la forma en que sus procesos serían llevados a cabo [63]; pero por otro lado, persistió la repetición de escándalos por el manejo político de las escuchas telefónicas (tal como ha pasado muchas veces en la historia de la inteligencia argentina), donde se filtraron a medios de comunicación conversaciones entre la expresidenta Cristina Fernández y el ex secretario de inteligencia Oscar Parrilli (parte de una investigación judicial sobre este último realizada por el juez Ariel Lijo) [64].

La nueva estructura ha sido cuestionada por la sociedad civil en la actualidad porque se cuenta con información de que existen otras unidades de inteligencia, tanto en las fuerzas armadas como en las de seguridad (a nivel provincial y federal), con la particularidad de

63 ADC: *El cambio que no llega…*op. cit*.,* pp. 8-9. Supuestamente, dichos informes revelarían el tipo de solicitud de intervención, los oficios y procesos iniciados por ella, la autoridad que requirió la intervención y los delitos por los que se investiga a la persona, entre otros. También se informó que se emitiría un protocolo sobre la cadena de custodia y un sistema de auditoría interno. Esta información fue otorgada en respuesta a una solicitud de información realizada por la ICCSI.

64 ADC: *El cambio que no llega…*op. cit*.,* pp. 9-10. Aunque esto provocó que se iniciaran investigaciones y causas penales para dar con las personas responsables, y se señaló (esto por el mismo Parrilli) al presidente Macri como el supuesto responsable del espionaje político, no ha tenido mayores consecuencias y refleja las prácticas anteriores de impunidad alrededor del uso político de los servicios de inteligencia.

Este escándalo generó comunicaciones (a pedido de la Corte Suprema) entre la OCC y el Máximo Tribunal, y también la creación de una comisión especial en el Congreso para investigar sobre dichas filtraciones, así como distintos pronunciamientos/acusaciones de las personas involucradas en las filtraciones hacia el presidente Macri y la legisladora Margarita Stolbizer personas de su gobierno. Al respecto ver: http://www.infobae.com/politica/2017/04/02/la-furia-de-cristina-kirchner-contra-margarita-stolbizer-insultos-denuncias-y-carpetazos/ y http://www.infobae.com/politica/2017/03/26/nuevas-escuchas-de-cristina-kirchner-macri-es-un-mafioso-sostenido-por-los-medios/.

que sus regulaciones se amparan en la secrecía que protege al sistema de inteligencia argentino [65].

Además de los órganos principales de inteligencia y de control judicial, desde la ley 25.520 ha existido la Comisión Bicameral de la Ley de Seguridad Interior (establecida en su artículo 32). Si bien desde 1991 la ley de Seguridad interior establecía una Comisión revisora (que estuvo parcialmente activa para investigar casos de espionaje dirigidos a sectores gremiales y estudiantiles en 1993), no fue hasta los primeros años del siglo XXI que se estableció claramente que sería la Comisión Bicameral quien controlaría y escrutaría las intercepciones de comunicaciones privadas realizadas por la entonces Secretaría de Inteligencia (y que debían contar con autorización judicial). Sin embargo, la información relacionada con el trabajo de esta Comisión es secreta e inaccesible, ya que desde su establecimiento en 2004 los informes anuales que debe elevar al Congreso y al Poder Ejecutivo (artículo 33.2) se clasifican como secretos y normalmente no se distribuyen a los diputados [66]-[67].

El estado institucional actual muestra que dos problemas sobre la vigilancia estatal no han sido resueltos: por un lado, la conciliación del principio de transparencia y de rendición de cuentas frente al principio de secrecía de las operaciones de inteligencia (bajo el argumento de su efectividad y eficiencia) y, por otro lado, la falta de voluntad de la clase política para hacerse cargo de las implicancias relacionadas a la vigilancia estatal (parte por desconocimiento sobre lo que estas actividades implican, parte por no querer hacerse cargo de ellas o por el miedo aparente de enfrentarlas) [68].

65 ADC. *Educar para vigilar,* Argentina, diciembre de 2015, pp. 6-7.

66 ADC. *Quién vigila a quienes vigilan*…op. cit.*,* pp. 13-14.

67 Primero, la Comisión no tuvo presupuesto para ser funcional hasta 2004, después sus actividades son completamente secretas y el informe anual se clasifica expresamente como secreto, además, dado el decreto No. 950/2002 que lo reglamenta (en sus artículos 11 y 20), se deja a voluntad del Secretario de Inteligencia otorgar la información que la Comisión solicita. ADC, *El (des) control democrático*… pp. 29-30.

68 ADC, *El (des)control democrático*…op. cit., p. 6.

IV. El contexto histórico argentino de la vigilancia estatal: ¿cómo podemos estar así?

Para completar el análisis sobre la vigilancia estatal, es necesario hacer un recorrido histórico por las últimas décadas del ejercicio de la inteligencia estatal. Esto permite hacer una evaluación concreta que supere un análisis normativo superficial que pudiera ser engañoso. Observar a profundidad la práctica de la vigilancia estatal permite mostrar los problemas y tensiones de ésta con los derechos y la democracia. Este trabajo de crítica debe hacerse también a la luz del contexto regional, puesto que es con esta doble mirada (externa/interna) que las dimensiones del espionaje estatal pueden verse más claramente.

En los últimos años se ha demostrado que Latinoamérica ha adoptado como práctica común la compra de *software* específico para realizar espionaje estatal, y que lo ha utilizado en muchas ocasiones para vigilar opositores y periodistas, así como otras personas que resulten de interés político para el Estado [69]. Esto es una práctica reciente sólo en cuanto al tipo de tecnologías y al tipo de acciones de invasión a la privacidad de las personas. Sin embargo, la historia de espionaje y violaciones a la privacidad en Argentina es larga; en este sentido, la vigilancia personalizada puede leerse como una continuación de las prácticas más antiguas de espionaje estatal.

Tras abandonar la última dictadura cívico-militar se inició un proceso de "desmilitarizar la seguridad interior" a través de cambios institucionales que intentaron alejar las tareas de inteligencia de la lógica intervencionista generalizada de la doctrina de seguridad nacional de corte militar que existía. El primer resultado de esto fue quitar al Ejército las tareas de combate al terrorismo y al narcotráfico [70]. No es exagerado decir que los avances institucionales y culturales de Argentina frente a los gobiernos dictatoriales son referentes en la región (donde los juicios a las juntas militares y los

69 Pérez de Acha, Gisela. *Hacking Team Malware Para la Vigilancia en América Latina*, Derechos Digitales, Marzo de 2016. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf; Brito, Carlos y Narváez Herrasti, Santiago. *Medir y acotar la vigilancia estatal*… pp. 300-301.

70 Saín, Marcelo Fabián, *Las 'nuevas amenazas' y las Fuerzas Armadas en la Argentina*… op. cit. *supra* en nota 18.

procesos de concientización en torno a los derechos humanos son sólo dos ejemplos que son constantemente tomados como referencia en Latinoamérica), lo que muestra una paradoja clara en el tema de los servicios de inteligencia y vigilancia estatal.

Parece así que el aparato estatal relacionado con los servicios de inteligencia no sólo fue excluido del proceso de transformación, sino que fue utilizado intencionalmente por los grupos que ocuparon el poder civil (en particular el Poder Ejecutivo) a partir de este entonces [71]. En palabras de la ADC: "Es un sistema que desde 1983 a esta parte se presenta como altamente autónomo pero parte esencial del presidencialismo argentino: sirve a placer del presidente de turno pero, a la vez, es capaz de manejar una agenda propia que constituye una verdadera amenaza para la democracia argentina y los derechos de los ciudadanos" [72].

Hasta hace poco tiempo (como mostré arriba), la realidad es que quienes debían ser controlados controlaban los mecanismos de control de los sistemas de inteligencia. Esto llevó a que pudieran realizar acciones de vigilancia ilegal sin mayores consecuencias y (muchas veces) a que se simulara un cumplimiento de las leyes. Pero además, esto fue posible porque los órganos de control fueron cooptados por los partidos que estaban en el poder (es posible observar que desde 1983, tanto desde el radicalismo como desde el justicialismo, la entonces Secretaría de Inteligencia ha respondió a

71 ADC. *El (des)control democrático*… op. cit. Como ejemplo del último punto hay casos que pueden rastrearse desde el gobierno de Alfonsín, pasando por el gobierno de Menem y los casos de espionaje a periodistas críticos al gobierno mediante escuchas telefónicas, el escándalo del manejo de la información de la Secretaría de Inteligencia en relación a la causa AMIA (relacionado con la red de cooptación y corrupción entre la Secretaría de Inteligencia, los fiscales y los jueces en el país, bajo un sistema de pagos con fondos reservados, también conocida como la "cadena de la felicidad"), el *caso de las coimas del Senado* (con dinero supuestamente proveniente de la Secretaría de Investigación) y su labor de dispersión de la protesta social en la época de crisis de inicios de siglo (pp. 6-12).

72 ADC. *El (des)control democrático*… op. cit., p. 2. En esta etapa, organizaciones de la sociedad civil presentaron distintas críticas, foros de discusión sobre su modificación y demandas concretas sobre la misma (por ejemplo con la *Iniciativa Ciudadana para el Control del Sistema de Inteligencia* presentado por la ADC y el Instituto Latinoamericano de Seguridad y Democracia *ILSED* en 2013), sin mucho éxito (p. 3).

los intereses presidenciales y que, en cuanto a la Comisión Bicameral, estuvo controlada casi siempre por legisladores que actuaron de forma funcional a la presidencia y mantuvieron la práctica de vigilancia muy lejos del marco legal) [73].

En este siglo sobran ejemplos de lo peligroso que resulta el descontrol de los servicios de inteligencia y de la vigilancia estatal. No es poco decir que tanto el actual presidente Mauricio Macri como la ex presidenta Cristina Fernández de Kirchner hayan sido acusados de participar en acciones ilegales relacionadas con intervención de comunicaciones privadas y el uso de los servicios de inteligencia para fines políticos y sociales por fuera de la ley. Tampoco lo es que, sin importar las filtraciones de información relacionada con la posible adquisición de equipo avanzado de espionaje y de los intereses estatales con empresas que prestan servicios de espionaje como *Hacking Team*, no hayan existido cambios sustanciales en la opacidad con que funciona el sistema de inteligencia, ni mucho menos un proceso de rendición de cuentas real para saber con certeza las prácticas del gobierno en este tema.

Tan sólo en la campaña de las últimas elecciones presidenciales, uno de los temas a discutir fue el hallazgo de que en 2007 se encontró equipo para intervenir líneas telefónicas de legisladores, ministros, y funcionarios de partidos de la oposición (y también oficialistas). Supuestamente, el equipo no pertenecía a la entonces Secretaría de Inteligencia. La entonces legisladora Patricia Bullrich (hoy Ministra de Seguridad de la Nación), quien había sido parte de la Comisión Bicameral revisora entre 2009 y 2011, corroboró que cuando visitaron el edificio de la DOJ sólo les mostraron tecnología antigua y que habrían escondido los equipos modernos [74]. Ninguna

73 Esto es lo que se muestra del manejo de la Comisión en las últimas décadas tomando en cuenta la integración del Congreso y la conformación de este órgano. Como dato adicional en cuanto a la secrecía, es interesante ver que en 12 años, la Comisión solamente emitió 31 dictámenes (sólo lo hizo en cuatro años: 2004 con 19, 2005 con 4, 2006 con 3, 2008 con 2, 2009 con 3). Como dato adicional a la cooptación y control interno del sector de inteligencia, están los testimonios sobre el ingreso a la Secretaría de Inteligencia, donde priman las conexiones familiares en lugar de los exámenes u otros mecanismos transparentes de selección. Al respecto ver: ADC. *El (des)control democrático*…op. cit., pp. 30-34.

74 Ibid., pp. 21-22.

de las denuncias al respecto tuvieron resultados y las investigaciones se estancaron.

Este escándalo se relacionaría con el del informe del parlamento alemán, donde se documentó que el gobierno de Cristina Kirchner compró equipos de espionaje electrónico y tecnologías de vigilancia que fueron posteriormente declaradas secretas, impidiendo a la sociedad argentina saber de qué tipo y para qué efectos eran. Los equipos se adquirieron en 2010 y 2011, y la información fue confirmada por el entonces jefe de gabinete argentino en noviembre de 2014 [75]. El monto de las tecnologías habría sido de €1.183 millones de euros y €169.357 euros cada año. Como con el resto de los asuntos sobre los equipos de inteligencia, el caso se mantuvo en total secrecía y el gobierno nacional no explicó casi nada al respecto [76].

Pero incluso antes que esto, el actual presidente Macri (entonces jefe de gobierno de la CABA) ya había sido procesado judicialmente por su supuesta participación en una asociación ilícita de espionaje estatal. En ella, habría sido parte de una "estructura de inteligencia subterránea" de escuchas telefónicas en las que se habría espiado a personas dentro de los que destacan familiares del atentado a la Asociación Mutual Israelita Argentina (AMIA) (opositores al gobierno de la ciudad) [77]. Tal como a nivel nacional, la situación en la CABA dista de lo que formalmente se reconoce en la ley, manteniendo el problema del descontrol democrático de la vigilancia estatal.

Poco tiempo después del procesamiento de Macri, el escándalo del **Proyecto X** salió a la luz. En 2012 se descubrió que la Gendarmería Nacional habría realizado actividades de inteligencia ilegales

75 Ibid., pp. 25-26.

76 ADC. *Educar para vigilar,* Argentina, diciembre de 2015, pp. 24-25. Al respecto ver: https://advox.globalvoices.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/, http://www.spiegel.de/politik/deutschland/deutsche-spaehtechnik-gabriels-ausfuhrkontrollen-bleiben-wirkungslos-a-987555.html, y https://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs182067_1.pdf.

77 Privacy International…op. cit., nota 45, p. 39; en el mismo sentido ver también: http://www.bbc.com/mundo/america_latina/2010/05/100514_2318_macri_proceso_buenos_aires_jg.shtml y https://www.pagina12.com.ar/diario/elpais/1-145731-2010-05-15.html.

(recolección y sistematización de información) desde 2005. Ninguna medida estaba autorizada por un juez ni era parte de una causa judicial o se rindió cuenta de ellas a la Comisión Bicameral, y tenían como objetivos a organizaciones sociales, familiares de víctimas de la represión, movimientos sociales y organismos de derechos humanos, entre otros. El espionaje se realizaba con un *software* prohibido por la ley de Inteligencia Nacional, cuyo uso fue reconocido por la entonces Ministra de Seguridad Nilda Garré, quien señaló que era solicitado por jueces de todo el país (no sólo jueces federales) y fiscales (sosteniendo que no era ilegal) [78].

La supuesta legalidad de este programa fue defendida también por la Secretaria de Cooperación con los Poderes Judiciales, Ministerios Públicos y Legislaturas, del Ministerio de Seguridad, Cristina Camaño, quien reconoció su existencia y dijo que las acciones de Gendarmería constituían acciones de "investigación criminal" y contaban con órdenes judiciales. Reconoció que "El *software* de carga y entrecruzamiento de datos 'PROYECTO X' fue utilizado en 285 causas penales relativas a contrabando y tráfico de drogas a requerimiento del juez de la causa **o del ministerio público Fiscal**" (*énfasis mío*). Todo esto habría sido determinado como legal por una supuesta auditoría interna realizada por el Ministerio de Seguridad [79]. La causa sobre este caso no ha resultado, al menos hasta la redacción de este trabajo, en ninguna indagatoria [80].

Otro caso que no puede obviarse es el de la muerte del Fiscal Alberto Nisman. El 18 de enero de 2015 fue encontrado con un disparo en la cabeza quien había estado a cargo de la causa del atentado a la AMIA. Esto sucedió un día antes de comparecer en el Congreso para explicar los fundamentos de su denuncia contra la entonces

78 Dicho reconocimiento se hizo públicamente en una rueda de prensa que puede verse en: https://www.youtube.com/watch?v=DoSZ4b8BGBA. Al respecto ver también: Privacy International… p. 39; http://chequeado.com/ultimas-noticias/cfk-quisieron-montar-que-habia-una-suerte-de-espionaje-de-la-gendarmeria-proyecto-x-inexistente/;.

79 Dicha respuesta se dio el 26 de marzo de 2012 a través de una nota firmada por la Secretaria Camaño, que puede consultarse aquí: http://morales.radicales.org.ar/wp-content/uploads/2012/02/RESP-MIN-SEGURIDAD-PROYECTO-X.pdf.

80 Privacy International… p. 40.

presidenta Cristina Fernández de Kirchner. Además de esta acusación, Nisman había solicitado el procesamiento del actual presidente Mauricio Macri precisamente por los hechos relacionados con espionaje estatal que describí más arriba [81].

Tras su muerte, se encontró que Nisman había sido atacado con un *malware* (un *softweare* malicioso) para infectar su computadora con Windows (sin que se sepa si abrió el archivo desde ésta). El fiscal descargó el archivo a su celular (*Android*) y por ello no habría sido infectado. De acuerdo a una investigación experta, este intento de infección no habría sido un hecho aislado y habría otros casos de espionaje en el país y en la región [82]. El tipo de intento de infección (utilizar un documento que supone ser un archivo *.pdf* u otro similar para tomar control de los equipos y la información de la persona que se intenta espiar) se ha repetido en contextos de países en crisis graves de derechos humanos, donde además existe mayor información sobre la adquisición de equipos de espionaje personalizado por parte de los gobiernos (de forma ilegal), tal como sucede en el caso de México. En dichos casos, existe una fuerte presunción del uso ilegal de equipos de inteligencia por parte de gobiernos para utilizarlos en contra de opositores políticos o personas críticas al gobierno, y hay señalamientos y circunstancias similares a las del caso argentino.

A todo esto debe sumarse que, en la actualidad (recién a inicios de 2017), los escándalos de escuchas telefónicas con manejo político se siguen revelando (como el caso de las conversaciones entre la ex presidenta Cristina Fernández y el ex jefe de inteligencia Oscar Parrilli) como parte de una práctica política (ilegal) de antaño normalizada en el presente. Los avances en la transparencia de los servicios de inteligencia se han derrumbado con decretos presiden-

81 Esto sumado a las posteriores revelaciones que mostraban que el celular de Nisman estaba infectado con virus que afectaría su privacidad. Al respecto ver: ADC: La ADC Alerta: software de intercepción y vulneración a los derechos humanos, Agosto de 2015, en: https://adcdigital.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf.

82 Privacy International…op. cit., p. 41. La investigación fue realizada por el experto en seguridad Morgan Marquis-Boire, y titulada: *Insidethe Spyware Campaign Against Argentine Troublemakers*, publicada en The Intercept el 21 de abril del 2015, puede consultarse en: https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/.

ciales que han reinstaurado la secrecía y la ausencia de rendición de cuentas. Muestra de esto es el nombramiento de las cabezas de la Agencia Federal de Inteligencia, que son abiertamente opuestas a las exigencias de profesionalización y experiencia, y son una clara muestra del uso de los servicios de inteligencia a partir de la lógica de cercanía y lealtad al presidente [83].

Recientemente, la propia AFI estuvo en el centro de otro escándalo de supuesto espionaje ilegal, publicado por el diario *Clarín* en donde una supuesta oficina alterna a la oficina de la Subdirectora de este organismo habría realizado escuchas ilegales. En los hechos, que enfrentaron a la dirigente Elisa Carrió del partido político Coalición Cívica para la Afirmación de una República Igualitaria -central para la coalición del gobierno del presidente Macri-, la diputada habría sido monitoreada en un viaje a Paraguay y se habrían hecho escuchas de distintas llamadas telefónicas. La respuesta de la AFI fue que nada de esto era cierto, ya que las escuchas y ese tipo de espionaje estaba ahora en manos de la Corte Suprema, por lo que se deslindaron de responsabilidades y abrieron una investigación interna para cooperar con el órgano judicial [84]. Días después, la diputada señaló que tras una comunicación privada con el Director

83 ADC: *El cambio que no llega*…op. cit., pp. 13-15. Es asombroso, por una parte, que el presidente haya nombrado como Director de la AFI a Gustavo Arribas, quien fuera amigo de él y proviniera del mundo de la compra-venta de jugadores de fútbol y su representación y, como Subdirectora, a Silvia Majdalani, quien fungiera dentro de la Comisión Bicameral de Fiscalización de Organismos y Actividades de Inteligencia, en una etapa en que ésta fue más ineficiente y opaca. Ambas personas están involucradas en causas judiciales (el primero por evasión tributaria relacionada también con el caso de Odebrecht, y la segunda por temas de enriquecimiento ilícito y lavado de activos). Es igual de asombroso que el Senado aprobara dichos nombramientos ignorando la crítica de distintos sectores por su falta de idoneidad y acusaciones de acciones ilegales. Para más al respecto ver: http://www.iccsi.com.ar/observaciones-a-los-pliegos/, http://www.lanacion.com.ar/1974791-un-operador-de-odebrecht-le-giro-us-600000-al-jefe-de-inteligencia-argentino y http://www.iccsi.com.ar/gustavo-arribas-la-iccsi-demanda-la-urgente-investigacion-de-los-hechos-que-lo-ubican-en-una-trama-de-corrupcion/.

84 Al respecto ver: "El escándalo del espionaje ilegal: a Carrió también le escuchan sus llamados", *Diario Clarín,* 26 de mayo de 2017. Disponible en: https://www.clarin.com/politica/escandalo-espionaje-ilegal-carrio-escuchan-llamados_0_H10-kxrZZ.html;

de la AFI, reconocía que no había sido espiada y que le había sido presentado un "informe satisfactorio" de esto, que se mantendría estrictamente reservado (en secreto) [85].

En distintos momentos, la ADC y el ILSD han pedido el acceso a la información de las actividades de inteligencia que la AFI debe rendir (información estadística que puede ser publicada) pero se ha mantenido secreta, reflejando el "paradigma de secreto excesivo" existente, faltando al principio de transparencia y de rendición de cuentas [86].

Finalmente, es indispensable señalar la situación actual de las empresas que ofrecen servicios y tecnologías avanzadas para la infección de dispositivos electrónicos y la intercepción de las comunicaciones de las personas, y que tienen relaciones con distintos países en la región. Si bien no existe información demostrada de que Argentina haya materializado transacciones con ellos, sí existen numerosos indicios de que el gobierno argentino tuvo comunicación con estas empresas en distintas ocasiones durante años, lo que debería ser razón suficiente para que rindiera cuentas al respecto.

A partir de la revelación de la relación de la empresa italiana *Hacking Team* con distintos países en Latinoamérica (incluidos Argentina) [87], es sabido que los Estados llevan a cabo prácticas de

85 Al respecto ver: "Elisa Carrió dio marcha atrás y aclaró que la AFI no la espió en Paraguay", Diario La Nación, 30 de mayo de 2017. Disponible en: http://www.lanacion.com.ar/2028734-elisa-carrio-dio-marcha-atras-y-aclaro-que-la-afi-no-la-espio-en-paraguay.

86 ADC. *Quién vigila*…op. cit., pp. 15, 21. Esto se realizó a partir de la *Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI)*. La información solicitada fue: la cantidad de reuniones en los últimos tres años de la Comisión, los informes producidos de los últimos tres secretarios, el número de pedidos de informes realizados por la Comisión a la Secretaría de Inteligencia, etc. Ante la falta de respuesta se presentó un amparo que no ha sido resuelto. Ver: ADC. *El (des)control democrático*…op. cit., p. 30.

87 Por medio de la filtración de los más de 400 GB de información de la empresa *Hacking Team*, *hackeada* para revelar esta información (que fue publicada el 5 de julio de 2015). Con estas filtraciones se mostraron emails, audios, código de fuente de distintos *software*, listas de clientes, información fiscal, contratos y documentos financieros. Al respecto ver: ADC: La ADC Alerta: software de intercepción… pp. 2-3.

vigilancia personalizada apoyados en las facilidades de obtener los equipos de espionaje. En Argentina se reveló que durante 2014 y 2015 distintos intermediarios de empresas de seguridad y vigilancia en Argentina (como *Nullcode Team*, *TAMCE* y *Global Interactive Group S.R.L.*) sostuvieron reuniones con representantes de esta empresa para intentar contratar sus servicios y adquirir equipos de inteligencia para entregarlos a organismos gubernamentales como la AFI. En este contexto, destacan dos situaciones preocupantes: i) que en las comunicaciones entre las empresas intermediarias y *Hacking Team* se aseguraba la participación de agencias gubernamentales y su interés en adquirir *software* de espionaje, y ii) que se mencionó también que el mercado de agencias interesadas en contratar este *software* incluía al Ejército, la Gendarmería, la Prefectura, la Policía Federal, la AFI y policías provinciales, quienes carecerían de facultades legales para llevar a cabo acciones de inteligencia [88].

En las comunicaciones se mencionó que algunas agencias estatales estaban decidiendo entre la empresa italiana y la empresa israelí *NSO Group*, y que existen otras empresas en el mismo rubro con presencia en Argentina, tal como *Blue Coat* [89].

Como parte de este contexto, el 20 de octubre de 2015 se presentó una denuncia en contra de la AFI por el supuesto espionaje de más de cien personas que habrían sido víctimas de vigilancia estatal, incluidos los tres ministros y la ministra de la Corte Suprema argentina, jueces, fiscales, miembros de la oposición kirchnerista, políticos de distintos partidos (incluido el hoy presidente Mauricio Macri), numerosos periodistas y personajes polémicos relacionados con los servicios de inteligencia y el Ejército, como el ex-director de la entonces SIDE Antonio Horacio Stiuso y el ex jefe del Ejército César

88 ADC: La ADC Alerta: software de intercepción…op. cit., nota 81, pp. 4-5. En marzo de 2013 integrantes de *Hacking Team* habrían asistido a Buenos Aires para reunirse con funcionarios del Ministerio de Seguridad de la Nación, el Ministerio Público Fiscal y el Ministerio de Justicia y Seguridad de la Provincia de Buenos Aires, teniendo como resultado el interés de algunos funcionarios en el equipo de la empresa, y haciendo la especificación de que para cerrar los contratos "se debería sobornar a los diferentes jefes de cada departamento por cada producto (software) que trajera al país" (p. 4).

89 ADC: La ADC Alerta: software de intercepción…op. cit., p. 4.; ADC: Ciberseguridad… op. cit., p.10.

Milani. De acuerdo a la denuncia, el espionaje incluía mensajes de *Whatsapp*, mails, teléfonos y computadoras personales. De manera similar a los otros escándalos relacionados con el espionaje estatal, el caso no fue resuelto [90].

V. Conclusiones

En Argentina la intimidad y privacidad de las personas está en una posición desfavorable. Existe evidencia suficiente de que han sido (y siguen siendo) vulnerados en numerosas ocasiones. Su andamiaje institucional y legal ha sido insuficiente para controlar la vigilancia estatal. Esto es particularmente claro (y grave) en el caso del espionaje o la vigilancia dirigida (personalizada).

La secrecía de los servicios de inteligencia es incompatible con los principios de transparencia, el acceso a la información y los derechos a la intimidad y la privacidad. Es precisamente por la impunidad y la falta de información sobre la forma en que se ha procedido que parece claro que no existe la voluntad política para transformar el ámbito de la vigilancia y los servicios de inteligencia. El discurso de la efectividad de la vigilancia y la seguridad pareciera tener más peso que el de los derechos.

Existen casos documentados en la región (como el de México) que muestran que su grado de intrusión no compensa la efectividad que prometen: la vigilancia es poco útil para lograr los fines legítimos que persigue [91]. Como señalan otras investigaciones, la evidencia de que la vigilancia es de gran utilidad en la prevención e investigación de delitos es poca o nula, y normalmente los resultados existentes muestran que no es esencial en la prevención de ataques terroristas o criminalidad [92]. Nuestro caso es preocupante porque las pocas he-

90 Privacy International, *The Right to Privacy in Argentina*… p. 10; La Nación, "Denuncian espionaje de la Secretaría de Inteligencia a jueces, políticos y periodistas", 20 October, 2015. Disponible en: http://www.lanacion.com.ar/1838176-denuncian-espionaje-de-la-secretaria-de-inteligencia-a-jueces-politicos-y-periodistas.

91 Brito, Carlos y Narváez Herrasti…op. cit., pp. 313-315; R3D, *El Estado de la Vigilancia*… op. cit.

92 Kirchner, Lauren, *"What's the evidence that Mass Surveillance Works? Not Much"*, Propublica, November 2015. Disponible en http://

rramientas para enfrentar la secrecía (la Comisión Bicameral o el hecho del traslado al Poder Judicial) han resultado en fortalecerla. Estos cambios han llegado de la mano del Poder Ejecutivo, no de una discusión democrática, lo que aleja estas decisiones aun más del ámbito democrático al que deberían someterse (los avances se atan la voluntad del o la presidenta en turno).

Mecanismos de control como el la notificación diferida (derecho de notificación) o el mecanismo independiente de auditoría a las medidas de vigilancia se ven lejanos. Tanto porque la voluntad política de lograrlos parece poca (y la de mantener la secrecía mucha), como porque estas decisiones no están pasando por las y los legisladores. En cuanto a la Comisión Bicameral, su práctica y su regulación han mantenido una simulación de transparencia que en los hechos sólo puede tener un papel formal. Tampoco queda claro que la supervisión pública independiente se resuelva con la centralización en la Corte Suprema (y sus auditorías internas); el regreso a la secrecía de su funcionamiento y su información es la mejor prueba de ello.

El problema de la vaguedad y ambigüedad de la legislación es grave. Hay demasiados casos que generan zonas grises donde la intimidad y la privacidad están en riesgo (como el de las acciones de inteligencia por "atentados contra el orden constitucional" de la Ley de Inteligencia; los casos señalados arriba de los códigos procesales penales o el de la ley "Argentina Digital" sobre la obligación de acceso al ENACOM por las empresas de telecomunicaciones para acceder a "información que él estime pertinente"). La formalidad legal, necesidad y proporcionalidad no se cumplen. Además, en algunos casos se permite la intercepción de comunicaciones en delitos no graves, bajo el criterio de "información pertinente o útil", sin valorar el grado de invasión a los derechos. Todo esto es incompatible con los estándares en la materia, y puede resultar en flexibilizar distintos controles, en particular el del control judicial.

Los problemas de los controles democráticos y el desfase entre la práctica de las acciones de inteligencia y sus regulaciones for-

---

ow.ly/5A4K30dSL4N. El análisis de la vigilancia en EUA muestra que no fue esencial para la prevención de los ataques terroristas en el periodo que llevó del año 2001 al año 2014. Éste es el tipo de datos requerido en Latinoamérica para poder discutir seriamente en torno a la vigilancia.

males es preocupante. El espionaje estatal es probablemente la deuda más grande del tránsito a la democracia Argentina. En él no hay espacio para los derechos. Ésta es la cara obscura de nuestra democracia.