El secreto
La seguridad nacional como coartada para un Estado sin controles*

Tras los atentados de 2001 en los Estados Unidos, la vigilancia y el secreto se convirtieron en ordenadores de muchas de las respuestas estatales a las llamadas "nuevas amenazas mundiales". Las luchas o guerras contra el terrorismo, el narcotráfico, las migraciones y el crimen organizado pasaron al centro de la agenda de la seguridad nacional. Al ataque militar de otros Estados se sumaron estas "amenazas híbridas", transnacionales, que se invocan para justificar un mayor despliegue represivo porque, se dice, ponen en juego a la nación y a su orden institucional. Esta razón de Estado y la ideología del orden –que opone una supuesta tranquilidad social frente al caos de la conflictividad– habilitan el crecimiento de los aparatos de seguridad e inteligencia. Se trata de un modelo de Estado que recopila y usa cada vez más información, amplía sus funciones represivas, invade la vida privada, restringe los controles democráticos, e intenta justificar todo esto en las razones de seguridad nacional. Es un Estado que necesita el secreto para funcionar.

En la Argentina de estos últimos años, la decisión gubernamental consistió en adscribir tanto desde lo político como desde lo ideológico a este paradigma.[1] Los puntos de quiebre fueron el Decreto 683/2018, que modificó la reglamentación de la Ley de Defensa Nacional y otorgó algunas funciones de seguridad a las Fuerzas Armadas, y la Directiva de Política de Defensa Nacional, el Decreto 703/2018, que marcó de forma

* Este capítulo fue elaborado por Paula Litvachky, Margarita Trovato, Tomás Griffa, Juliana Miranda, Andrés López Cabello, Ezequiel María y Federico Efrón, integrantes del Equipo de Trabajo del CELS.

1 Para una revisión más extensa de los antecedentes y las implicancias de las medidas adoptadas por el actual gobierno argentino en el marco de la perspectiva sobre "nuevas amenazas", véase M. Tufró y J. Miranda, "El peligroso camino hacia la militarización de la seguridad ciudadana", en *Xumek Asociación Civil, Informe 2018. Situación de los derechos humanos en Mendoza*, 2018, pp. 93-101.

expresa ese alineamiento. Desde fines de 2015 y hasta el mismo período de 2019, la gestión del gobierno nacional en seguridad y defensa se centró en la "guerra contra el narcotráfico y el terrorismo", en establecer acuerdos de cooperación e intercambio de información con otros países, en la compra de armamento y *software*, y en un notable incremento del presupuesto para inteligencia.

La principal vocera de esta política fue la ministra de Seguridad Patricia Bullrich, que expresó la síntesis entre fortalecer la faz militar y policial del Estado, achicar el espacio público en el que se manifiestan los conflictos y el disenso, y promover los negocios de armas y tecnologías de control social. Su posición está en línea con los Estados Unidos e Israel en los debates globales y regionales. En noviembre de 2016, participó en Tel Aviv, junto con una delegación del Ministerio de Seguridad, en la IV Conferencia Internacional de HLS & Cyber, una de las ferias del negocio de la seguridad más grandes del mundo. Allí, países, empresas y lobistas retroalimentan el paradigma de las "amenazas del siglo XXI": hacen acuerdos, compran armas y *software* de vigilancia. Como explicó el presidente de la Cámara de Comercio argentino israelí Mario Montoto, también asesor de los ministerios de Seguridad y de Defensa:

> De todas las exposiciones, quedó claro que nadie está exento de sufrir un ataque terrorista en este mundo tan convulsionado y cambiante, que pueden provenir de los más sofisticados *softwares* criminales o de bombas incendiarias de fabricación casera.[2]

De este viaje se desprendieron acuerdos y compras importantes de material bélico y tecnología de vigilancia. Al respecto la ministra informó: "La Argentina va a poner tecnología para terminar con el problema de la triple frontera".

La gestión de Cambiemos postuló que, para enfrentar los riesgos globales, se necesitan nuevas tecnologías que aumenten la capacidad de vigilar y de acopiar información personal, junto con otras herramientas de investigación que son invasivas de la privacidad. El Estado desplegó nuevas y viejas prácticas de inteligencia legal e ilegal, de vigilancia y de criminalización de activistas, referentes y organizaciones. Algunas de estas prácticas no son nuevas, ni exclusivas de nuestro país. Otras parecen

2 M. Montoto, "Israel: al tope del desarrollo mundial", *Infobae*, 27 de noviembre de 2016.

propias de este momento: en particular, la expansión de la agenda, de los aparatos de seguridad e inteligencia y del secreto de Estado justificada en los riesgos para la seguridad nacional. El discurso oficial asumió, como si fuera un nuevo sentido común, que las herramientas de vigilancia cada vez más invasivas deben ser parte de la vida política y social. Que el Estado vigila para investigar y cuidarnos. Este supuesto realismo político requiere debilitar los controles democráticos porque las expectativas de transparencia y acceso a la información son presentadas como incompatibles con las exigencias de la seguridad nacional. De este modo, hoy casi no existen vías para obtener información sobre la legalidad del uso de estas herramientas de control y vigilancia.

1. Inteligencia secreta

Terroristas inventados

Anil Baran, de nacionalidad turca, viajó de Córdoba a la Ciudad Autónoma de Buenos Aires (CABA) para hacer el trámite que le permitiría acceder a la nacionalidad argentina. El 24 de octubre de 2018 fue detenido por personal policial, acusado de haber participado en incidentes violentos durante una protesta frente al Congreso nacional. Después de tres meses, el fiscal de primera instancia afirmó que no había ninguna evidencia que sustentara la acusación y archivó el caso. Pero antes de que esto sucediera, el gobierno nacional respaldó la versión policial sobre la detención e intentó expulsar del país a Baran. Varios medios de comunicación se sumaron a la difusión de "información" en *off* que afirmaba que otros de los detenidos eran oficiales de inteligencia de gobiernos extranjeros y Baran, un "terrorista" entrenado para causar disturbios durante la cumbre del G-20.

Baran preguntó a los ministerios de Relaciones Exteriores y Culto, de Seguridad y de Defensa, a la Dirección Nacional de Migraciones y a la Agencia Federal de Inteligencia (AFI) qué información poseía el Estado sobre él. Las carteras de Seguridad y Relaciones Exteriores le respondieron sin aportar nada relevante. La contestación de Defensa fue que solo proveería la información ante una intimación judicial, pese a que la Ley 25 326 obliga a los bancos de datos públicos a brindar a la persona que lo solicite la información que sobre ella tienen. La AFI rechazó la solicitud sin justificación. La Dirección Nacional de Migraciones se negó a recibir la petición de acceso, lo que motivó una queja ante la Dirección Nacional de Datos Personales. Por último, Baran solo pudo conocer el expediente

de Migraciones en el que consta un pedido de dictamen sobre la expulsión inmediata que pretendía el Ministerio de Seguridad, y que no consiguió. Allí no aparece información que justifique una expulsión. Así es que o bien fue producida por otro organismo o bien las autoridades intentaron expulsarlo sin sustento. El expediente tampoco se cerró tras el archivo judicial.

El gobierno nacional aprovechó la detención arbitraria para hacerlo pasar por un "desestabilizador", apoyándose en prejuicios sobre su origen y en supuesta información de inteligencia. Cuando se les requirió justificación, las agencias se ampararon en el secreto para no responder y otras dieron información recortada. Ninguna explicó de dónde salió la versión de que Baran era un terrorista o un desestabilizador que había que expulsar del país por violento o por ser un agente extranjero. Todo fue parte de una campaña de estigmatización de les extranjeres y de endurecimiento de la política migratoria.

El gobierno usó la cumbre del G-20 para endurecer, también, su discurso contra la protesta social y para exagerar su "guerra contra el terrorismo". Difundió información sobre organizaciones nacionales e internacionales que organizaban la contracumbre y las asoció con supuestas maniobras desestabilizadoras. A las acciones de vigilancia sobre protestas se agregó otra práctica grave: difundió que estaban siendo investigadas por movimientos de fondos sospechosos y nexos con el extranjero. También en este caso, envió información malintencionada a algunos medios de comunicación que afirmaba por ejemplo que la Inspección General de Justicia y los entes reguladores de lavado de activos investigaban la sede argentina de Attac, una de las organizadoras de la contracumbre, de la que incluso se filtraron datos bancarios secretos. Attac desmintió la acusación y no prosperó ninguna investigación formal en su contra. Sin embargo, estas maniobras fueron atemorizantes. Las organizaciones identificadas como desestabilizadoras se oponían al programa económico de los países que integran el G-20.

La sobreactuación tuvo su mayor expresión también durante el G-20, en la detención de los hermanos Kevin Gamal y Axel Ezequiel Abraham Salomón. Los jóvenes, integrantes de la comunidad musulmana en la Argentina, fueron acusados de pertenecer a Hezbollah. La Delegación de Asociaciones Israelitas Argentinas (DAIA) los denunció en la Unidad de Investigación Antiterrorista de la Policía Federal. La causa judicial se inició el 31 de enero de 2018, a partir de un correo electrónico anónimo que mencionaba el presunto entrenamiento militar en el Líbano de los acusados y la tenencia de un arma AK 47. Recién el 13 de noviembre, cuando la Policía Federal los detuvo en un allanamiento espectacular en el

barrio de Flores, supieron de esa denuncia. Dos días después, el Ministerio de Seguridad informó: "Luego del análisis técnico sobre distintas redes sociales, especialmente Facebook, los efectivos de la fuerza lograron individualizar los perfiles de los investigados y corroborar el contenido de la denuncia". El comunicado omitió que el juez federal Rodolfo Canicoba Corral había desestimado la denuncia de la DAIA porque no había encontrado ninguna conexión de los hermanos con supuestas células terroristas. El juez federal había enviado la investigación a la justicia ordinaria para que se investigara una posible tenencia ilegal de armas. En septiembre de 2018, la DAIA había ratificado la denuncia en el Juzgado nacional nº 36 y aportado la dirección del gimnasio donde ambos entrenaban. Ese mes, tras algunas tareas de inteligencia de la Policía de la Ciudad, el fiscal nacional de la causa solicitó su incompetencia porque como podía tratarse de personas vinculadas a redes terroristas le correspondía investigar a un fiscal federal. Uno de los principales elementos que valoró el fiscal fue que al local de venta mayorista de artículos de limpieza que posee la familia entraba poca gente. La defensa argumentó que el cliente principal del negocio es un colegio de la comunidad judía que está a metros del comercio familiar. Luego de que la investigación volviera al fuero federal, el juez ordenó el allanamiento y la detención de Kevin y Axel. El día de la detención, Patricia Bullrich dijo que el Ministerio de Seguridad y la AFI venían investigándolos y que los habían detenido por "mucha información internacional de agencias de Estados Unidos, Inglaterra, Canadá".

Los hermanos Salomón estuvieron veintidós días detenidos en el penal de Ezeiza. Les rechazaron la excarcelación mientras en los medios de comunicación asociaban este y otros casos con una "violencia anarquista" que, según la ministra, ponía "en juego al Estado". Casi cinco meses después, el juez Sebastián Ramos los sobreseyó.

Como consecuencia del montaje del operativo, la comunidad musulmana fue forzada a explicar que los hermanos no eran terroristas. Sus nombres, domicilios y religión fueron repetidos infinidad de veces por los medios. La conmoción fue enorme para ellos y su familia. Ya con la libertad recuperada, narraron lo vivido. Kevin Gamal lo sintetizó así: "El Estado nos expuso ante los medios mostrando nuestro rostro y nombre, perdí mi trabajo, tiempo de estudio, ponés mi nombre en internet y salgo esposado al lado de la Federal, las armas de mi bisabuelo y títulos como 'terrorista'".[3]

3 A. Meyer, "El gobierno de Patricia Bullrich nos arruinó la vida", *Página/12*, 4 de abril de 2019.

Como se mencionó, el origen de este montaje fue un correo electrónico anónimo que recibió la DAIA, pero en la investigación no se peritaron ni la computadora, ni la cuenta que recibió el mensaje. Nadie dio explicación alguna. Las actividades de inteligencia que justificaron las detenciones quedaron bajo secreto, al igual que las supuestas investigaciones por lavado de activos contra las organizaciones que se oponían al G-20. Con el pretexto de la seguridad nacional, el Poder Ejecutivo una vez más corrió el límite que separa la inteligencia legal del espionaje ilegal. La vigilancia de organizaciones y personas por sus opiniones políticas o su nacionalidad no es prevención del terrorismo, sino espionaje ilegal contra la disidencia. Su difusión no busca otra cosa que demonizar e intimidar a sectores y grupos sociales. En esta lógica del secreto, el Poder Judicial convalidó la trama de producción de información: liberó a quienes fueron acusados falsamente, pero no desarmó ni criticó el dispositivo de producción de información y de seguridad que llevó a las acusaciones y al despliegue político mediático.

Activistas perseguides

Un año antes, en diciembre de 2017, tuvo lugar en la CABA la IX Conferencia Ministerial de la Organización Mundial del Comercio (OMC). El 29 de noviembre, varies integrantes de organizaciones acreditades para participar en los foros recibieron un correo electrónico del jefe de Relaciones Exteriores de la OMC en el que les informaba que el gobierno argentino había decidido cancelar sus acreditaciones. El episodio advirtió sobre las prácticas de vigilancia secretas que el gobierno estaba desplegando en "defensa de la seguridad nacional".

Alrededor de sesenta argentines y extranjeres fueron desacreditades. El 2 de diciembre, el Ministerio de Relaciones Exteriores informó:

> El equipo de Seguridad de la organización de esta Conferencia Ministerial anticipó a la OMC la existencia de algunos inscriptos, registrados por dicha Organización en nombre de algunas ONG, que habían hecho explícitos llamamientos a manifestaciones de violencia a través de las redes sociales, expresando su vocación de generar esquemas de intimidación y caos. En función de la calificación de tales antecedentes, la organización local ha entendido oportuno indicar que las personas asociadas a tales propuestas disruptivas y/o violentas no podrían ser acreditadas para ingresar al recinto de reuniones de la Conferencia Ministerial.

Es decir que la peligrosidad se basó en el análisis de expresiones y antecedentes personales recolectados en las redes sociales. El listado de personas elaborado, según la Cancillería, por el "equipo de Seguridad" fue enviado a Migraciones y a la OMC.

No obstante, algunes activistas decidieron venir a la Argentina. Varies fueron demorades en el aeropuerto de Ezeiza y a otres directamente se les impidió ingresar. Por esta situación, el CELS presentó un hábeas corpus luego del cual el Estado no demoró a nadie más en el aeropuerto. Les extranjeres requirieron apoyo a sus países para que se revisara la exclusión, mientras que les argentines que habían sido calificades de peligroses por su propio país, no pudieron ingresar a la conferencia.

Del comunicado oficial derivan dos cuestiones. Por un lado, que alguna agencia estatal recolectó y analizó información de quienes habían pedido acreditación, datos que en principio provinieron de las redes sociales. Por otro, que algún órgano del Poder Ejecutivo consideró que se trataba de "personas asociadas a propuestas disruptivas y/o violentas" a partir de la "calificación de antecedentes" y envió esa lista a la OMC para que no participaran de la conferencia, y a la Dirección Nacional de Migraciones para que les extranjeres no ingresaran al país.

En resumen, una dependencia del Ejecutivo ordenó tareas de inteligencia sobre les acreditades a la OMC y restringió sus derechos porque consideró que sus expresiones y opiniones políticas evidenciaban una "vocación de generar esquemas de intimidación y caos". Que el motivo de las desacreditaciones haya sido este es una conjetura, dado que nunca explicaron cuáles fueron esas expresiones. El CELS solo pudo reconstruir por vía judicial que la AFI le envió información a la Cancillería de las personas afectadas. Una suerte de derecho de admisión al país y a la Conferencia, sin explicitar los criterios ni justificar la desacreditación en cada caso. Esto ocurrió aunque la Ley Nacional de Inteligencia prohíbe a todos los organismos

> obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.

Esta norma, sancionada en 2001 durante el gobierno de la Alianza como parte del acuerdo político posdictatorial, prohibió expresamente que las

agencias encargadas de la inteligencia realizaran espionaje político, de cualquier tipo.

En respuesta a un pedido de acceso a la información y un hábeas data presentados por el CELS, la Cancillería acompañó las notas enviadas a la OMC en las que había solicitado la desacreditación de les activistas y a la Dirección Nacional de Migraciones con la lista de quienes no debían ingresar. No aportó información sobre cómo se había confeccionado ese listado, qué datos habían justificado las desacreditaciones, ni si esos datos habían quedado recopilados y registrados en alguna dependencia estatal. La Cancillería, además, redirigió la solicitud del CELS al Ministerio de Seguridad y a la Agencia Federal de Inteligencia. Seguridad respondió que no contaba con información pública ni personal sobre las personas en cuestión, mientras que la AFI sostuvo, a través de una nota a la que también le aplicó un código de seguridad, que la información solicitada era secreta y que ni la Ley de Acceso a la Información Pública ni la de Protección de Datos Personales eran aplicables a esa agencia. Se negó a confirmar, incluso, si tenía o no información.

Con respecto a este último punto, la AFI explicó:

> Responder que no existe dato alguno relativo al actor, implicaría en los hechos revelar información, no ya del nombrado, sino que no ha sido objeto de actividad de inteligencia alguna. A modo ilustrativo, podemos señalar que de considerar el acceso a los bancos de datos de la AFI en los términos que solicita el actor, podría implicar dotar a futuro a quienes realicen las actividades delictivas que son materia de las competencias de esta Agencia (delitos federales complejos relativos a terrorismo, narcotráfico […] así como los delitos contra los poderes públicos y el orden constitucional), conocer por esta vía, si son o han sido sujetos de las actividades propias del Organismo.

Esta respuesta es clarificadora: cualquier persona puede ser objeto de inteligencia estatal porque puede estar relacionada con actividades delictivas de su competencia. La AFI afirma que no está obligada a justificar qué estándares objetivos la habilitan a recopilar, acopiar y evaluar datos personales. Tampoco considera que deba responder a los requerimientos judiciales que le preguntan por estos criterios o por los motivos concretos de una vigilancia realizada.

No hay forma de saber, entonces, si la AFI recopila datos personales o de organizaciones, ni tampoco en base a qué circunstancias –sean legales o ilegales– se decide hacer inteligencia sobre esos "objetivos", porque

siempre responderá que las actividades de inteligencia no están alcanzadas por los controles. Sin duda, el argumento se muerde la cola: si nadie puede conocer esas acciones, ¿cómo se las controla política y judicialmente para asegurar que estén dentro de la legalidad? Pero, además, la AFI no es una agencia de investigación criminal, aunque lo pretenda y se lo pidan. Las investigaciones penales tienen otra lógica que, justamente, permite el ejercicio de la defensa en juicio.

La respuesta de la AFI no indica qué circunstancias concretas relacionan a quien pidió conocer los datos con alguna hipótesis de riesgo para la seguridad nacional. Esta situación implica una denegación del derecho a acceder a la información, pero implica también algo más grave: está en juego la posibilidad de defenderse de una sospecha estatal. ¿Por qué el Estado puede sostener ese nivel de incertidumbre sobre si una persona está siendo investigada por terrorismo o narcotráfico y privarla de su derecho a defenderse? ¿Cómo puede alguien articular una defensa, si no puede conocer los motivos por los que se le acusa y se violentan sus derechos? ¿Cómo se asegura que, una vez descartada cualquier hipótesis criminal, los datos personales serán destruidos? ¿Ni siquiera bajo requerimiento judicial el Poder Ejecutivo debe informar qué datos recopiló? ¿Es una necesidad del Estado mantener ese secreto?

La decisión oficial de desacreditar activistas de la cumbre de la OMC se basó en información recopilada por la AFI, que fue usada para restringir los derechos de reunión, libertad de expresión, privacidad e intimidad. Es posible que esta información, o parte de ella, provenga de las redes sociales a las que se suele llamar "fuentes abiertas", porque el acceso a esos datos no requiere una intrusión legal, como el caso de una orden judicial para intervenir un teléfono en la investigación de un secuestro, o ilegal. Pero que la fuente sea "abierta" no convierte de manera automática el trabajo de inteligencia en legal. Por un lado, las personas tienen una expectativa lógica de privacidad que es vulnerada cuando la vigilancia sobre ellas es masiva y sistemática. Por otro, el uso que se hace de la información personal compilada de fuentes abiertas puede ser ilegal si viola las categorías que están prohibidas por la Ley Nacional de Inteligencia, en este caso los motivos políticos (art. 4, inc. 2 de la Ley 25 520).

El gobierno nacional expandió sus prácticas de inteligencia y las sostuvo en el mayor secreto por razones de "seguridad nacional". La sospecha activa el engranaje estatal de la vigilancia, pero no hay explicación que justifique esa sospecha ni las acciones que de ella se derivan. El aval político a la negativa de la AFI a brindar información consolida la incertidumbre. Bajo esta lógica, todes pueden ser vigilades y nadie puede saber si se le investiga.

2. Políticas secretas

Una AFI sin control

El sistema de inteligencia nacional siempre estuvo regido por la lógica del secreto. Desde sus comienzos, se lo asoció a la doctrina de la seguridad nacional de corte militar, a la cultura política del espionaje político y, luego del atentado a las Torres Gemelas en 2001, a la justificación de la doctrina de las "nuevas amenazas". En 2015, tras la crisis provocada por la muerte del fiscal Alberto Nisman y la salida de Antonio Stiuso de la Secretaría de Inteligencia, se avanzó en la reforma de la Ley Nacional de Inteligencia y en modificar en parte esta opacidad con la introducción de reglas de mayor publicidad. Pero la ley tuvo sus limitaciones, y aspectos esenciales quedaron sujetos a su reglamentación. El Decreto 1311/2015 reguló cuestiones importantes como el régimen de fondos reservados, los procedimientos de desclasificación de la información y una estructura organizacional más transparente. Sin embargo, esos cambios normativos, que tampoco habían llegado a implementarse del todo, los desarmó el presidente Mauricio Macri con el Decreto 656/2016.

En respuesta a pedidos de acceso a la información presentados por el CELS, el Poder Ejecutivo y la AFI dijeron explícitamente que todo lo relativo al sistema de inteligencia nacional había vuelto a ser absolutamente secreto por razones de seguridad nacional. Incluso la AFI clasificó su propia respuesta como secreta:

> La Ley de Acceso a la Información Pública […] no es aplicable a esta AFI, atento a la existencia de la ley específica […]. Toda la información de esta Agencia es reservada siendo necesaria, aún en los supuestos de menor grado de reserva, de la dispensa a la que hace referencia el art. 16 y cc. de la referida Ley de Inteligencia, facultad delegada en el sr. director general de esta Agencia Federal de Inteligencia (conforme art. 11 del Decreto 950/2002).

Según la AFI, la información que produce, su regulación y actividad son secretas. Esto abarca todo: la normativa general, la estructura, las tareas que desempeña, la ejecución de fondos, la información producida y la nómina de personal. La AFI no pone a disposición ninguna información pública, ni justifica las restricciones de acceso a la información. Pero esta interpretación contradice al art. 16 bis de la Ley Nacional de Inteligencia, que establece tres clasificaciones de seguridad: secreto, confidencial y público. También desconoce los estándares constitucionales e

internacionales sobre el derecho a acceder a información pública. Estos estándares obligan al Estado, aun cuando alegue la excepción de seguridad nacional, a justificar la restricción y a clarificar los criterios por los que la información es clasificada como secreta o confidencial.[4] Así, la AFI funciona como si estuviera exceptuada de cumplir las normas que establecen controles a su funcionamiento.

En un primer pedido de acceso en 2016, el CELS consultó por la regulación de los fondos reservados, un gran porcentaje del presupuesto de la AFI por el que nadie rinde cuentas. Estos fondos permiten las operaciones y acciones encubiertas, como el armado de empresas pantalla, el uso de agentes inorgánicos y los pagos a informantes. Son los recursos que permiten sostener las redes, legales e ilegales, de agentes. La ley exige que los organismos del sistema tengan procedimientos de registro y rendición de estos fondos, con la documentación de respaldo que sea posible.

El pedido había sido dirigido al jefe de Gabinete Marcos Peña, pero la respuesta fue del director de la AFI, Gustavo Arribas: "Se han establecido y se encuentran vigentes diversos procedimientos y controles que conforman un sistema de administración de fondos que responde a los más elevados estándares de transparencia y profesionalismo". No especificó ningún procedimiento, ni dónde estaban regulados los controles supuestamente vigentes.

Además, Arribas apeló en abstracto al régimen del secreto de la Ley de Inteligencia, incluso para negarse a informar sobre la existencia o no de regulaciones administrativas generales. Tampoco respondió sobre qué políticas habían desarrollado para transparentar las actividades de inteligencia, ni cómo planeaba cumplir con el Decreto 812/2005, que materializa los compromisos asumidos por el Estado argentino en el caso AMIA ante la Comisión Interamericana de Derechos Humanos (CIDH) y que obliga a transparentar el sistema de control de fondos reservados. La respuesta también fue negativa para el intento de conocer cómo estaban reguladas las categorías de clasificación de seguridad de la información y los plazos y procedimientos para su desclasificación; si existían acuerdos

4 Véase, por ejemplo, "Seguridad nacional y acceso a la información en América Latina: estado de situación y desafíos", CAinfo y CELE, 2012, y los "Principios globales sobre seguridad nacional y el derecho a la información ('Principios de Tschwane')", 2013.

de intercambio de información de inteligencia con terceros países;[5] y la cantidad, el mecanismo de resguardo y el control parlamentario de las captaciones telefónicas de inteligencia.

Frente a esta denegatoria absoluta por parte de la AFI, el CELS presentó un amparo judicial. El juez de primera instancia convalidó la interpretación de la Agencia. Pero a fines de junio de este año la Cámara Federal de Apelaciones en lo Contencioso Administrativo reconoció de manera parcial el derecho de acceso a la información pública. En la primera sentencia de Cámara contra la AFI por un reclamo de este tipo, los jueces sostuvieron que, por más que se trate de información de inteligencia, no dejan de aplicarse los principios del derecho al acceso a la información pública. La Cámara afirmó que la Ley de Inteligencia regula específicamente la actividad de la Agencia, pero que no se puede desestimar *per se* un pedido de acceso sin evaluar judicialmente si corresponde aplicar la excepción de que se trata de un tema de seguridad nacional o defensa para el que deba regir el secreto. En este sentido, afirmó que no toda la información en poder de la AFI es necesariamente secreta y le exigió que entregara el reglamento que rige la desclasificación de la información, uno de los puntos solicitados en el amparo, para así poder evaluar si fue arbitraria o no la negativa a informar. Si la sentencia queda firme, la AFI deberá suministrar esa reglamentación, lo que permitirá conocer qué está clasificado y qué no y romperá el secreto absoluto que pretende mantener. El problema, aun en este escenario es que, en general, les jueces son reticentes a revisar el contenido del secreto o de las excepciones que alegan los organismos de inteligencia, concediendo la justificación de defensa y seguridad nacional.

La AFI volvió a negarse a brindar información en 2018, cuando el CELS le consultó por la desacreditación de participantes a la cumbre de la OMC.

El silencio burocrático del Ministerio de Seguridad

Desde fines de 2015, la gestión de Patricia Bullrich promovió la política activa de inserción de la Argentina en la coalición global contra las "nuevas amenazas". La ministra viajó en reiteradas oportunidades a los Estados Unidos, Israel y Gran Bretaña para generar "una agenda de tra-

5 Este punto se desprende de un proyecto realizado en coordinación con los demás miembros de la red Inclo, que dio lugar al informe "Preguntas sin respuesta. Intercambio internacional de inteligencia", 2018.

bajo común" con esos países, que incluyó acuerdos sobre seguridad, ciberseguridad, adquisición de tecnología e intercambio de información. La comunicación oficial mostró esos actos como parte central de la política de seguridad y ubicó a la Argentina en la pelea contra las amenazas a la seguridad nacional y al orden público. Según esta lógica, el Estado debe incrementar su vigilancia sobre la población para protegerla de estos peligros indeterminados. Más allá de lo que circuló en la prensa, es muy poco lo que se sabe de estos acuerdos.

Esta política de expansión secreta de las prácticas de inteligencia y vigilancia quedó al descubierto cuando en 2017 estalló el escándalo de la Operación Huracán, en Chile, un operativo que buscó criminalizar a las comunidades mapuches y a las organizaciones y activistas que los apoyaban. La causa judicial que investiga cómo se efectuó el espionaje ilegal, con responsabilidades que llegan a la jefatura de inteligencia de Carabineros y a miembros del Ministerio Público Fiscal, reveló un vínculo muy aceitado de intercambio de información de inteligencia entre la Gendarmería Nacional Argentina y los Carabineros de Chile, validado por las autoridades políticas argentinas y chilenas.[6] La documentación que se pudo conocer muestra que esa colaboración ilegal busca ampararse en la hipótesis de seguridad nacional que llaman "conflicto mapuche", al que dan una connotación de carácter "subversivo". Entre los documentos y chats encontrados, estaba el envío de información por parte de Gendarmería a Carabineros sobre la desaparición de Santiago Maldonado, minutas de reuniones de las jefaturas de inteligencia de ambas fuerzas, informes de migraciones, referencias a datos personales de activistas y de comunidades. El análisis permite sospechar que hubo una triangulación de captación de comunicaciones realizadas por los Carabineros sobre personas de nacionalidad argentina. Estas prácticas de vigilancia denunciadas, y ahora conocidas, quedan enmarcadas en las posiciones del Ministerio de Seguridad que, frente a los conflictos ambientales y por la tierra en la Patagonia, distribuyó el llamado informe "R.A.M." en el que asociaba las comunidades indígenas con hechos de desestabilización y violencia. Las regulaciones para estos intercambios y los acuerdos de colaboración se mantienen en secreto.

6 N. Sepúlveda, "Chats de inteligencia: la red de Carabineros para inculpar a mapuches en tráfico de armas que involucró a agentes argentinos", *Ciper*, 23 de abril de 2019; S. Premici, "Caso Maldonado: espionaje conjunto entre Gendarmería y Carabineros", *Cadena del Sur*, 29 de abril de 2019.

Entre 2016 y 2018, el CELS envió treinta solicitudes de información pública al Ministerio de Seguridad de la Nación sobre acuerdos celebrados por el ministerio con otras entidades o gobiernos, reglamentación y protocolos, represión de la protesta social y otros hechos de violencia institucional, funciones de las dependencias y programas, sumarios administrativos por irregularidades por parte de agentes federales de seguridad, y datos sobre detenciones y uso de la fuerza. El ministerio no siempre invocó motivos de "seguridad nacional" para rechazar los pedidos. También apeló al silencio burocrático como contestación: en ocasiones no respondió, y en otras, aun cuando existió una respuesta formal, omitió los puntos solicitados. El secreto –por seguridad nacional– y el silencio se retroalimentaron.

El silencio burocrático fue la respuesta, por ejemplo, a la solicitud de información sobre los acuerdos firmados por la ministra en su visita a la sede del Comando Sur de los Estados Unidos, en mayo de 2018, y sobre el diseño del operativo en el que fue asesinado Rafael Nahuel, el integrante de la comunidad mapuche de Villa Mascardi.

Con esta misma lógica, se mantuvieron en secreto cuestiones relativas a la política de defensa y la actuación de las Fuerzas Armadas en tareas de seguridad interior. Tras el lanzamiento del Operativo Integración Norte –que el Ministerio de Defensa creó con la Resolución 860/2018–, el gobierno estableció que las Fuerzas Armadas cumplieran funciones de apoyo logístico, adiestramiento operacional y apoyo a la comunidad en la frontera del norte argentino. Las "reglas de comportamiento" para les militares destinades a dicho operativo fueron declaradas bajo "secreto militar". Esto no había sucedido en gestiones anteriores de Defensa –incluso de este mismo gobierno, como la de Julio Martínez– que implementaron operaciones en la frontera norte. Así, les habitantes del país no tienen posibilidad de saber lo que les militares deben o no hacer en Integración Norte. Esto es un obstáculo para el control civil de la actuación militar, mientras se profundizan las funciones de les militares en ámbitos de seguridad interna. El ministerio extendió este uso del secreto militar a los operativos de seguridad, por lo que tampoco se puede conocer gran parte de la política que guía su actuación.

3. El Estado espía

En el marco de la política de ampliar las redes estatales de vigilancia e investigación para "luchar contra las amenazas", el gobierno y varios ac-

tores judiciales buscaron incorporar tecnologías digitales invasivas en los sistemas de inteligencia y de investigación criminal. El avance tecnológico abrió puertas a intervenciones estatales secretas que pueden afectar la vida privada de las personas y sus actividades políticas y sociales. La preocupación por el uso de estas herramientas y sus efectos en los derechos humanos y en la vida democrática es global. En la Argentina, aún falta desarrollar un marco regulatorio y mecanismos de control reales, mientras ya no quedan dudas sobre la existencia de una red extendida de intercambio ilegal de información de inteligencia, extorsiones y espionaje político, con fuerte inserción estatal. A pesar de que a esta altura no pueden ocultarse los vínculos ilegales entre las estructuras de inteligencia y los sectores judiciales y políticos, la mayor parte del sistema político acepta la extensión y ramificación de las herramientas de vigilancia y producción de información masiva.

Bienvenido Rafael a la Argentina

En octubre de 2018, poco antes de la cumbre del G-20 en la CABA, el Ministerio de Defensa compró un *software* de vigilancia de la empresa privada Rafael Systems, en el marco del Memorándum de Entendimiento sobre Cooperación Industrial y Tecnológica en Defensa firmado por la Argentina e Israel en 2010. En el *Boletín Oficial*, se publicó la aprobación del gasto derivado del Acuerdo de Implementación entre los ministerios de Defensa de esos países. De ese acuerdo surge que el Ministerio de Defensa argentino acordó con el de Israel la contratación de bienes y servicios para el Proyecto Núcleo de Computer Security Incident Response Team (Csirt) y Computer Emergency Response Team (CERT). El contratista principal del proyecto fue la empresa estatal israelí Rafael Advanced Defense Systems Ltd., en nombre del ministerio israelí.

En distintas notas en los medios a raíz de la cumbre del G-20, el gobierno difundió la contratación de Rafael Systems. La empresa desarrolla herramientas que utilizan inteligencia artificial y *machine learning* para monitorear fuentes abiertas y procesar esa información en función de los parámetros que recibe sobre lo que se pretende buscar. Esto permite, por ejemplo, comprender o predecir acciones que grupos activistas podrían estar organizando a través de sus redes sociales. El acuerdo tiene diez anexos que no son públicos, tampoco lo es el objeto de la contratación ni en qué consisten los bienes y servicios que Rafael Systems prestaría. Sin embargo, la información disponible alcanza para afirmar que se trata de un *software* de vigilancia con la potencialidad de afectar de manera desproporcionada la privacidad de les usuaries de internet.

Los medios se hicieron eco del posible uso que tendría una vez finalizado el G-20:

> Obviamente, después del G-20 esa tecnología y las capacitaciones que fueron necesarias quedan, seguirán profundizándose, y las Fuerzas Armadas locales tienen ahora capacidad para resolver los hitos más complejos en materia de cruce de información sensible.[7]

La Argentina no cuenta con un marco normativo ni mecanismos de control sobre este tipo de herramientas, que en otros países se emplean para vigilancia masiva ilegal.[8] Tampoco hay una regulación sobre qué se entiende por fuentes abiertas o qué es lícito hacer con ese tipo de información, indefiniciones que pueden habilitar prácticas prohibidas. El *software* se adquirió y opera en condiciones de secreto y, hasta donde se puede conocer, ningún organismo del Estado verifica su uso, quién lo administra y si es proporcional al peligro que se busca prevenir. En otras palabras, no hay manera de saber si se ajusta a lo previsto en la Ley de Inteligencia o si se trata de vigilancia o inteligencia ilegal.

El 25 de abril de 2019, la CABA comenzó a implementar el sistema de reconocimiento facial para detectar y detener a quienes cuenten con una orden judicial de captura. Según el vicejefe de Gobierno de la Ciudad Diego Santilli, a cargo del Ministerio de Seguridad local, este sistema permitirá agilizar la búsqueda de "material forense", es decir, pruebas que antes requerían muchas horas de examen y que ahora se procesarán de manera automática. El sistema utilizará la capacidad instalada de cámaras y centros de monitoreo de la ciudad que, según el gobierno, ya cuenta con 10 000 dispositivos.[9]

La experiencia del uso de esta tecnología en otros territorios no fue exitosa. Por ejemplo, en Gales del Sur hubo hasta un 92% de falsos

7 S. Mercado, "Cómo funciona la empresa israelí de seguridad que inventó la 'cúpula de hierro' y ya opera en la Argentina", *Infobae*, 24 de diciembre de 2018.

8 Véase Inclo, "Vigilancia y democracia. Historias en diez países", noviembre de 2016. A principios de 2019, las trece organizaciones de la red Inclo manifestamos al Relator Especial de Naciones Unidas –en el marco de la elaboración de su informe sobre el tema– nuestra preocupación sobre el derecho a la libertad de reunión pacífica y de asociación, por el uso de estas tecnologías en contextos de protesta y reunión.

9 "Desde el 15 de abril buscarán a prófugos con sistema de reconocimiento facial", *Ámbito Financiero*, 4 de abril de 2019.

positivos en un episodio reciente, según datos de la policía,[10] y 0% de efectividad en Nueva York, según un correo electrónico interno de la Autoridad Metropolitana de Transporte (MTA) al que el *Washington Post* tuvo acceso.[11] Los falsos positivos no son inocuos: obligan a las personas sospechadas a demostrar su inocencia. En la CABA, el reconocimiento facial masivo no pasó por la Legislatura ni implicó algún tipo de discusión política. No se sabe cuál es el *software*, cómo fue adquirido, quién lo ejecuta, ni bajo qué normas o mecanismos de control.

Cuando investigar es espiar

La tendencia a ampliar las capacidades estatales para invadir la privacidad llegó también al ámbito de la investigación penal. Durante 2016 y 2018, les diputades y senadores debatieron la pretensión del Ejecutivo y de algunas fuerzas políticas de modificar el régimen procesal penal federal e incorporar nuevas técnicas de investigación que implicaran algún tipo de vigilancia: acústica, remota de los equipos informáticos y a través de dispositivos de seguimiento y de localización. El acceso remoto a los teléfonos móviles puede conducir a un seguimiento en tiempo real mediante la cámara, el micrófono o el GPS, de manera encubierta. Estas tecnologías permiten registrar capturas de pantalla de lo que la persona está viendo, pulsaciones sobre el teclado y lo que escribe (nombres de usuarie, contraseñas, historial de navegación), así como todas las comunicaciones (mensajes, correos electrónicos, llamadas). También es posible manipular los datos almacenados, adulterarlos o borrarlos. Todas estas actividades, además, pueden efectuarse sin dejar rastros. Un grupo amplio de organizaciones[12] realizaron fuertes críticas, y distintos bloques de la oposición rechazaron el capítulo relacionado con la vigilancia que

10 Universities' Police Science Institute Crime and Security Research Institute, Cardiff University, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, septiembre de 2018.

11 "MTA's Initial Foray Into Facial Recognition at High Speed Is a Bust", *The Wall Street Journal*, 7 de abril de 2019, y "Nueva York probó un sistema de reconocimiento facial en las calles y fue un fracaso rotundo", *TN*, 9 de abril de 2019.

12 Comunicado conjunto de la Asociación por los Derechos Civiles (ADC), Asociación Civil por la Igualdad y la Justicia (ACIJ), Asociación Pensamiento Penal (APP), Instituto de Estudios Comparados en Ciencias Penales y Sociales (Inecip) y el CELS, "La reforma del Código Procesal amplía las facultades del Estado para vigilar", 17 de abril de 2018.

el gobierno había agregado al proyecto de reforma procesal. Finalmente, no fue aprobado.

El Poder Ejecutivo de la CABA también intentó impulsar estas medidas, aunque el sistema de justicia local no tiene a su cargo la investigación de delitos de criminalidad compleja que podrían requerir tales herramientas. Eso puso más en evidencia la receptividad política del *lobby* de negocios, policial y de inteligencia para contar con dicha tecnología y sus posibles usos. Varias organizaciones especializadas y de derechos humanos lograron frenar las medidas más problemáticas de vigilancia electrónica, pero se incorporaron figuras como el agente encubierto y revelador, y los informantes con remuneración económica, que ya habían sido agregadas con controversias al ámbito nacional en la Ley 27 319.

La Corte Suprema como parte del sistema de inteligencia

La cuestión de las escuchas de inteligencia o judiciales es otro nudo del debate, que muestra la pulsión estatal por ampliar sus capacidades de vigilancia e involucrar al sistema judicial en la expansión de esas herramientas.

En la Argentina, la facultad de captar comunicaciones y hacer escuchas estuvo asociada al espionaje ilegal. La reforma del sistema de inteligencia en 2015 desarmó la oficina de la vieja SIDE –conocida como "Ojota" por las iniciales de Observaciones Judiciales– y sus competencias pasaron al Ministerio Público Fiscal. Sin embargo, como parte de su disputa contra la entonces procuradora general de la Nación, Alejandra Gils Carbó, a fines de 2015 el Ejecutivo transfirió por decreto la competencia a la Corte Suprema de Justicia de la Nación. Con este pase de magia, la Corte vio ampliado su poder e incorporó facultades de inteligencia e investigación que no le correspondían. Según ellos mismos difunden en notas periodísticas, la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado (Dajudeco) se dedica además a realizar análisis financieros, mapas de relaciones, perfiles económicos y rastreos en redes sociales, entre otras facultades abocadas a investigar el crimen organizado y la corrupción pública y privada.[13] La Corte incorporó también funciones de centralización y análisis de información y firmó convenios con la AFI, la Unidad de Información Financiera (UIF), la Administración Federal de Ingresos Públicos (AFIP) y el Ministerio de

13 M. Jastreblansky, "Amplían las atribuciones de la oficina de escuchas", *La Nación*, 8 de abril de 2018.

Justicia de la Nación que, entre otras cuestiones, le otorgaron acceso a las bases de datos.

Este armado consolidó de un modo increíble y legalmente cuestionable otro de los aspectos claves de la crisis del sistema: el convenio entre la Corte y la AFI restauró el viejo esquema de escuchas y convalidó la gestión e intervención directa de la estructura judicial federal en áreas y tareas de inteligencia, con apoyo directo de la AFI. Que la Corte sostenga una estructura de inteligencia en su propio ámbito alimenta vicios naturalizados con consecuencias muy negativas para la legalidad, la transparencia y la legitimidad de las investigaciones judiciales. La participación de las áreas de inteligencia en las investigaciones penales implica el riesgo de tergiversar las reglas procesales, limita la capacidad de control para las partes y de rendición de cuentas en general. Bajo este esquema, la Corte quedó involucrada en la crisis del sistema de inteligencia.[14] Estas decisiones implican que el máximo tribunal comparte el programa político que sostiene que, para ser eficaz "en la lucha contra el crimen y la corrupción", la Corte Suprema misma debe convertirse en una agencia de investigación e inteligencia en vez de fortalecer su función constitucional de control y resguardo de derechos.

En estos últimos años proliferaron las intervenciones telefónicas en casos penales. Cada vez más, les fiscales y jueces, de diverso fuero, piden y aceptan medidas invasivas de la privacidad que afectan a acusades, víctimas y testigues. Esta lógica punitiva naturaliza la expansión de la intervención estatal con herramientas de vigilancia. Tanto el gobierno como un amplio sector judicial plantean que las intervenciones telefónicas son necesarias para investigar cualquier delito y celebran el incremento de estas prácticas como un indicador de eficiencia. Al mismo tiempo, se conocieron tantas filtraciones de escuchas que ya es habitual que se reproduzcan comunicaciones privadas en los medios sin que se cuestione su origen. Por ejemplo, en la investigación sobre la desaparición y muerte de Santiago Maldonado las partes se enteraron de que estaban siendo escuchadas a partir de una nota periodística. Incluso los diarios divulgaron diálogos privados del hermano de Santiago.

14 Comunicado de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia (Iccsi), "Escuchas: la Corte Suprema en el centro de la crisis del sistema de inteligencia", 5 de abril de 2018.

4. Controlar a las personas, no controlar a los poderes

Mientras el secreto de las actividades estatales de inteligencia y seguridad es la regla, se impone la pregunta por los esquemas de control: ¿cómo pueden las personas u organizaciones controlar y saber qué información se tiene sobre ellas y si la actividad estatal es legal? Las instancias administrativas, judiciales y políticas son incapaces de confrontar el secreto y la resistencia de los organismos a ser controlados. Sus prácticas –por convicción ideológica, complicidad o desidia– son parte o convalidan la opacidad creciente del sistema de seguridad e inteligencia.

El Congreso (a través de las Comisiones Bicamerales de Seguridad y de Fiscalización del Sistema de Inteligencia) y el Poder Judicial tienen funciones de control de las políticas y el desempeño de las agencias de inteligencia y seguridad, así como de protección de derechos en casos concretos. También la Agencia de Acceso a la Información Pública (AAIP) tiene funciones relevantes para pelear contra la lógica del secreto que prevalece, como vimos, aun cuando se lograron avances normativos para acceder a este tipo de información. Por ejemplo, las leyes 27 275 de Información Pública, 25 520 de Inteligencia (reformada por la 27 126) y 25 326 de Datos Personales establecen reglas para definir cuándo la información debe ser pública y cuándo puede desclasificarse y entregarse aunque se la haya considerado confidencial o secreta. Si bien estas leyes e instituciones no conforman una estructura de control muy sofisticada, tampoco suelen funcionar de manera adecuada.

La Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia casi no tiene actividad. Y si la tuviera, sería secreta. Se trata de un mecanismo político casi inactivo, alcanzado además por la lógica del secreto, por lo que es parte del mismo sistema degradado.

En las vías de reclamo administrativo, los intentos del CELS por conseguir información fracasaron: no hubo respuestas satisfactorias a las solicitudes de acceso a la información pública, ni a los reclamos ante la AAIP y la Dirección de Datos Personales que depende de ella (órganos de aplicación de las leyes de Acceso a la Información Pública y de Protección de Datos Personales, respectivamente).

Varios meses después del reclamo por el rechazo de los pedidos sobre la cumbre de la OMC, la Agencia respondió que el Ministerio de Seguridad había contestado todas las preguntas de forma clara, que la Cancillería lo había hecho "en tiempo y forma" cuando luego de la intimación judicial tuvo que mostrar memos y cables internos muy relevantes, y que tampoco había habido denegatoria injustificada de la AFI

porque había informado su no intervención "en las cuestiones relacionadas con la acreditación de los participantes a la Cumbre Mundial de la OMC". No se pronunció sobre la interpretación de la AFI de quedar fuera del ámbito de aplicación de las leyes de acceso a la información y de datos personales. Pero sí agregó que

> si la reclamante considerara que hubo un accionar "malicioso" por parte de los sujetos obligados requeridos […] debería presentarse ante la sede correspondiente ya que dichas especulaciones no configuran elementos dentro de un reclamo de acceso a la información pública.

Con esta respuesta terminó la posibilidad de reclamo administrativo sin que ninguna dependencia del Ejecutivo contestara en serio sobre la base de qué información había desacreditado por "peligrosos" a les participantes de la cumbre.

En su informe anual, la Relatoría Especial de Libertad de Expresión (RELE) de la CIDH mencionó la situación del derecho de acceso a la información pública en la Argentina, en los casos en que se rechaza el acceso por "seguridad nacional".[15] Asimismo expresó su preocupación por la dificultad, casi imposibilidad, de las personas para acceder a información vinculada con temas de inteligencia o seguridad nacional porque es considerada secreta, y señaló las debilidades de las instancias de control para hacer valer los estándares internacionales. Hizo mención al caso de la cumbre de la OMC, y recordó los estándares que deben regir en estos supuestos.

Pocos días después de la publicación de este informe, la AAIP resolvió, en otra demanda, que la AFI tiene la obligación de brindar cierta información.[16] La AFI había entendido que lo que le solicitaban era secreto y lo había justificado en una resolución también secreta que no presentó. La Agencia decidió que, si bien la información solicitada en efecto era secreta –en función de las leyes de Inteligencia Nacional y de Acceso a la Información Pública–, la AFI debía hacer público "el índice de información que se encuentra reservada por el organismo": "Corresponde que el sujeto obligado tenga en cuenta que al momento de denegar la información debe notificar el acto administrativo que se dicte al efecto, lo cual se

15 Relatoría Especial de Libertad de Expresión, CIDH, *Informe Anual 2018*.
16 Véase RESOL-2019-46-APN-AAIP, 26 de marzo de 2019.

omitió en el caso". La solución de la AAIP es correcta para garantizar el debido proceso ya que exige que se den a conocer el listado (o índice) de documentación que la AFI clasifica como secreta o confidencial y el fundamento de la denegatoria de acceso. Sin embargo, su alcance es limitado para romper la lógica del secreto con que funcionan las agencias de inteligencia y seguridad. Para esto es preciso que los órganos de control intervengan con más fuerza y desarrollen mejores estándares sobre la cuestión del secreto y las excepciones aplicables, los criterios de clasificación y los procesos para acceder a información pública o pedir la desclasificación. En esta resolución, por ejemplo, sigue habiendo referencias a categorías de clasificación de seguridad del decreto reglamentario previo a la reforma de 2015. La resolución tampoco es explícita respecto a que las excepciones por razones de seguridad nacional deberían interpretarse de modo restrictivo.

Tampoco hubo una respuesta judicial efectiva. En todos los casos e instancias, les jueces se limitaron a repetir de forma dogmática los argumentos de rechazo de las agencias demandadas y a convalidar su interpretación del secreto en absoluta deferencia al Poder Ejecutivo. Les jueces convalidaron el secreto de la información cuando se solicitó información a la AFI sobre fondos reservados, acuerdos de cooperación y escuchas. Se limitaron a afirmar que se trataba de información secreta solo por el hecho de estar en poder de la AFI. Esta interpretación contradice los estándares constitucionales y convencionales de acceso a la información pública. El Poder Ejecutivo tampoco aporta información relevante cuando se le solicita en instancias judiciales. La Cancillería nunca entregó información sobre los alegados "llamamientos a manifestaciones de violencia", ni especificó qué dependencia hizo ese análisis.

Uno de los jueces que recibió un pedido de información del CELS sobre criterios de clasificación, fondos reservados, escuchas y acuerdos de intercambio de información consideró que la Comisión Bicameral de Fiscalización era el único órgano habilitado legalmente a controlar a la AFI y que, por lo tanto, no tenía obligación de garantizar el acceso a la información de inteligencia. Se limitó a repetir la interpretación de la propia AFI sobre el régimen legal del secreto sin analizar el pedido ni ponderar los derechos en juego. No desarrolló ningún argumento que justificara dejar de lado el principio de máxima divulgación que establecen los estándares constitucionales y la Ley de Acceso a la Información. Tampoco contempló la posibilidad de tomar contacto con la información y, en función de eso, decidir si debía ser pública o accesible al menos para les solicitantes. Así, la vía judicial para reclamar quedó desna-

turalizada y se convalidó, al menos en esta instancia, que la AFI no tiene que rendir cuentas sobre temas centrales de su funcionamiento. Temas que, además, han estado en el corazón de las denuncias públicas por el uso ilegal de fondos, el tráfico de información y la filtración de escuchas.

En uno de los casos por las acreditaciones en la OMC que llegó a la Cámara de Apelaciones en lo Contencioso Administrativo Federal, la sala III rechazó la acción de hábeas data y la posibilidad de que el solicitante accediera a su información personal, por lo que su estado de incertidumbre y sospecha persiste. Habrá que esperar a conocer qué regla y estándar fijará la Corte Suprema. Hasta el momento, las vías judiciales han sido ineficaces para obtener una orden de acceso a la información personal y un control de la actividad de inteligencia estatal. En este sentido, que parte del aparato de vigilancia dependa ahora del máximo tribunal resiente su imparcialidad.

5. Romper la opacidad

Este conjunto de políticas y de prácticas es parte de una visión del Estado y del vínculo que este debe establecer con las personas. La expansión del aparato de seguridad y de inteligencia, así como la lógica del secreto justificado en la seguridad nacional tienen consecuencias bien concretas: restringe derechos y propone un Estado menos democrático.

Con estas reglas, el sistema institucional opera con amplios márgenes de arbitrariedad de los que es muy difícil defenderse, y en función de los cuales se desarrollan prácticas formales e informales que corren el límite de la vigilancia y de la inteligencia estatal. Al mismo tiempo, refuerzan a los grupos de poder estatales y privados asociados a estos temas que se van autonomizando de los poderes democráticos y reclaman más funciones y más recursos.

Las demandas de acceso a la información pública suelen funcionar con otros temas de la vida democrática, pero no con estos. En buena medida porque predomina un modo de hacer estatal cada vez más cercano a una perspectiva bélica y de construcción de enemigos públicos.

En un Estado democrático, el secreto no puede alcanzar a todas las actividades de inteligencia, ni de seguridad. Tampoco puede sostenerse de manera indefinida. En el marco de la política de memoria, verdad y justicia, fue importante la jurisprudencia de la Corte Suprema y de los tribunales para lograr la apertura de algunos archivos estatales y desandar, parcialmente, la lógica del secreto del terrorismo de Estado. Aun

con limitaciones, las vías judiciales como el hábeas data y el acceso a la información resultaron herramientas claves con las cuales el sistema judicial fijó estándares normativos y dio órdenes para desarticular en parte un Estado autoritario. Ahora, cuando nos enfrentamos a otros modos de autoritarismo y de endurecimiento de la respuesta estatal frente los conflictos y la disidencia, se precisan también mensajes y estándares de apertura. Es fundamental redefinir el programa político-ideológico sobre la intervención estatal que busca justificarse en la seguridad nacional y sus prácticas. Y también, repotenciar los espacios institucionales de control para que, al menos, se abran ciertas grietas que rompan la opacidad establecida.