Vigilancia y democracia

HISTORIAS EN DIEZ PAÍSES

INCLO

INTERNATIONAL NETWORK OF
CIVIL LIBERTIES ORGANIZATIONS

Vigilancia y democracia

HISTORIAS EN DIEZ PAÍSES

Foto de tapa: una cámara de seguridad colocada sobre el costado de un edificio observa desde arriba una intersección de calles en el centro de Manhattan, el 31 de julio de 2013 en Nueva York. Foto: Mark Lennihan/AP

ACERCA DE LA INCLO

La Red Internacional de Organizaciones por los Derechos Civiles (INCLO) está formada por un grupo de organizaciones nacionales e independientes de derechos humanos abocadas a promover los derechos y las libertades fundamentales mediante el apoyo y fortalecimiento mutuo del trabajo de las organizaciones miembros que trabajan en sus respectivos países, y mediante la colaboración a nivel bilateral y multilateral. Cada una de las organizaciones trabaja en la promoción y protección de derechos en su país, de manera independiente del gobierno, a través de la combinación de herramientas de litigio, campañas públicas, campañas legislativas y activismo. Los miembros de la INCLO que participaron en este informe son: la American Civil Liberties Union (ACLU); la Association for Civil Rights (ACRI) en Israel; el International Human Rights Group Agora (Agora) en Rusia; la Canadian Civil Liberties Association (CCLA); el Centro de Estudios Legales y Sociales (CELS) en Argentina; la Egyptian Initiative for Personal Rights (EIPR); la Human Rights Law Network (HRLN) en India; la Hungarian Civil Liberties Union (HCLU); el Irish Council for Civil Liberties (ICCL); la Kenya Human Rights Commission (KHRC), y el Legal Resources Centre (LRC) en Sudáfrica.

CELS
CENTRO DE ESTUDIOS LEGALES Y SOCIALES

LRC
Legal Resources Centre

ACLU
AMERICAN CIVIL LIBERTIES UNION

Irish Council for Civil Liberties

Egyptian Initiative for Personal Rights

HRLN
Human Rights Law Network

ASZ
HCLU HUNGARIAN CIVIL LIBERTIES UNION

AGORA

CANADIAN CIVIL LIBERTIES ASSOCIATION
ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Pamoja Tutetee Haki
KENYA HUMAN RIGHTS COMMISSION

índice

AGRADECIMIENTOS

Este informe ha sido un esfuerzo de colaboración de diez organizaciones de la INCLO. Los autores de los capítulos principales son:

ESTADOS UNIDOS
Larry Siems, escritor, y Brett Max Kaufman, abogado del Centro para la Democracia de la ACLU.

ISRAEL
Avner Pinchuk, abogado senior, ACRI.

RUSIA
Damir Gainutdinov, abogado, y Pavel Chikov, director ejecutivo, Agora.

CANADÁ
Brenda McPhail, directora, Proyecto de Privacidad, Tecnología y Vigilancia, CCLA.

ARGENTINA
Ignacio Bollier, miembro del equipo Seguridad Democrática y Violencia Institucional, Ximena Tordini, directora de Comunicación, y Paula Litvachky, directora del Área de Justicia y Seguridad, CELS.

INDIA
Saikat Datta, periodista independiente, y Eliza Relman, trabajadora paralegal, ACLU, con el apoyo de HRLN.

HUNGRÍA
Fanny Hidvegi, directora, Programa de Protección de Datos y Libertad de Información, y Rita Zagoni, directora de proyecto, Programa de Protección de Datos y Libertad de Información, HCLU.

IRLANDA
Stephen O'Hare, investigador principal y director del programa de políticas, ICCL.

KENIA
Andrew Songa, director de programa, Justicia Transformativa, KHRC.

SUDÁFRICA
Avani Singh, abogada, Unidad de Litigio Constitucional, y Michael Laws, investigador, Unidad de Litigio Constitucional, LRC.

El editor principal del informe fue Larry Siems. Lucila Santos (coordinadora de programas, INCLO), Brett Max Kaufman (abogado del Centro para la Democracia de la ACLU) y Steven Watt (abogado senior, Programa de Derechos Humanos de la ACLU) también contribuyeron a la edición.

Jameel Jaffer (subdirector de asuntos legales de la ACLU y director del Centro para la Democracia) revisó y editó el informe final.

Mariana Migueles y Carolina Marcucci estuvieron a cargo del diseño y maquetación del informe. Jazmín Tesone fue la editora de fotografía del informe. Hilary Burke fue la correctora del informe.

La INCLO agradece a la Open Society Foundations, a la Fundación Ford y a la Fundación Oak por el generoso apoyo que le brindan para su trabajo en este área.

introducción

Este informe ofrece una mirada al ras de algunas de las formas en que la vigilancia, en particular la vigilancia electrónica digital, está impactando en la vida de ciudadanos y residentes de diez países de África, América, Asia, Europa y Medio Oriente.

Las diez organizaciones que elaboraron el informe son miembros de la Red Internacional de Organizaciones por los Derechos Civiles (INCLO), y sus testimonios surgen de sus experiencias como litigantes y defensoras de los derechos civiles y humanos en sus respectivos países. Sus historias son distintas y reflejan realidades políticas locales y nacionales, pero tanto sus preocupaciones como las tecnologías de vigilancia en sí son transnacionales, están interconectadas y cada vez son más compartidas.

En Estados Unidos, un veterano del Cuerpo de Marines intenta abordar un avión y se entera de que está en una lista secreta de exclusión aérea basada, al parecer, en comunicaciones privadas e inofensivas de correo electrónico.

En Israel, agentes de seguridad del Estado convocan a activistas políticos pacíficos a “conversaciones de advertencia” que dejan en claro que sus vidas y comunicaciones están siendo monitoreadas.

En Rusia, y después de repetidas detenciones, un respetado defensor de los derechos humanos descubre que está en la sección “activistas de derechos humanos” de la base nacional de datos de vigilancia.

En Canadá, un juez descubre que los servicios de inteligencia de su país han eludido la ley y los tribunales para espiar a los ciudadanos canadienses.

En Argentina, la investigación del peor atentado terrorista sobre su suelo incluyó actividades ilegales de vigilancia e inteligencia para encubrir la verdad, dejando el caso irresuelto hasta el día de hoy.

En la India, un periodista que está a punto de revelar que el gobierno vigila a políticos de la oposición se convierte él mismo en blanco de la vigilancia.

En Hungría, los vecinos de un barrio multiétnico de Budapest se encuentran viviendo bajo la mirada de cámaras que pueden reconocer sus rostros.

En Irlanda, la oficina del defensor independiente del pueblo, encargada de la supervisión de la policía nacional del país, sospecha que está siendo vigilada por esa misma policía.

En Kenia, un imán radical es asesinado a tiros en la calle, y las investigaciones apuntan a escuadrones de la muerte autorizados por el Estado que operan sobre la base de información obtenida a través de un intercambio transnacional de inteligencia.

En Sudáfrica, el jefe de una organización ambiental de renombre internacional es objeto de una solicitud de “evaluaciones específicas de seguridad” que un gobierno extranjero envía al gobierno de Sudáfrica, y la organización sudafricana Legal Resources Centre (LRC) se entera de que ha sido vigilada ilegalmente por el Cuartel General de Comunicaciones del Gobierno (GCHQ) de Reino Unido.

Por separado, estas historias describen casos concretos en los que los gobiernos han utilizado la vigilancia para violar derechos civiles y humanos. Juntas, desafían la noción de que las operaciones digitales y tradicionales de vigilancia son intrusiones inofensivas, y de que en los países democráticos estas herramientas se utilizan con adecuada limitación y supervisión.

Esta publicación no es de ninguna manera un estudio exhaustivo de los programas de vigilancia tradicionales y digitales que operan en esos países. En cambio, las organizaciones miembros de la INCLO se han centrado en casos nacionales específicos en los que la vigilancia gubernamental abusiva ha salido a la luz, y donde las

organizaciones miembros y otras organizaciones de derechos civiles y humanos han intentado cuestionar o limitar esas prácticas. Si bien la naturaleza y finalidad de las operaciones difiere significativamente de un país a otro, estas organizaciones han enfrentado –y todavía enfrentan– un conjunto común de obstáculos en la búsqueda de hacer frente a los abusos; sobre todo, marcos legales pobremente definidos para delimitar los poderes de vigilancia y proteger los derechos individuales; falta de transparencia respecto de las leyes y prácticas relativas a la vigilancia; mecanismos débiles o insuficientes para supervisar a las agencias de inteligencia y sus operaciones de inteligencia; y alternativas limitadas para impulsar la transparencia cuando las herramientas de vigilancia de los servicios de inteligencia son usadas de modo indebido.

No se trata de desafíos novedosos. La vigilancia, piedra angular de los Estados opresores, ha planteado siempre un reto singular para las sociedades abiertas y democráticas; casi por definición, las tareas clandestinas de inteligencia deterioran las estructuras democráticas y violentan los compromisos fundamentales con el debido proceso, la transparencia y el control ciudadano. Pero hay algo nuevo en el alcance y la injerencia de la vigilancia, producto de los impresionantes avances tecnológicos que han abierto puertas completamente nuevas hacia las actividades y la vida privada de los ciudadanos. Esta expansión exponencial de los poderes de vigilancia electrónica digital ha traído consigo una preocupación generalizada de que la recolección de información por parte de los servicios de inteligencia puede estar dañando la propia democracia, debilitando los procesos y las instituciones democráticas en los países en los que suele dárselos por sentado, y obstaculizando o menoscabando el desarrollo de estructuras democráticas en países que acaban de salir de sistemas más autoritarios y de regímenes de vigilancia abusivos.

Nada dio cuenta de la magnitud de las nuevas tecnologías de vigilancia con más claridad que la valiosa colección de documentos clasificados de la Agencia Nacional de Seguridad de Estados Unidos (NSA) que Edward Snowden entregó a la prensa en mayo de 2013. Durante años, algunos miembros de la INCLO intentaron –mayormente en vano– descubrir de qué modo sus países estaban utilizando las nuevas tecnologías y poderes de vigilancia tanto a nivel nacional como internacional. Pero la libertad para hacer solicitudes de información y de litigar contra iniciativas específicas de vigilancia suelen ser obstaculizadas por el secreto y frustradas por vagas declaraciones gubernamentales respecto de la seguridad nacional. Ahora el mundo podía ver que varias agencias de inteligencia poseían la capacidad de monitorear las comunicaciones electrónicas procedentes de cualquier lugar de la tierra, y que esas agencias creían que tenían el derecho de recoger lo que el ex director de la NSA llamó “todo el pajar” de las comunicaciones globales, independientemente de los requerimientos nacionales e internacionales del debido proceso.

Pero los servicios de inteligencia de Estados Unidos y los de sus socios –conocidos como “Cinco Ojos”– en el Reino Unido, Canadá, Australia y Nueva Zelanda, no solo poseyeron y desplegaron esos nuevos y amplios poderes; también compartieron entre sí la información que reunían, a menudo eludiendo las leyes que limitan la vigilancia interna en sus propios países. Esos países también han colaborado con los servicios de inteligencia de otros países para formar coaliciones de vigilancia conocidas como “Nueve Ojos”, “14 Ojos”, “Rampart-A” (o “33 Ojos”) y “41 Ojos”, creando redes transnacionales para recopilar, almacenar y compartir información de inteligencia que no solo desafían las leyes nacionales sino también los conceptos de soberanía nacional, y distorsionan nociones fundamentales de la responsabilidad de los gobiernos para con la ciudadanía y el consentimiento de los gobernados.

Todas estas tendencias están ilustradas en el presente informe. En la mayoría de los países aquí retratados, los servicios nacionales de inteligencia han empleado nuevas herramientas de vigilancia sobre sus propias poblaciones. En Canadá, la India, Irlanda, Israel, Rusia y Estados Unidos, lo han hecho eludiendo restricciones legales destinadas a actuar como baluartes contra el espionaje interno. En Argentina, Hungría, Kenia y Sudáfrica –países que han luchado en los últimos años para construir instituciones democráticas más fuertes y transparentes– el espionaje ha replicado o perpetuado estructuras de inteligencia de regímenes opresores anteriores. En Canadá, Estados Unidos, Hungría, Kenia y Sudáfrica, la vigilancia incluye cierto grado de vigilancia transnacional e intercambio de inteligencia.

Desde mucho antes de las filtraciones de Snowden, los miembros de la INCLO han trabajado para exponer y desafiar los abusos descritos aquí; en algunos casos, las revelaciones de Snowden les han permitido litigar de manera más eficaz y comunicar con mayor claridad las formas en que los poderes de vigilancia están afectando la vida de los ciudadanos y residentes de sus países. Pero como se ve en el capítulo de Sudáfrica, esas revelaciones también ponen en evidencia la manera en que nuestras propias organizaciones miembros, muchas de ellas históricamente objeto de vigilancia en sus países de origen, se enfrentan a nuevas vulnerabilidades en la edad de vigilancia digital transnacional, como ocurrió cuando el LRC, nuestro miembro sudafricano, descubrió que sus comunicaciones habían sido interceptadas ilegalmente por el GCHQ de Reino Unido.

Para los miembros de la INCLO no hay demostración más clara de cómo, en este gran mundo nuevo de vigilancia digital transnacional, estamos realmente todos en el mismo barco.

vigilancia en diez países

los casos

Te estamos observando (y agregando a una lista)

1
ESTADOS UNIDOS

Una oficial de la TSA (Transportation Security Administration) revisa el pasaje, la tarjeta de embarque y el pasaporte de un pasajero como parte de los controles de seguridad del aeropuerto internacional John F. Kennedy de Nueva York el 30 de octubre de 2014.
Foto: Mark Lennihan/AP

ESTADOS UNIDOS

Te estamos observando (y agregando a una lista)

el caso

Para Ibraheim “Abe” Mashal, el viaje era otra demostración del éxito de Marine Corps Dog Training, el negocio que había lanzado al volver a Illinois después de servir como adiestrador de perros en la Marina estadounidense. Ahora tenía clientes no solo en el área de Chicago sino en otros 20 estados, y el 20 de abril de 2010 iba rumbo a Spokane, Washington, para conocer a una nueva clienta que estaba dispuesta a contratarlo desde tan lejos para que entrenara a sus perros.

Abe viajaba seguido en avión, y le pareció raro no poder hacer el check-in en línea. Llamó a la aerolínea. Le dijeron que podría recoger su tarjeta de embarque en el mostrador del aeropuerto Midway de Chicago antes de su vuelo.

En el aeropuerto le entregó su permiso de conducir a la encargada, quien lo observó, desapareció y regresó justo cuando Abe percibía que estaba montándose una escena a su alrededor. Al tiempo en que 30 agentes de la Administración de Seguridad en el Transporte (TSA) y de la Policía de Chicago se le venían encima, la representante de la aerolínea le informó que estaba en la “lista de exclusión aérea” (“No Fly List”) del gobierno estadounidense y que no podría subir a ese ni a ningún otro avión.

La lista de exclusión aérea del gobierno de los Estados Unidos es un subconjunto de la *Terrorist Screening Database* (TSDB): la lista de vigilancia maestra que el Centro de Detección de Terroristas del FBI ha compilado y administrado desde 2003. La lista se extrae de una base aún mayor: la *Terrorist Identities Datamart Environment* (TIDE), de la que un informe gubernamental clasificado de 2014 se jactaba por haber “superado el hito de un millón de personas”. El gobierno dice que incluye a alguien en la TSDB si tiene una “sospecha razonable” basada en “hechos articulables” de que la persona “es conocida o sospechada de, o ha estado involucrada en una conducta que constituya una preparación para, a favor de o relacionada con el terrorismo y las actividades terroristas”. Entre 500.000 y 800.000 personas estaban en la base de datos TIDE, y 10.000 de ellas en la lista de exclusión aérea en la mañana en la que Abe Mashal fue rodeado por un pelotón de policías y agentes federales en el mostrador de Southwest Airlines del aeropuerto Midway.

Mashal fue llevado a una habitación trasera. Un agente del FBI volvió a comprobar su identificación, salió de la habitación para hacer una llamada y luego comenzó a interrogarlo sobre el motivo de su viaje y su fe religiosa. Mashal respondió a las preguntas del agente y formuló algunas propias. ¿Cómo había terminado en esa lista? El agente dijo que no sabía –y aunque lo supiera, no podía decirlo. ¿Cómo podía Abe corregir el obvio malentendido? El agente le dijo que entrara al Programa TRIP del Departamento de Seguridad Nacional al llegar a casa.

Anunciado como “Un proceso integral de reparación al viajero” para quienes “tienen preguntas o buscan una solución respecto de las dificultades que experimentaron durante los controles de seguridad en los centros de transporte”, el Programa de Consultas y Resolución de Problemas del Departamento de Seguridad Nacional (DHS TRIP) no era exactamente un programa. En esencia, consistía en presentar un formulario de queja en línea y luego esperar una “carta de determinación”; una carta que, si llegaba, a menudo no determinaba nada. La carta no confirmaría ni negaría que el solicitante estuviera en la TSDB o la lista de exclusión aérea. No brindaba información acerca de por qué la persona estaba en esa lista. Ni siquiera aclaraba si, después de la revisión del gobierno, la persona podría volver a subir a un avión.

Mashal presentó su queja TRIP tan pronto como llegó a su casa desde el aeropuerto. Esa misma tarde, otros dos agentes del FBI lo visitaron e interrogaron en su sala de estar, indagando profundamente en sus creencias y prácticas religiosas, sus antecedentes familiares (su padre palestino había emigrado a los Estados Unidos y trabajó durante años como gerente de distribución de una compañía de dulces bien conocida, y su madre es católica e ítalo-americana),

así como la formación que había recibido en la Marina. Una vez más, Mashal respondió a todo, y el intercambio parecía ir bien; los agentes llamaron unos días más tarde para decirle que estaban enviando sus respuestas a Washington con una recomendación para que se lo eliminara de la lista de exclusión aérea.

Dos meses después, esos mismos agentes llamaron con "una gran noticia", y le pidieron a Mashal reunirse con ellos en un hotel del área de Chicago. Pero en una habitación del hotel le dieron en cambio "malas y buenas noticias". La mala, que Mashal estaba, en efecto, en la lista de exclusión aérea; la buena, que podrían sacarlo de allí si se convertía en uno de sus informantes pagos. Dieron a entender que tenían una amplia red de informantes como él en las comunidades musulmanas de todo el Medio Oeste. También dieron a entender por qué Mashal podría haber terminado en esa lista, sugiriendo que le había enviado un correo electrónico a alguien que estaba bajo vigilancia. Le preguntaron si alguna vez había enviado un correo a algún imán estadounidense para que lo asesorara sobre la crianza de niños en un hogar interreligioso. Mashal, cuya esposa es cristiana y con la que tenía tres hijos pequeños, lo había, en efecto, hecho.

"En ese momento, me harté", Mashal recordaría más tarde.

Les dije que no iba a contestar más preguntas sin un abogado presente. Nada de eso tenía sentido. ¿Era siquiera legal que entraran en mi correo electrónico? Si de hecho yo le había enviado un correo electrónico a alguien que estaba bajo vigilancia, ¿cómo podía saber que esa persona estaba bajo vigilancia? ¿Era legal que me chantajearan poniéndome en una lista de exclusión aérea, a cambio de convertirme en un informante? Una vez que les dije que quería un abogado presente, los agentes me dieron la mano y me dijeron que tenía que irme.

Mashal contactó a la American Civil Liberties Union (ACLU), que acababa de presentar una demanda en la corte federal del distrito en Oregon en nombre de un grupo de clientes que habían quedado atrapados en

Un manifestante sostiene una pancarta en una protesta contra los programas secretos de vigilancia PRISM, TEMPORA e INDECT y se solidariza con los informantes Edward Snowden, Bradley Manning y otros en Berlín el 27 de julio de 2013.
Foto: Reuters/Latinstock

Ibraheim 'Abe' Mashal en 1999. Foto: cortesía de Ibraheim Mashal

experiencias similares de exclusión aérea. Mashal se convirtió en uno de los 13 querellantes que demandaron al Departamento de Justicia, al FBI y al Centro de Detección de Terroristas en *Latif v. Holder* por violar sus derechos al debido proceso bajo la Constitución de los Estados Unidos. Seis de los demandantes se enteraron de que estaban en la lista de exclusión aérea mientras viajaban o vivían fuera del país, y habían quedado varados en el extranjero; siete, incluyendo a Mashal, se enteraron cuando intentaban abordar vuelos en sus ciudades y pueblos de origen en los Estados Unidos. Al igual que Mashal, otros tres eran veteranos de las fuerzas armadas de ese país. Y al igual que Mashal, varios de los otros demandantes denunciaron que agentes del FBI habían tratado de reclutarlos como informantes a cambio de retirar sus nombres de la lista de exclusión aérea. En la demanda, los querellantes solicitaban una orden judicial para que el gobierno los eliminara de la lista de exclusión aérea, o bien para proporcionarles un proceso justo para averiguar si estaban allí y por qué y, si así fuese, exigir su exclusión de esa lista negra.

En los meses previos a que el caso llegara a la corte, el FBI siguió presionando a Mashal, primero llamándolo a él directamente y luego interrogando a algunos de sus familiares y amigos. Uno de esos amigos, un empleado de otra agencia federal, llamó a Mashal después de la visita del FBI para transmitirle el mensaje de que no lo eliminarían de la lista de exclusión aérea a menos que retirara la demanda de la ACLU y reanudara su conversación con los agentes del FBI. Fue entonces cuando llegó la carta de determinación de TRIP. "Después de consultar con otras agencias federales, según el caso", se leía, "se ha determinado que no se autorizan cambios o correcciones a ninguno de los registros aplicables en este momento". El mensaje a Mashal era claro: todavía estaba en la lista de exclusión aérea.

En mayo de 2011, un juez federal de Portland, Oregon, desestimó la demanda de los 13 querellantes, diciendo que el tribunal carecía de jurisdicción en el caso. La ACLU apeló y el Tribunal de Apelaciones del Noveno Circuito revocó la decisión y ordenó que el tribunal de distrito lo examinara. En esa orden, la Corte de Apelaciones puso de relieve la naturaleza kafkiana del caso. "En los argumentos orales", señalaba "el gobierno no supo qué responder a lo que consideramos una pregunta relativamente sencilla: ¿qué deben hacer los ciudadanos de Estados Unidos y los residentes legales permanentes si creen que han sido incluidos erróneamente en la lista de exclusión aérea?".

En agosto de 2013, el tribunal del distrito dictaminó que los ciudadanos y residentes estadounidenses tienen la libertad constitucionalmente protegida de hacer viajes internacionales. Un año más tarde, en junio de 2014, el tribunal revocó el procedimiento del programa TRIP DHS como inconstitucional, señalando que el proceso fue "totalmente ineficaz" y que "sin la debida notificación u oportunidad de ser escuchado, un individuo podría ser condenado a permanecer de manera indefinida en la lista de exclusión aérea". Se ordenó al gobierno a decirle a los 13 demandantes si estaban o no en la lista y por qué, y a darles la oportunidad de impugnar ese estado de acuerdo con los derechos constitucionales del debido proceso.

Finalmente, el 10 de octubre 2014 –cuatro años y medio después de que a Abe Mashal se le anunciara que tenía prohibido realizar viajes aéreos–, la ACLU recibió una carta indicando que Mashal y seis de sus compañeros de demanda "no están en la lista de exclusión aérea a partir de la fecha de esta misiva". Mashal describió el impacto de la noticia unas horas más tarde:

Hace más de cuatro años se me negó el embarque en un aeropuerto en el que me rodearon agentes de la TSA y fui interrogado por el FBI. Ese día me fueron robadas muchas libertades que daba por sentadas. Nunca me dijeron por qué pasó lo que pasó, si yo estaba oficialmente en esa lista, o lo que podía hacer para conseguir de nuevo mis libertades. Ahora puedo reanudar el trabajo con clientes a los que no podía llegar manejando. Puedo asistir a bodas, graduaciones y funerales que estaban demasiado lejos como para llegar en coche o tren. Puedo viajar con mi familia a Hawaii, Jamaica o cualquier otro lugar de vacaciones. Hoy me enteré de que vuelvo a tener mis libertades.

Para seis de los otros demandantes, sin embargo, el padecimiento continúa. Desde entonces, han recibido "sumarios" no clasificados de algunas de las razones por las que fueron colocados en la lista de exclusión aérea, pero están lejos de recibir una explicación completa. El gobierno todavía no les ha dado una

audiencia significativa. Para estos hombres y mujeres, y para muchos más que han presentado quejas a través del proceso TRIP DHS, la saga continúa. Por esa razón, la ACLU ha cuestionado el nuevo proceso de resolución del gobierno por estar muy por debajo de los requisitos constitucionales al proceso justo.

Y decenas de nuevos nombres se añaden a la lista de exclusión aérea todos los días. La lista se duplicó en tamaño en 2012, de alrededor de 10.000 a 21.000; al año siguiente aumentó más del doble, llegando a casi 50.000; y en septiembre de 2014, contenía aproximadamente 64.000 nombres. Al igual que Abe Mashal, la mayoría de estos hombres y mujeres nunca sabrán que están en las listas del gobierno de los Estados Unidos hasta que intenten abordar lo que pensaban que sería un vuelo rutinario de negocios o hacia sus vacaciones.

el contexto

Las listas de vigilancia de los Estados Unidos, en continua expansión, son alimentadas por poderes de vigilancia con una capacidad y alcance impresionantes.

A principios de junio de 2013, el periódico *The Guardian* publicó la filtración de una orden secreta del Tribunal de Vigilancia de Inteligencia Extranjera (FISC) de los Estados Unidos, que revelaba que la Agencia de Seguridad Nacional (NSA) estaba recolectando los registros telefónicos de millones de estadounidenses de manera continua, diaria, dando al mundo un primer vistazo del programa de vigilancia nacional más extenso de la historia de los Estados Unidos. Apenas unos días después, *The Washington Post* informó sobre PRISM, un programa que permite a la NSA recibir datos directamente de compañías estadounidenses como Google y Facebook, incluyendo el contenido de correos electrónicos, mensajes de texto, chats de video, fotografías y más de los blancos extranjeros de la NSA y de cualquier persona en comunicación con dichos blancos. Solo después nos enteramos de que la fuente de esas impresionantes revelaciones era Edward Snowden, un empleado contratado por la NSA que había huido de los Estados Unidos con una valiosa colección de documentos que exponían el asombroso alcance del poder de vigilancia digital de la Agencia de Seguridad Nacional. Durante los días y semanas siguientes las revelaciones continuaron llegando, y no se han detenido.

A pesar de todo lo que hemos aprendido –y a pesar de los desafíos legales y las reformas legislativas– las infraestructuras físicas y jurídicas básicas del espionaje de la NSA permanecen intactas. El gobierno continúa sus redadas de vigilancia al amparo de dos autoridades legales: una ley de 2008 llamada Ley de Enmiendas FISA o FAA, y un decreto de la época de Ronald Reagan que permite a la NSA monitorear grandes flujos de tráfico de internet por medio del desvío de enormes cantidades del mismo, a menudo en bloque, para copiar y explorar desde sus propias bases de datos de comunicaciones. El gobierno lleva a cabo esta redada, en parte, a través de colaboraciones secretas con empresas de telecomunicaciones que operan en la "columna vertebral" de internet: la red global de cables de alta capacidad que transportan comunicaciones digitales alrededor del mundo. Cuenta también con agencias de inteligencia asociadas, tanto dentro como fuera de los países así llamados Cinco Ojos, para acceder a varios flujos masivos de datos de todo el mundo.

Dentro de los Estados Unidos, esta redada de vigilancia se lleva a cabo bajo la FAA, una ley que expandió el poder de la NSA para adquirir una gran cantidad de comunicaciones internacionales desde proveedores de internet y de telecomunicaciones dentro de los Estados Unidos. Según la interpretación que el gobierno da a la ley, prácticamente todas las comunicaciones internacionales –es decir, todas las comunicaciones que entran o salen del país– están dentro del alcance de la vigilancia de la NSA. Lo que es más, en virtud de esa interpretación de la ley, a la NSA se le permite retener las comunicaciones de los estadounidenses que la agencia intercepta "incidentalmente", lo que significa que cada vez que la NSA apunta a comunicaciones de extranjeros (ya sea de forma individual o en bloque), tiene derecho a copiar, revisar y guardar comunicaciones que involucren a estadounidenses, todo ello sin solicitar una orden judicial, como exige la Cuarta Enmienda de la Constitución de los Estados Unidos. (De hecho, en audiencias anteriores a la aprobación de la ley, funcionarios del gobierno admitieron que esta forma de evadir el requisito de la orden judicial de la Cuarta Enmienda era precisamente la intención de la nueva legislación).

Fuera de los Estados Unidos, la red del gobierno se sustenta en una orden ejecutiva sobre la que ningún tribunal tiene autoridad supervisora alguna y en la que la supervisión del Congreso es escasa. El gobierno argumenta que cuando un estatuto federal o la Constitución no regula su conducta de vigilancia, la única autoridad que lo hace es la orden ejecutiva. Es decir, en opinión del gobierno, la vigilancia llevada a cabo en el extranjero es más o menos un todos contra todos. La orden crea extensos permisos para llevar a cabo una vigilancia que no implique a estadounidenses y que no tenga lugar en suelo estadounidense, lo que le permite efectivamente al gobierno de los Estados Unidos monitorear a cualquier extranjero con el propósito de reunir "inteligencia exterior" –un término vagamente definido– incluyendo periodistas, defensores de los derechos humanos o abogados.

Los informes han indicado que el alcance de la vigilancia mundial realizada por la NSA en virtud de esta orden ejecutiva es enorme: incluye colecciones de listas de contactos y libretas de direcciones, el hackeo de administradores de sistemas, la instalación de malware y, quizás lo más sorprendente, el registro y la conservación de prácticamente todas las llamadas que tienen lugar en las redes telefónicas de varios países extranjeros. Además, los documentos han demostrado que la NSA ha utilizado esta orden sobre instituciones de la Unión Europea, empresas estatales de Brasil y líderes mundiales en la cumbre del G-20 de 2009. Más sorprendente aún, en virtud de lo que se denomina

> “Más sorprendente aún, en virtud de lo que se denomina como vigilancia, el gobierno cree que puede controlar la red troncal de comunicaciones en internet utilizando palabras clave; es decir, que puede buscar a través de los contenidos de los mensajes que atraviesan la red en todo el mundo.”

como vigilancia, el gobierno cree que puede controlar la red troncal de comunicaciones en internet utilizando palabras clave; es decir, que puede buscar a través de los contenidos de los mensajes que atraviesan la red en todo el mundo.

Todas las actividades propias de la NSA se ven agravadas por su cooperación con y dependencia de gobiernos extranjeros. En 2015, un fallo sin precedentes del Tribunal de Poderes de Investigación de Reino Unido determinó que el Cuartel General de Comunicaciones de Reino Unido (GCHQ) había actuado de forma ilícita durante dos años al acceder a millones de comunicaciones personales de la población después de que hubieran sido recogidas por la NSA, y el intercambio de información entre la NSA y el GCHQ parece ser rampante. Dicho intercambio supone la alimentación de información recolectada a través del GCHQ –incluyendo videos privados obtenidos gracias a un programa llamado “Nervio Óptico”– en XKeyScore, la base de datos de inteligencia de señales de la NSA. La NSA también recibe datos desde varios puntos de recolección de inteligencia de señales alrededor del mundo, incluyendo varios sitios del Reino Unido y Australia. Y la NSA comparte de manera rutinaria información de inteligencia, inclusive datos personales de estadounidenses y otros, con organismos de inteligencia extranjeros, incluyendo la unidad SIGINT de Israel.

La ACLU ha pasado gran parte de los últimos años litigando contra la redada de la NSA en los tribunales. Pocos días después de que *The Guardian* publicara la previamente secreta orden FISC, relativa a la colección masiva de registros telefónicos de la NSA, la ACLU presentó una demanda contra el programa de recolección masiva basándose en motivos legales y constitucionales. Mientras que la demanda sigue pendiente en el Tribunal de Apelaciones del Segundo Circuito de Estados Unidos, en mayo de 2015 el tribunal de apelaciones dictaminó que el uso por parte del gobierno de la Sección 215 de la Ley Patriótica para recolectar registros telefónicos “no tenía precedentes y era injustificado”. Esa victoria legal coincidió con la aprobación, en el Congreso, de la USA Freedom Act, una legislación que repudiaba los registros telefónicos del gobierno e hizo otros cambios –si bien menores– a otras autoridades que recogían información y a las normas de transparencia del gobierno.

La ACLU también ha demandado a la FAA en la corte, participando en varios casos penales en los que los acusados fueron notificados del uso de la ley en sus juicios, y en el caso civil de marzo de 2015 *Wikimedia v. NSA*, llevado adelante por nueve organizaciones de la sociedad civil. (Debido a varias doctrinas jurídicas formuladas por la Corte Suprema, las demandas de extranjeros o incluso estadounidenses contra la vigilancia posibilitada por la orden ejecutiva han sido muy difíciles de llevar adelante). La ACLU argumenta que la FAA viola la prohibición de la Cuarta Enmienda contra incautaciones y registros arbitrarios, prescindiendo de cualquier revisión judicial individualizada de las decisiones, y que viola la Primera Enmienda por entrometerse en los derechos de libre asociación y libertad de expresión. Esos casos están en curso, al igual que una acción legal similar, *Jewel v. NSA*, interpuesta por la organización *Electronic Frontier Foundation*.

Estas acciones legales enfrentan obstáculos enormes. En primer lugar, es difícil establecer una “legitimidad” para demandar –en esencia, el derecho legal de llegar a la corte– en los casos de vigilancia. Desde la decisión del Tribunal Supremo en un caso anterior de la ACLU, *Clapper v. Amnesty International EE.UU.*, presentado en 2008 contra la misma ley, los demandantes que se enfrentan a la vigilancia del gobierno deben demostrar que la recolección que este haya hecho de sus comunicaciones no se basa en especulaciones o suposiciones no comprobadas sobre las formas en las que funciona la vigilancia gubernamental; en esencia, los demandantes deben demostrar que han sido blanco de lo que, por definición, es un programa secreto. Afortunadamente, la gran cantidad de información adquirida a partir de las revelaciones de Snowden e indirectamente a través de, por ejemplo, revelaciones oficiales del gobierno, ponen la “legitimidad” de la vigilancia de la NSA bajo una luz muy diferente que en la demanda original de *Amnesty*, y casos como los de *Wikimedia* podrían finalmente tener éxito en conseguir que las puertas de los tribunales se abran para demandar a la NSA.

Pero incluso si consiguen el derecho a demandar, los querellantes se enfrentarán a un reto formidable en el juicio, donde el privilegio del “secreto de Estado”

invocado por el gobierno es a menudo fatal en los casos de vigilancia. La doctrina del "secreto de Estado" permite efectivamente que el gobierno ponga fin a un litigio al afirmar que continuar con la demanda hace peligrar secretos de seguridad nacional.

Por último, es fundamental tener en cuenta que el propio Edward Snowden –el informante cuyo valor impulsó el renovado debate global sobre la vigilancia gubernamental tanto en Estados Unidos como en otros países, y cuyas acciones han conducido directamente a reformas de vigilancia dentro y fuera del país– no puede regresar a los Estados Unidos. El gobierno ha acusado a Snowden de violaciones a la Ley de Espionaje, uno de los delitos más graves de la ley estadounidense. Durante cualquier juicio por estos crímenes, a Snowden se le impediría, según la ley estadounidense, organizar una defensa basada en la Primera Enmienda que pusiese de relieve su intención de informar al público estadounidense sobre las actividades de la NSA, que explicara la inocuidad de las filtraciones para los intereses de los Estados Unidos, y los beneficios que esas filtraciones han tenido en el debate público y que el propio gobierno reconoce que nunca hubiera sido posible sin él. Si bien Snowden sigue llevando una vida digna en el exilio en Rusia y participa del debate sobre la vigilancia global, es hora de que el gobierno de los Estados Unidos encuentre la manera de devolverlo a casa.

conclusión

Un gobierno tiene oídos en todas partes. Oye la conversación privada de un hombre y pone al hombre en una lista. Hay puertas que se cierran para ese hombre por estar en esa lista. Cuando se topa con una de esas puertas y descubre que está en una lista del gobierno, no puede descubrir por qué. Cuando trata de eliminar su nombre de la lista, se le dice que la única manera de hacerlo es convirtiéndose en otro par de oídos del gobierno; oídos que escuchen conversaciones privadas y pongan a otras personas en las listas.

En muchos sentidos, la historia de Abe Mashal se lee como una parábola de la seguridad convencional del Estado adaptada a la era digital: si las revelaciones de Edward Snowden han arrojado luz sobre el impresionante alcance de los poderes de vigilancia digital de los Estados Unidos, las experiencias de los demandantes de la ACLU incluidos en la lista de exclusión aérea señalan de qué manera esa vigilancia penetra profundamente en la vida privada de los ciudadanos y residentes de los Estados Unidos. Las dificultades kafkianas que han atravesado para intentar salir de esa lista ponen de relieve la naturaleza de autoprotección y autoperpetuación de los sistemas secretos y ubicuos de vigilancia. Abe Mashal y los otros demandantes ganaron una importante victoria al desafiar la lista de exclusión aérea. Pero cuando se trata de listas impulsadas por sistemas de vigilancia en Estados Unidos, es apenas un comienzo.

Un vistazo a la vigilancia en los Estados Unidos

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
Sí.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
Sí.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
Sí.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Reducido en algunos aspectos y aumentado en otros.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
Sí.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia del gobierno, ¿dicha legislación estrecharía o ampliaría el poder de vigilancia gubernamental?
Lo estrecharía.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Sí.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional gubernamental han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
Sí.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos, o no ha modificado su percepción sobre las agencias de inteligencia?
Menos.

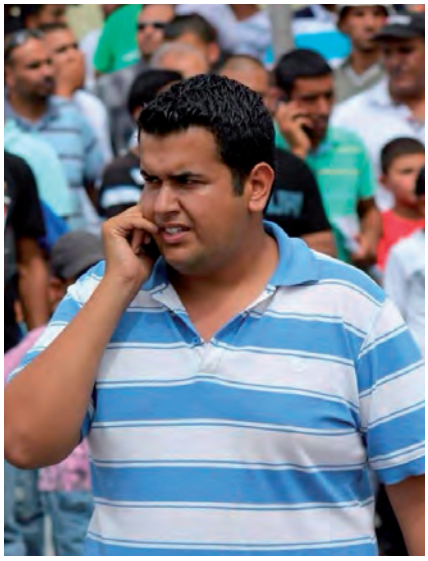
Conversaciones de advertencia: ¿una estrategia intimidatoria contra el activismo?

2
ISRAEL

Manifestantes gritan consignas durante una protesta contra el Plan Prawer-Begin en Haifa el 30 de noviembre de 2013.
Foto: Mareike Lauken/Active Stills

ISRAEL

Conversaciones de advertencia: ¿una estrategia intimidatoria contra el activismo?



Rateb Abu-Krinat durante una de las protestas contra el Plan Prawer en 2013.
Foto: Eslam Alsana

el caso

Como trabajador social de la ONG Foro de Coexistencia del Néguev para la Igualdad Civil, Rateb Abu-Krinat promovía activamente los derechos civiles y la igualdad de los ciudadanos árabe-beduinos de la región del Néguev, al sur de Israel. Entre 2012 y 2013, su activismo incluyó la participación en protestas públicas contra el "Plan Prawer", una controvertida iniciativa del gobierno para regular las estructuras de tenencia de tierra de los beduinos del Néguev.

En junio de 2012, Rateb recibió una llamada solicitando se reportara a la estación de policía local como parte de una investigación. Rateb, ciudadano árabe-israelí, cumplió voluntariamente. Cuando llegó, fue sometido a un registro corporal humillante y luego trasladado a una sala y presentado a un hombre que se identificó como "Jamil" del Shin Bet, el Servicio General de Seguridad (GSS). Insistiendo en que se trataba solo de una "conversación normal", Jamil procedió a interrogar a Rateb durante dos horas y media sobre sus estudios y su trabajo, y lo presionó para que le brindara detalles acerca de sus familiares y amigos. Hacia el final de la conversación, Jamil le preguntó por su opinión sobre el Plan Prawer. El funcionario del GSS concluyó la sesión dejándole claro a Rateb que ya sabía mucho sobre su vida y sus actividades y que si bien actualmente estaba "incontaminado" debía cuidarse de no participar en actividades que pudieran perjudicar la seguridad del Estado. Jamil agregó que debería "rezar" para que no hubiera necesidad de que volvieran a encontrarse.

Ocho meses después, Rateb recibió otra citación para un seguimiento de la reunión en la comisaría. Esta vez recurrió a la Association for Civil Rights in Israel (ACRI).

Durante varios años, la ACRI había estado reuniendo testimonios de activistas de la sociedad civil que habían sido convocados para "conversaciones de advertencia" similares con agentes del GSS. Un empleado de la ACRI que trabajaba para defender los derechos de los residentes de Jerusalén era uno de ellos. Un activista involucrado en actividades políticas judeo-árabes en el norte de Israel también había sido llamado, interrogado

y advertido, al igual que activistas que participaban en protestas contra la ocupación, la construcción de la barrera de seguridad y el bloqueo de la Franja de Gaza.

Los testimonios que recogió la ACRI seguían un patrón. Los convocados a estas "conversaciones" eran todos activistas que participaban en la promoción de políticas que desafiaban el consenso público. Las conversaciones, que no formaban parte de investigaciones formales de delitos específicos, tenían el tenor de interrogatorios, con agentes del GSS cuestionando a activistas sobre sus vidas personales y actividades políticas. A los activistas se les pedía con frecuencia que suministraran nombres y números de teléfono de familiares o amigos y, en ocasiones, se les preguntó por detalles de su situación financiera. En algunos casos, los agentes del GSS dijeron explícitamente a los activistas que, aúnque no fuesen sospechosos de violar la ley "por ahora", debían tener cuidado de no hacerlo en el futuro; otras veces los agentes hacían afirmaciones vagas, sin acusaciones concretas, de que los activistas habían estado implicados en alteraciones del orden. A veces, las advertencias y amenazas eran directas: a uno de los "sospechosos" se le decía que "debía ser consciente de que pondríamos en marcha un caso en tu contra", pero no se le daba ninguna explicación de qué supuesta conducta ilegal podría precipitar un caso así.

Lo más inquietante: en muchas de las "conversaciones de advertencia" se dejaba bien en claro a los convocados que el GSS ya sabía mucho acerca de ellos y había estado monitoreando sus actividades. Uno de los activistas contó cómo:

[El agente] comenzó a traer a colación todo tipo de información personal sobre mi vida que incluso personas cercanas a mí no sabían […] Era como si me estuviera diciendo "sabemos quién eres, sabemos lo que haces".[1]

Con el aumento de los informes sobre estas "conversaciones de advertencia", la ACRI se contactó varias veces con el Servicio General de Seguridad y el Procurador General para exigir que pusieran fin de inmediato a esa práctica. Una de las pocas respuestas recibidas en una carta de la Oficina del Procurador General, firmada por un asesor de este, solo intensificó la preocupación.[2]

La carta explicaba que el activista en cuestión había sido convocado a una conversación porque el GSS poseía información relativa a su participación en una manifestación violenta en el norte del país, a pesar de que los agentes del GSS no habían planteado tal alegación durante su conversación con él. En cuanto a la base jurídica para convocar a los ciudadanos a "conversaciones de advertencia", la carta hacía referencia a la Ley de Servicio General de Seguridad (GSSA), que autoriza a la agencia a impedir o prevenir actividades ilegales cuyo objetivo es dañar la seguridad del Estado, el régimen democrático o sus instituciones. Esto a pesar del hecho de que, según la ley israelí, las actividades que se consideran alteraciones públicas pertenecen al ámbito de la policía israelí, y no el Servicio General de Seguridad.

Y no solo el supuesto fundamento de las "conversaciones de advertencia" era débil; la carta también sugería, como los agentes del GSS habían insinuado durante las "conversaciones", que estas estaban vinculadas a pruebas reunidas a través de otros poderes de inteligencia. Según la carta, cuando los ciudadanos israelíes son objeto de "conversaciones de advertencia", generalmente es después de la recolección de información de inteligencia. Cuando se recibe dicha información, tal como se explica en la carta del Procurador General, se examina su credibilidad y se hace un intento para complementarla tanto como sea posible con "herramientas de recolección" de inteligencia adicionales; herramientas que, a veces, pueden incluir una reunión indagatoria, es decir, una "conversación de advertencia".

Cuando Rateb alertó a la ACRI de que había recibido una segunda convocatoria para presentarse a la estación de policía para ser interrogado, la organización envió una carta urgente al Procurador General y al Shin Bet exigiendo que se rescindiera la citación. A la mañana siguiente –muy rápido– la ACRI recibió

> “El funcionario del GSS concluyó la sesión dejándole claro a Rateb que ya sabía mucho sobre su vida y sus actividades y que si bien actualmente estaba ‘incontaminado’ debía cuidarse de no participar en actividades que pudieran perjudicar la seguridad del Estado.”

una respuesta del departamento jurídico del Servicio General de Seguridad aclarando que Rateb Abu-Krinat no estaba obligado a asistir a la reunión.

Pero solicitudes adicionales de la ACRI para que el GSS y el Procurador General explicaran y delinearan los límites de la supuesta autoridad del GSS para llevar a cabo esas “conversaciones de advertencia” no tuvieron respuesta. Así, en julio de 2013, la ACRI presentó una petición legal contra el Servicio General de Seguridad a la Corte Suprema de Israel.

el contexto

La vigilancia digital es un fenómeno generalizado en Israel con poderes distribuidos entre las cuatro principales entidades de recolección de información: Unidad 8200, que es la Unidad de Inteligencia de Señales (SIGINT) de las Fuerzas de Defensa de Israel; el Servicio General de Seguridad; el Mossad; y la policía israelí.

Como servicio de seguridad interna de Israel, el Servicio General de Seguridad tiene acceso indiscriminado a todas las comunicaciones en Israel. Bajo el GSSA, el GSS está autorizado “a recibir y recoger información”[3] con el fin de llevar a cabo sus misiones, incluyendo “proteger la seguridad del Estado y el orden y las instituciones del régimen democrático frente a las amenazas de terrorismo, sabotaje, subversión, espionaje y la revelación de secretos de Estado”.[4] Para el GSS, esto incluye la facultad de intervenir teléfonos y supervisar las actividades en internet de los ciudadanos israelíes sin supervisión judicial. Para utilizar estas herramientas, es suficiente simplemente recibir la aprobación del primer ministro.

Para recoger los metadatos de las comunicaciones, el GSS no necesita ni siquiera obtener la aprobación del primer ministro. El permiso está dado por el Jefe de Servicio.[5] Apéndices secretos –que están asociados a las franquicias y licencias que el Estado extiende a las empresas de comunicaciones (de acuerdo con la Ley de Comunicaciones)[6], y que incluyen especificaciones sobre la infraestructura técnica (equipos e instalaciones ubicadas en las instalaciones del licenciatario)– conceden a las agencias de inteligencia israelíes acceso directo y completo a sus bases de datos, lo que permite al GSS monitorear todas las comunicaciones y recoger todos los metadatos directamente, sin ninguna intervención o conocimiento específico de las empresas.

En 2007, como parte del litigio de la Ley de Libertad de la Información, el Ministerio de Comunicación se negó a revelar los apéndices secretos adjuntos a las franquicias y licencias. Sin embargo, en la investigación de la corte, el ministro confirmó que el GSS posee “la llave” a las bases de datos, lo que quiere decir que las empresas proveedoras de servicios de internet ni siquiera saben cómo y cuándo el GSS accede a sus bases de datos.

La población israelí ignora el alcance de la vigilancia que se lleva a cabo bajo esta figura. El GSS está totalmente exento de la Ley de Libertad de Información, por lo que

Activistas palestinos e internacionales reaccionan a las granadas de aturdimiento lanzadas por fuerzas israelíes durante una protesta en el "Día de la ira" contra el Plan Prawer-Begin frente al asentamiento israelí Bet El, Al Jalazun, Cisjordania, el 30 de noviembre de 2013.
Foto: Ryan Rodrick Beiler/Active Stills

la población no tiene medios para averiguar con qué frecuencia y en qué circunstancias se utiliza ese poder. Mientras que el primer ministro está sujeto a solicitudes de información bajo la Ley de Libertad de Información (conocidas como FOIA), la exención del GSS significa que incluso algo tan general como el número de escuchas telefónicas que el primer ministro aprueba cada año sigue siendo un secreto. Cuando este fue presionado directamente sobre la cuestión, insistió en que la información no estaba en su posesión "física", porque devuelve todas las solicitudes y aprobaciones de escuchas telefónicas al GSS. Cuando la ACRI presentó una petición FOIA buscando estadísticas en la oficina del primer ministro sobre el número de permisos de vigilancia que había aprobado, el Tribunal de Distrito y luego el Tribunal Supremo rechazaron la petición, aceptando el argumento del Estado de que los datos relevantes están enteramente en manos del Servicio General de Seguridad. Esta posición distorsiona el alcance del secreto profesional del Servicio General de Seguridad y pone en entredicho la eficacia y rigurosidad con la que el primer ministro supervisa las solicitudes de escuchas telefónicas del GSS.

En 2012, Avi Dichter, jefe del Servicio General de Seguridad entre 2000 y 2005, reconoció que se las arregló para que buena parte de la sección principal que rige al SIGINT pasara desapercibida gracias a que en ese momento la gente no conocía la importancia de los metadatos de las comunicaciones ni lo reveladores que pueden ser. Dichter también insistió en que el GSS "pagó" por aquellos fantásticos poderes legales al aceptar la "transparencia" de sus actividades de vigilancia digital. Pero esa transparencia se limitaba a informes secretos y limitados para ciertos ministros de gobierno, un comité cerrado del Knesset, y el fiscal general; informes tan ocultos del público como los propios programas de vigilancia y que, Dichter admitió, eran de poco interés para los supervisores del gobierno. En sus palabras:

No puedo recordar un solo caso como jefe del Servicio General de Seguridad […] en que una autoridad legal o un funcionario de gobierno nos hubiera llamado para decirnos que no habíamos cumplido los plazos para proveer actualizaciones escritas u orales. En todos los casos, sin una sola excepción, siempre fuimos nosotros quienes nos arremangamos y contactamos al Procurador General o al comité ministerial para decirles: "Amigos, se les olvidó que estamos obligados a informarles". [7]

Los propósitos que facultan al Servicio General de Seguridad para extraer metadatos de comunicaciones están definidos a grandes rasgos y vagamente. Las escuchas telefónicas están condicionadas, al menos

La policía israelí avanza mientras jóvenes beduinos lanzan piedras durante una protesta contra el Plan Prawer-Begin en la carretera 31 cerca de Hura, Israel, el 30 de noviembre de 2013. Foto: Oren Ziv/Active Stills

en el texto de la ley, al hecho de ser "necesarias para las necesidades de seguridad del Estado", y antes de conceder al GSS permiso para realizar escuchas, el primer ministro debe sopesar esas necesidades contra el derecho a la privacidad. Por el contrario, una autorización para recoger o usar metadatos es emitida por el jefe del Servicio General de Seguridad una vez que él o ella esté "convencido de que esa autorización fue requerida por el Servicio para cumplir con sus funciones en virtud de [la GSSA]".[8]

Se trata del mismo criterio establecido por el GSS para justificar su práctica de convocar a activistas a "conversaciones de advertencia". Pero mientras que la recolección de metadatos y la mayoría de las otras actividades de vigilancia del Servicio General de Seguridad funcionan de modo subrepticio, las "conversaciones de advertencia" se realizan en el ámbito público, ofreciendo un atisbo singular de los tipos de actividades en los que el GSS se involucra en el rubro de la seguridad nacional. Al peticionar en contra de las "conversaciones de advertencia", la ACRI ha tratado de sacar a la luz la interpretación que el GSS hace de sus funciones y facultades.

La GSSA define el papel del GSS de una manera extremadamente amplia, afirmando que "el servicio será responsable de la protección de la seguridad del Estado y de las instituciones del régimen democrático contra las amenazas".[9] Estas amenazas incluyen no solo el terrorismo o el espionaje, sino también la "subversión" y las amenazas a "otros intereses del Estado vitales para la seguridad del Estado nacional, según lo prescrito por el Gobierno".[10] La petición de la ACRI desafió la amplia interpretación de los términos legales del Servicio General de Seguridad, especialmente en relación a las "actividades subversivas".

En una respuesta de 2007 a una consulta de la ACRI, Yuval Diskin, jefe del Servicio General de Seguridad entre 2005 y 2011, afirmó que "la posición del GSS es que la 'subversión' también puede incluir el propósito de alterar los valores fundamentales del Estado anulando su carácter democrático o judío".[11] Una publicación del GSS de 2012 llamada "Derecha e izquierda radical" indica que el servicio no solo está reuniendo información sobre dicha presunta subversión, sino que ha actuado en virtud de esa información, señalando que "la información de Shin Bet, remitida a las autoridades estatales competentes, ha contribuido a frenar actos de deslegitimación de Israel".[12]

En su respuesta a la petición de ACRI contra las "conversaciones de advertencia", el Estado afirmó por primera vez que, tras revisar en 2009 la definición de "subversión", las actividades o protestas contra el

> “En muchas de las ‘conversaciones de advertencia’ se dejaba bien en claro a los convocados que el GSS ya sabía mucho acerca de ellos y había estado monitoreando sus actividades.”

“carácter judío del Estado” ya no eran consideradas “actividades subversivas” por el Servicio General de Seguridad. El hecho de que una decisión como esa se hubiese tomado cuatro años antes, en secreto, y solo fuese revelada en respuesta a la petición de la ACRI, fue preocupante en sí mismo. Sin embargo, más preocupante fue que el Estado supiera que el GSS, no obstante, seguía monitoreando manifestaciones por casos de subversión. De acuerdo con el Estado:

Por regla general, en una democracia, las protestas (que excedan los límites de la ley) son asunto de la policía y no una cuestión del Servicio General de Seguridad. Sin embargo, el Servicio General de Seguridad debe actuar para desbaratar una protesta organizada por razones ideológicas de motivación subversiva y nacionalista, y bajo circunstancias en las que la naturaleza de la protesta suponga un riesgo para la seguridad del Estado.[13]

En su respuesta, el Estado no explicó cómo se distingue una protesta aceptable de una manifestación “organizada por razones ideológicas de motivación subversiva y nacionalista” que supone “un riesgo para la seguridad del Estado”.

¿Por qué algunas manifestaciones, como las realizadas en nombre de la comunidad beduina y contra el Plan Prawer en las que Rateb participó, son consideradas asuntos de seguridad de Estado y quedan sujetas al escrutinio del GSS, mientras que otras protestas, como las organizadas por judíos ultraortodoxos contra el reclutamiento militar, no son tratadas como tales, incluso cuando existe temor de que se produzcan disturbios públicos? ¿En qué medida los problemas que son de vital importancia para los árabes israelíes, por ejemplo, tienen más probabilidades de ser clasificados y tratados como amenazas “nacionalistas” y “subversivas” a la seguridad del Estado, o como actividades que sirven para “deslegitimar” a Israel, actividades que el Servicio General de Seguridad tiene autoridad para controlar y frustrar?

En respuesta a la acción de la ACRI respecto de las “conversaciones de advertencia”, el Estado afirmó que frustrar la “deslegitimación” no fue la base legal para convocar a los demandantes nombrados en la petición. Sin embargo, como hemos mencionado antes, las “conversaciones de advertencia” son solo una de las muchas “herramientas de recolección” de inteligencia del Estado (un término que cubre una amplia gama de actividades de vigilancia). Por otra parte, el gobierno israelí no hace distinciones entre un llamamiento a deslegitimar la ocupación de los territorios ocupados y un llamamiento a deslegitimar la existencia misma de Israel como un Estado, haciendo que un gran espectro de actividades anti-ocupación y de protestas “anti-israelíes” sean vulnerables al (mucho más penetrante) seguimiento y vigilancia del Servicio General de Seguridad.

La petición de la ACRI argumenta que “invitar” a activistas políticos a “conversaciones de advertencia” excede la autoridad legal del Servicio General de Seguridad, y se opone a la manera excesiva en que el GSS entiende su autoridad y el amplio espectro de actividades políticas que considera de su competencia. En la petición se afirma que las “conversaciones de advertencia” violan derechos fundamentales constitucionales –en primer lugar, a la libertad de expresión y de protesta, y también los derechos a la dignidad, la privacidad, la libertad, la igualdad y el debido proceso–, y que estas “conversaciones” tienen un efecto negativo sobre la actividad legal de la protesta. Se alega, además, que la actividad de la protesta, en general, pertenece al ámbito propiamente de la policía que, a diferencia del GSS, está sujeta a la supervisión pública y el control judicial, más allá de que estos poderes de control sean insuficientes en la práctica.

Después de una audiencia pública sobre la petición de la ACRI –una audiencia en la que uno de los jueces señaló que los criterios con los que el Servicio General de Seguridad determina si las manifestaciones y otras acciones de protesta constituyen una amenaza a la seguridad podrían aplicarse a casi todas las protestas o actividades políticas de los ciudadanos árabes de Israel– los jueces anunciaron que continuarían la audiencia en privado solo con los representantes legales del Servicio General de Seguridad. Posteriormente el tribunal emitió un fallo confidencial en el que, de acuerdo con su explicación en la audiencia pública, los jueces pidieron más aclaraciones. También anunciaron que cuando recibieran dichas aclaraciones del GSS, llegarían a una decisión final y decidirían en qué medida podrían publicar una resolución pública

y no clasificada. Una vez que el Servicio General de Seguridad envíe sus explicaciones clasificadas, el veredicto final podría tomar hasta seis meses.

conclusión

Convocar a activistas políticos pacíficos a conversaciones amistosas alrededor de una taza de té con agentes de seguridad encubiertos difícilmente sea un sello distintivo de las sociedades democráticas, especialmente cuando esas conversaciones tienen el tenor de interrogatorios e incluyen preguntas que sondean en actividades y asociaciones políticas y personales, y cuando los agentes pertenecen a un servicio de seguridad que ejerce un enorme poder de vigilancia.

El caso de Abu-Rateb Krinat y sus compañeros activistas revela de qué manera, en manos de una agencia de seguridad que opera con poca supervisión o transparencia, los excesivos poderes de vigilancia pueden combinarse con tácticas de intimidación y volverse contra los disidentes. Como resultado, la vigilancia puede ser utilizada para acosar activistas y desalentar protestas pacíficas, e incluso actividades políticas legítimas y protegidas constitucionalmente.

Las "conversaciones de advertencia" son solo la punta visible de un aparato de recolección masiva de información que se maneja con una muy limitada supervisión de manera que en sí mismo puede suponer una amenaza para los derechos fundamentales de los ciudadanos israelíes.

Hay mucho en juego en el actual litigio. Como la ACRI argumentó ante la Corte Suprema:

Los límites de la autoridad del Servicio General de Seguridad para hacer seguimientos de la actividad política tienen implicaciones respecto del alcance del uso de herramientas de "recolección" de información, específicamente, recolección y análisis de datos de comunicaciones y escuchas telefónicas. Estas actividades no están sometidas a escrutinio judicial o público. En estas circunstancias, es de gran importancia un fallo aclaratorio que delimite las fronteras de la ley con respecto a las actividades políticas del GSS. Podemos suponer que, en muchos de los casos en los que se invita a los activistas a las "conversaciones de advertencia", se están llevando a cabo otras actividades desconocidas de "recolección" [de inteligencia]. Es necesario un fallo que establezca la interpretación de la autoridad del GSS para evitar la utilización excesiva y perjudicial de estas herramientas; una utilización que, por su naturaleza, nunca será sometida a un escrutinio directo.

notas

-

1. Petición de la ACRI (HCJ 5277/13 ACRI v. GSS), par. 23. Disponible, en hebreo, en: http://www.acri.org.il/he/wp-content/uploads/2013/07/hit5277.pdf [28/10/2016].
2. Carta enviada a la ACRI por Raz Nizry, entonces asesor principal de la Oficina del Procurador General, fechada el 9 de junio de 2010. La carta, en hebreo, está disponible en: http://www.acri.org.il/he/wp-content/uploads/2011/11/Nizri090610.pdf [28/10/2016].
3. GSSA, Sección 8(a)(1). Disponible en: http://www.knesset.gov.il/review/data/eng/law/kns15_GSS_eng.pdf [28/10/2016].
4. GSSA, Sección 7(a).
5. GSSA, Sección 11.
6. Ley de Comunicaciones (Telecomunicaciones y Radiotransmisión) 5742-1982, Sección 13(b). Disponible en: http://www.moc.gov.il/sip_storage/FILES/9/3889.pdf [28/10/2016].
7. Avi Dichter hablando en el panel "El décimo aniversario del Acta SGG", YouTube (en hebreo). Disponible en: http://youtu.be/BZ1sZqa0BR0?t=18m43s [28/10/2016].
8. GSSA, Sección 11(c) [Ver Sección 11(c) de GSSA, en nota al pie nº 6].
9. *Ibíd*
10. GSSA, Secciones 7-8.
11. "The Shin Bet - Guardian of Democracy?", *Haaretz* (12 de febrero, 2016). Disponible en: http://www.haaretz.com/print-edition/features/the-shin-bet-guardian-of-democracy-1.250879 [28/10/2016].
12. Servicio General de Seguridad. "Resumen anual 2012: datos y tendencias en el terrorismo y medidas de prevención", sitio web del GSS, p. 13. Disponible, en hebreo, en: https://www.shabak.gov.il/SiteCollectionImages/Hebrew/TerrorInfo/Years/2012-he.pdf [28/10/2016].
13. Sección 22 de la respuesta del Estado a la petición de la ACRI (HCJ 5277/13 ACRI v. GSS), 22 de febrero, 2014. Disponible, en hebreo, en: http://www.acri.org.il/he/wp-content/uploads/2014/03/hit5277meshivim0214.pdf [28/10/2016].

Un vistazo a la vigilancia en Israel

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
Sí.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Ninguna de las dos.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
Sí.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Las ampliaría (no a la vigilancia de inteligencia sino a la vigilancia policial y de otros organismos encargados de hacer cumplir la ley).

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
Sí.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
No ha modificado su percepción.

Estado espía: la “base de datos de vigilancia” y otras herramientas

3
RUSIA

Sergey Shimovolos, defensor de los derechos humanos de Nizhni Nóvgorod. Foto: cortesía de Sergey Shimovolos

RUSIA

Estado espía: la "base de datos de vigilancia" y otras herramientas

el caso

El viaje en tren de 600 kilómetros de Nizhni Nóvgorod a Samara es corto para los estándares rusos, y debería haber sido rutinario para Sergey Shimovolos, director de la Unión de Derechos Humanos de Nizhni Nóvgorod, una asociación no gubernamental que nuclea a diez organizaciones de derechos humanos y ambientales de la región. Pero tan pronto como Shimovolos subió al tren el 13 de mayo de 2007, comenzaron sus problemas.

Tres policías le cayeron encima, demandando ver sus documentos de identidad y conocer el motivo de su viaje. Durante el viaje de 15 horas fue interrogado dos veces más por agentes de policía que controlaron sus documentos, le preguntaron sobre el propósito de su viaje y quisieron saber si tenía conocidos en Samara. Incluso le ordenaron abandonar el tren y seguir a los agentes a la estación de policía, pero él se negó a acatar, y la policía no pudo dar con ningún fundamento legal para detenerlo.

Shimovolos tenía una idea de por qué le estaba ocurriendo eso. Viajaba a Samara para investigar la detención de varios activistas que habían participado en recientes protestas contra el Kremlin, y lo hacía cuatro días antes de que el presidente ruso, Vladimir Putin, fuese el anfitrión de la 19ª Cumbre UE-Rusia del 17 y 18 de mayo de 2007 en el complejo Volzhskiy Utyos de Samara. Entre los invitados estaría la canciller alemana Angela Merkel, que en ese momento ocupaba la presidencia del Consejo de la Unión Europea, y José Manuel Barroso, presidente de la Comisión Europea. En la agenda figuraban negociaciones para el nuevo Acuerdo de Colaboración y Cooperación UE-Rusia, cooperación energética, el despliegue de componentes de un sistema de defensa antimisiles de Estados Unidos en Polonia y la República Checa y la adhesión de Rusia a la Organización Mundial del Comercio. En la agenda también figuraba el historial de Rusia con los derechos humanos, que en 2007 incluyó la preocupación internacional sobre el manejo de las protestas de la oposición conocidas como "Marchas de la disidencia" en diferentes regiones del país durante los dos años anteriores.

Los activistas planeaban otra "Marcha de la disidencia" durante la Cumbre, y por primera vez desde 2005 la marcha había sido aprobada oficialmente por las autoridades locales. Pero eso no impidió que fuerzas policiales llevaran a cabo una serie de detenciones que impidieron que muchos activistas, defensores de los derechos humanos y periodistas pudieran tomar parte en las protestas. En Samara, varios activistas y organizadores de la marcha fueron detenidos con pretextos endebles en los días previos a la Cumbre, y otros destacados activistas que estaban planeando viajar a Samara fueron hostigados en todo el país

En Moscú, 27 personas fueron detenidas en el aeropuerto de Sheremetyevo en la víspera del evento, incluyendo a los líderes del Frente Civil Unido, Garry Kasparov, Alexander Ryklin y Alexander Osovtsov; al líder del Partido Nacional Bolchevique Eduard Limónov; al reportero del *Wall Street Journal* Alan Callison; al reportero de la televisión holandesa Allard Detiger; al reportero de *Daily Telegraph* Adrian Blumfeld; y a Alexander Petrov, representante de la oficina de Moscú *de Human Rights Watch*. Comparando los nombres de los pasajeros con los que figuraban en una lista, los agentes de policía confiscaron los pasaportes de varias de estas personas y se los devolvieron después de que el avión hubiera despegado, mientras que los oficiales del Servicio Federal de Seguridad (conocido como el FSB) impidieron a otros subir al avión.[1]

Las autoridades también se desplegaron a través del sistema ferroviario. Sergey Udaltsov, el líder de la Vanguardia de la Juventud Roja, fue detenido en la estación de ferrocarril Kazanskiy en Moscú cuando estaba comprando los pasajes para el tren Moscú-Samara. Denis Bilunov, director ejecutivo del Frente Civil Unido, fue detenido en un tren que se aproximaba a Samara, con el pretexto de verificar la autenticidad de su dinero de bolsillo. Las detenciones elevaron las alarmas en la comunidad de derechos humanos de Rusia. Para Sergey Shimovolos, el acoso que sufrió en el tren desde Nizhni Nóvgorod fue un ejemplo de aquello que precisamente se disponía a investigar en Samara.

> “De acuerdo con diversas fuentes, la ‘Base de datos de vigilancia’ incluye los nombres de 3800 a 6500 personas, algunas de ellas representantes de la extrema derecha y de organizaciones nacionalistas, y algunas de ellas activistas de los derechos civiles y políticos. Shimovolos fue incluido en la sección titulada ‘Activistas de Derechos Humanos’.”

Pero el acoso no terminó cuando llegó a Samara. Al descender del tren, Shimovolos fue detenido de nuevo por varios policías. Revisaron sus documentos de identidad y esta vez le ordenaron que fuera con ellos a la comisaría para que pudieran buscar su nombre en lo que llamaron “la base de datos”, amenazando con usar la fuerza si se negaba a cumplir la orden. Shimovolos fue retenido en la estación de policía por unos 45 minutos antes de ser liberado.

Shimovolos estaba enojado. Preocupado por lo que parecía ser una detención coordinada de activistas y periodistas, y por la insinuación de las autoridades de que mantenían una base de datos que incluía a disidentes pacíficos y defensores de los derechos humanos, Shimovolos intentó tres veces presentar reclamos formales contra los policías que lo detuvieron y, cada vez, los fiscales se negaron a abrir un proceso penal contra los agentes. Así, en mayo de 2007 y de nuevo en diciembre de 2008, Shimovolos presentó demandas civiles por su arresto y sus repetidas detenciones y por el hecho de estar incluido en la base de datos de vigilancia del gobierno ruso. Esos esfuerzos tampoco tuvieron éxito, y después de haber agotado todos los posibles recursos jurídicos de Rusia, Shimovolos presentó una solicitud ante el Tribunal Europeo de Derechos Humanos (TEDH), con el argumento de que su detención y la recolección de sus datos personales en una base de datos de vigilancia violaban los artículos 5 y 8 de la Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esos procedimientos y las investigaciones que siguieron revelaron no solo que Shimovolos había sido en efecto objeto de hostigamiento oficial deliberado, sino también que las autoridades mantenían un extenso e intrincado sistema de vigilancia destinado a controlar la circulación de personas “sospechosas” en Rusia.

Documentos que salieron a la luz a raíz de las quejas de Shimovolos revelaron que un mes y medio antes de su viaje, el Departamento del Interior de Nizhni Nóvgorod registró su nombre en la denominada “Base de datos de vigilancia” (‘Сторожевой контроль’) mantenida por

la policía. Unas semanas más tarde, a principios de mayo, los departamentos regionales de policía de todo el país fueron alertados de que varias organizaciones de la oposición estaban preparando concentraciones de protesta para que coincidieran con la cumbre UE-Rusia del 18 de mayo, y los agentes fueron instruidos para detectar y detener a todos los miembros de esas organizaciones que viajaran a Samara entre el 8 y el 20 de mayo de 2007; a los oficiales de los aeropuertos y estaciones de tren se les dijo que separaran a esos viajeros de los demás y los disuadieran de continuar hacia Samara. Shimovolos era uno de esos viajeros: después de haber comprado el pasaje de tren de Nizhni Nóvgorod a Samara, los departamentos locales de policía a lo largo de su ruta recibieron mensajes de télex, indicando que estaba viajando a Samara para participar en un evento de la oposición y que podría estar llevando consigo literatura extremista.[2] Debido a que no llevaba equipaje, la policía no pudo invocar el ardid de buscar literatura extremista; en cambio, fue detenido e interrogado en varias ocasiones durante el viaje. Pero la información en la "Base de datos de vigilancia" persiguió a Shimovolos mucho después de concluida la Cumbre de Samara. Más de un año después, en octubre de 2008, Shimovolos fue detenido en un tren durante un viaje a Moscú. La policía revisó su pasaporte y luego llevó a cabo un extenso registro, primero de su equipaje, luego de su compartimento, y finalmente de todo el vagón; incluso abrieron los paneles de la pared del vagón, en una inspección que retrasó el tren media hora.

A pesar de que las órdenes que crean y rigen el funcionamiento de las bases de datos internas de vigilancia en Rusia se mantienen en secreto, los litigios de Shimovolos ante el TEDH iluminaron algunos detalles cruciales acerca de cómo llegaron a existir esas bases de datos, y la forma en que operan. En dicho procedimiento, el gobierno ruso admitió que desde alrededor del año 2000, las autoridades del Ministerio del Interior de la Federación Rusa habían estado usando una "autopista de búsqueda" de datos ('Розыск-магистраль') que incluía a personas que figuraban en la de fugitivos de Interpol, a ciudadanos extranjeros sospechosos de delitos cometidos en territorio ruso, a extranjeros cuya entrada a la Federación Rusa estaba prohibida o restringida, a personas sospechosas de una variedad de delitos, desde actos terroristas, asesinato y tráfico de drogas a contrabando de antigüedades y delitos financieros, a líderes y miembros de grupos delictivos organizados y a líderes de comunidades étnicas. La orden que rige la creación y el funcionamiento de la base de datos nunca fue publicada. En 2005, el gobierno ruso amplió la base de datos de la "autopista de búsqueda" para incluir una base de datos de potenciales extremistas cuyo nombre en código era "Base de datos de vigilancia". En una declaración jurada presentada ante el TEDH, un oficial del Departamento del Interior de la Federación Rusa dijo que la decisión de incluir el nombre de una persona en la "Base de datos de vigilancia" es del Ministerio del Interior o de sus departamentos regionales sobre la base de información confidencial.

De acuerdo con diversas fuentes, la "Base de datos de vigilancia" incluye los nombres de 3800 a 6500 personas, algunas de ellas representantes de la extrema derecha y de organizaciones nacionalistas, y algunas de ellas activistas de los derechos civiles y políticos. Shimovolos fue incluido en la sección titulada "Activistas de Derechos Humanos". Presionadas para fundamentar la legitimidad de incluir a Shimovolos en la base, las autoridades rusas afirmaron que él había sido uno de los fundadores de Sociedad para la Amistad Ruso-Chechena, y que también publicaba el periódico *Defensa de los Derechos Humanos* ('Сторожевой контроль').

El 21 de junio de 2011, cuatro años después de la Cumbre de Samara, el TEDH declaró que la "Base de datos de vigilancia", que funcionaba sin las garantías mínimas para prevenir abusos, no cumplía con las normas internacionales del debido proceso y almacenamiento de datos y, más específicamente, que la inclusión del nombre de Sergey Shimovolos en ella (que permitió la recolección de información sobre sus movimientos en tren o avión dentro de Rusia), violó el artículo 8 de la Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que garantiza el derecho al respeto de la vida privada y familiar de una persona. El TEDH concluyó asimismo que la detención ilegal de Shimovolos en la estación de policía de Samara había violado su derecho a la libertad y a la seguridad.

En una entrevista con *Gazeta.ru* poco después de la decisión del TEDH, Sergey Shimovolos reflexionó sobre el camino que recorrió en su búsqueda de la verdad sobre las bases de datos de vigilancia clandestinas del gobierno ruso:

Ante mi insistencia, los agentes de policía de Samara elaboraron un informe de mi detención en el que escribieron que tenían instrucciones para realizar una búsqueda operativa, es decir, había habido un mensaje telefónico sobre mí. Esa fue una pista, y luego la investigación se inició y prolongó durante dos años. Me dirigí a la oficina del fiscal para iniciar una acción penal contra el FSB. En los materiales de investigación se observaba que existía "una base de datos", en la que había sido incluido bajo la sospecha de organizar las Marchas del disenso. Eso significa que se había establecido un régimen especial de recolección de información sobre una determinada persona, sobre sus movimientos, sus comunicaciones con las autoridades gubernamentales, con la Inspección de Seguridad del Tráfico en Carretera, con cualquier institución. Se crea un archivo personal. Todo eso va junto con la aplicación de medidas preventivas hacia la persona sospechosa de extremismo: si debe ser capturado o advertido; qué explicaciones deben exigírsele. Sin duda alguna, todo eso es ilegal.[3]

Curiosamente, después de la sentencia que el Tribunal Europeo emitió en el caso de Shimovolos, representantes del Ministerio del Interior intentaron negar la existencia de tal "Base de datos de vigilancia". La Agencia Interfax citó a un representante del ministerio que afirmaba que no había ninguna

Manifestante grita consignas contra el gobierno durante una protesta en Samara, Rusia, el 18 de mayo de 2007. Numerosos manifestantes marcharon por esa ciudad en una protesta organizada con motivo de una tensa cumbre entre Rusia y la Unión Europea.
Foto: Sergey Ponomarev/AP

disposición para una base de datos con esa denominación en los reglamentos del Ministerio del Interior. Sin embargo, reconocía que los agentes de policía utilizaban dicho término en su práctica operativa y que eso "a veces podía ser malinterpretado por los ciudadanos".[4]

el contexto

La "Base de datos de vigilancia" es solo uno de los componentes de un sistema de vigilancia integrado que permite a las autoridades rusas supervisar el movimiento y las comunicaciones de personas "sospechosas", todo en nombre de una lucha muy laxamente definida contra el extremismo. Bajo una ley federal titulada "de neutralización de las actividades extremistas", que fue promulgada el 25 de julio de 2002 y sigue vigente hoy en día, el "extremismo" incluye no solo la comisión de delitos de odio y amenazas al sistema constitucional, sino también incitar la enemistad hacia grupos sociales, acusar a funcionarios de delitos extremistas e impedir actividades legítimas de autoridades gubernamentales.[5]

En septiembre de 2008, se creó un departamento especial dentro del Ministerio del Interior para luchar contra el extremismo, y se establecieron centros de contraextremismo en cada departamento regional del Ministerio. Los así llamados Centros "E" se modelaron en base a los antiguos departamentos de lucha contra el crimen organizado, y en muchos aspectos adoptaron los mismos métodos. Al tratar a los opositores al gobierno como transgresores, y echando mano de un sofisticado aparato operativo y de investigación en su contra, los Centros "E" se convirtieron en una herramienta importante del espionaje político en Rusia.

Los procedimientos de búsqueda y vigilancia están regulados por la Ley de Actividades de Búsqueda Operativa de 1995, que regula una amplia variedad de operaciones que incluyen objetivos de vigilancia, el seguimiento de envíos postales y de telecomunicaciones, el acceso y descarga de información y comunicaciones digitales y la infiltración estratégica en grupos específicos. Por regla general, estas actividades operativas pueden llevarse a cabo solo dentro de procesos penales iniciados, y para actividades susceptibles de infringir los derechos constitucionales de los ciudadanos se requiere una orden judicial. Pero la falta de garantías claras para los derechos de los ciudadanos, combinados con la laxitud y la ineficiencia de controles judiciales, abren el camino para que el sistema de actividades de búsqueda sea utilizado como una herramienta para vigilar a miembros de la oposición, activistas políticos y defensores de los derechos. Muchas de estas debilidades salieron a la luz cuando Roman Zakharov, director del centro regional

Garry Kasparov habla con los medios de comunicación en el aeropuerto Sheremetyevo de Moscú el 18 de mayo de 2007. La policía impidió que el campeón ruso de ajedrez y líder de la oposición viajara ese día a la ciudad de Samara, donde planeaba participar en una marcha de protesta en ocasión de una cumbre entre Rusia y la Unión Europea, según explicó un asesor. Foto: Misha Japaridze/AP

de San Petersburgo para la Fundación de Defensa de la Glasnost, sospechó que sus llamadas por teléfono móvil estaban siendo interceptadas y presentó una demanda contra el gobierno ruso en el TEDH. Aunque Zakharov fue incapaz de demostrar que sus llamadas habían sido interceptadas, el tribunal consideró que los procedimientos operativos que regían la intervención de llamadas telefónicas violaban el artículo 8 de la Convención Europea de Derechos Humanos. En su dictamen de diciembre de 2015, el tribunal identificó una gran variedad de deficiencias fundamentales en la legislación rusa que permiten a los servicios de seguridad y a la policía eludir la exigencia de la orden judicial e interceptar comunicaciones sin necesidad de obtener una autorización judicial previa.

En primer lugar, el tribunal consideró que la legislación rusa no restringe lo suficiente la lista de personas cuyas comunicaciones telefónicas pueden ser interceptadas. Los objetivos potenciales no se limitan a personas sospechosas o acusadas de delitos, por ejemplo, sino que también pueden incluir a cualquier persona que pueda tener información sobre un delito o cualquier otra información que pueda ser relevante en un caso criminal. Por otra parte, el tribunal consideró que la Ley de Actividades de Búsqueda Operativa establece que las llamadas telefónicas y otras comunicaciones pueden ser interceptadas en base a información sobre una amplia y pobremente definida variedad de acontecimientos o actividades que se dice ponen en peligro la seguridad nacional, militar, económica o ecológica de Rusia.

En segundo lugar, el tribunal se enteró de que, aunque los servicios de seguridad estén obligados nominalmente a obtener una autorización judicial previa a la intervención, no tenían obligación de presentar una autorización de intervención al operador de red móvil. Esta laguna, esencialmente, dio a las autoridades policiales acceso directo a todas las comunicaciones de telefonía móvil y datos comunicacionales relacionados.

En tercer lugar, en virtud de la legislación, incluso cuando un tribunal dicta una orden de intervención telefónica, no es competente para supervisar su aplicación. El tribunal no es informado de los resultados de la vigilancia y no tiene poder para revisar si los servicios de seguridad o la policía cumplen con los términos o requisitos de la orden judicial.

Por último, el tribunal consideró que la policía estaba haciendo una utilización prolífica de estos poderes de vigilancia, con muy poca resistencia por parte de los tribunales. Según los datos publicados por el Departamento Judicial del Tribunal Supremo de la Federación Rusa, en el período comprendido entre 2007 y 2015, los tribunales rusos de jurisdicción general consideraron 4.659.325 solicitudes para monitorear e interceptar llamadas telefónicas y otras comunicaciones, y aprobaron 4.517.515, o el 96,96%, de esas solicitudes.[6] Por otra parte, el

> “En septiembre de 2008, se creó un departamento especial dentro del Ministerio del Interior para luchar contra el extremismo, y se establecieron centros de contraextremismo en cada departamento regional del Ministerio. (...) Al tratar a los opositores al gobierno como transgresores, y echando mano de un sofisticado aparato operativo y de investigación en su contra, los Centros ‘E’ se convirtieron en una herramienta importante del espionaje político en Rusia.”

número de solicitudes aumentó de año a año durante ese período, con la mayor tasa de aumento por fuera o antes de la apertura de un proceso penal formal. Con al menos dos personas implicadas en cada una de esas solicitudes de vigilancia, los datos sugieren que en los últimos nueve años un mínimo de nueve millones de personas en la Federación de Rusia –o el 6% de la población– podría haber tenido sus llamadas o comunicaciones interceptadas con autorización judicial. Y teniendo en cuenta que la Corte Europea determinó en el caso Zakharov que existía una falta general de control sobre el acceso que tienen los agentes del orden al aparato de vigilancia, es probable que las llamadas y comunicaciones de muchas más personas hayan sido monitoreadas sin autorización judicial o supervisión alguna.

Para los activistas de los derechos civiles y defensores de los derechos humanos en Rusia, la vigilancia puede incluir no solo el seguimiento de sus movimientos y el monitoreo de sus comunicaciones, sino también la grabación en audio y video de sus actividades diarias.

El 14 de agosto de 2009, miembros de la Asociación Agora descubrieron en sus oficinas una cámara oculta con un micrófono que había estado grabando video y audio de las conversaciones entre los líderes de la organización y visitantes por un período indeterminado. Los pedidos de Agora a las autoridades para poner en marcha una investigación criminal de esa vigilancia ilegal fueron rechazados.[7] Del mismo modo, en agosto de 2012, una cámara oculta y un micrófono fueron descubiertos en la oficina del Fondo Anticorrupción del político de la oposición Alexey Navalny.[8]

En febrero de 2012, un video de la vida privada del político Vladimir Ryzhkov, que había sido grabado con una cámara oculta, fue subido a internet. En marzo de 2016, un video de la vida privada de otro político, Mikhail Kasyanov, filmado también con una cámara oculta, fue emitido por el canal nacional de televisión NTV. Ambos videos contenían escenas de relaciones íntimas y claramente se habían hecho con el objetivo de exponer públicamente a esas personas.[9]

En todos estos casos, no hubo evidencia directa de que los videos fuesen hechos por las fuerzas del orden. Sin embargo, hay algunos indicios que apuntan en esa dirección. Por ejemplo, los abogados de Agora ordenaron un peritaje según el cual la cámara y el micrófono descubiertos en sus oficinas estaban incluidos en la lista de equipos especiales para la obtención secreta de información, que pueden ser utilizados solo por agencias estatales. Un mes después de que se encontrara la cámara, se abrió un caso criminal contra Agora, acusándola de evadir impuestos. El caso fue posteriormente desestimado.

El 5 de octubre de 2012, el canal de televisión nacional NTV mostró la película “Una anatomía de la protesta - 2”, que contenía imágenes tomadas con una cámara oculta de una reunión de la oposición con sede en Moscú, organizada por Serguéi Udaltsov, Leonid Razvozzhaev, Konstantin Lebedev y el político georgiano Givi Targamadze. Los realizadores alegaron

> “En el período comprendido entre 2007 y 2015, los tribunales rusos de jurisdicción general consideraron 4.659.325 solicitudes para monitorear e interceptar llamadas telefónicas y otras comunicaciones, y aprobaron 4.517.515, o el 96,96%, de esas solicitudes.”

que el material mostraba a un grupo discutiendo la organización de disturbios civiles y la financiación externa para el movimiento de la oposición.[10] Udaltsov, Razvozzhaev y Lebedev fueron posteriormente declarados culpables de organizar disturbios y condenados a largas penas de prisión.

Las invasiones a la privacidad de líderes de la oposición y activistas también han incluido la inspección de correos electrónicos y otras correspondencias digitales. En diciembre de 2011, inmediatamente después de las elecciones parlamentarias que suscitaron protestas masivas en Moscú y otras ciudades de Rusia, un medio de comunicación favorable al gobierno publicó extractos de la correspondencia de funcionarios de la importante organización no gubernamental Golos, que supervisó de forma independiente el proceso electoral. El medio anunció que había obtenido 60 megabytes de correspondencia electrónica privada que revelaban la financiación de actividades destinadas a desacreditar las elecciones en Rusia.[11] Lilia Shibanova, directora ejecutiva de Golos, protestó públicamente, señalando que la correspondencia había sido “tomada desde el buzón” de su segundo, Grigory Melkonyants, que a menudo enviaba mensajes desde su cuenta de correo electrónico bajo sus instrucciones, y que “hackear cuentas de correo electrónico es una violación de la ley”.[12] Melkonyants mismo informó que su cuenta de correo electrónico fue hackeada el 5 de diciembre de 2011, justo antes de una conferencia de prensa sobre las elecciones de la Duma Estatal. Como cuando Agora recurrió a los tribunales por las escuchas en sus oficinas, las autoridades rechazaron todos los pedidos de Golos para abrir una investigación.

A pesar de la falta de pruebas directas de que el hackeo hubiese sido ordenado por el gobierno, la constante negativa de investigar los ataques contra activistas civiles, periodistas y defensores de los derechos humanos suscita serias sospechas. En abril de 2013, la abogada de derechos humanos Marina Dubrovina, tras presentar una orden de representación de intereses del cliente al agente investigador del Departamento de FSB para la región de Krasnodar, se enteró de que sus llamadas telefónicas habían sido interceptadas y su cuenta de correo electrónico hackeada. Esto siguió al hackeo de mayo de 2012 del correo electrónico y cuentas de Skype y Facebook de otros tres abogados de derechos humanos: Olga Gnezdilova, de Vorónezh; Dmitriy Dinze, de San Petersburgo; y Svetlana Sidorkina, de Moscú. Aunque todos los casos fueron denunciados, ninguno de los hackers o los organizadores de los ataques informáticos fueron encontrados ni puestos a disposición de la justicia.[13]

Mientras tanto, la información recolectada a través de esta oscura vigilancia de correos electrónicos se ha utilizado en el procesamiento de actividades políticas y de derechos humanos. En el verano de 2015, la policía detuvo a tres miembros de un grupo de acción que exigía un referéndum “por un gobierno responsable”, abogando por enmiendas a la Constitución y la promoción de una ley de ética para los funcionarios de alto rango de la Federación Rusa. El publicista Yuriy Muhin, el oficial de reserva de la fuerza aérea

Manifestantes gritan consignas contra el gobierno durante una protesta en Samara, Rusia, el 18 de mayo de 2007. Foto: Sergey Ponomarev/AP

Kiril Barabash, el administrador de sistemas Valeriy Parfenov y el periodista Alexander Sokolov de RBC fueron acusados de participar en las actividades de una organización extremista.[14] Una pieza clave de las pruebas de cargo era la correspondencia de Gmail entre los acusados, que fue entregada a los investigadores por un agente que se había infiltrado en el grupo y estaba incluido en la lista de destinatarios de correo electrónico.

Al igual que con las grabaciones clandestinas de video y de audio, la vigilancia de correos electrónicos privados y otra correspondencia digital se ha utilizado específicamente para desacreditar a defensores de los derechos civiles y humanos. En marzo de 2016, como parte de una operación que tenía la clara intención de manchar a Igor Kalyapin, director del Comité para la Prevención de la Tortura, que trabaja con frecuencia en Chechenia, el canal de televisión local mostró sus comunicaciones SMS. Los mensajes de texto, que se remontaban a noviembre de 2014, evidentemente habían sido obtenidos por las autoridades policiales en el curso de sus actividades operativas.[15]

De modo similar, en marzo de 2016, la emisora nacional de televisión Pyatiy Kanal [Canal Cinco] mostró dos cortometrajes sobre las actividades del grupo de defensa de los derechos civiles *Komanda-29*, que se especializa en la defensa de quienes han sido acusados de alta traición y lidian con asuntos relacionados a la divulgación de secretos de Estado. Ambos informes acusaban a los abogados de *Komanda-29* de trabajar para otros países, ofreciendo como pruebas sus documentos y correspondencia de correo electrónico. Según Ivan Pavlov, director de *Komanda-29*, la información había sido obtenida como resultado de la inspección de correos electrónicos.[16]

conclusión

Cuando en 2007 Sergey Shimovolos bajó del tren en la estación de Samara y fue detenido por la policía, no sabía que desde 2005 las autoridades rusas habían estado desarrollando un sistema de control integrado que se utilizaba para atacar a activistas políticos y defensores de los derechos civiles. En los años transcurridos desde que a Shimovolos se le dijo que estaba en “la base de datos”, este sistema de vigilancia no ha hecho más que expandirse. Los litigios llevados adelante por Shimovolos y muchos otros activistas y organizaciones en los últimos diez años han revelado un sistema que incluye la vigilancia de los movimientos de los individuos dentro de la Federación Rusa y en los pasos fronterizos, intervención de comunicaciones telefónicas, grabaciones secretas de audio y video e inspección de correspondencia por correo electrónico y hackeo de cuentas de servicios de internet. A medida que estos poderes han crecido, son cada vez más

utilizados para monitorear y desacreditar a aquellos a quienes el gobierno designa como “la quinta columna” y “traidores nacionales”.

De hecho, los casos descritos muestran de qué manera, en ausencia de un control público y judicial, un sistema de vigilancia establecido formalmente para contrarrestar e investigar delitos puede convertirse en una herramienta de persecución política. Y aquellos que se convierten en el blanco de ese sistema disponen en Rusia de pocas opciones: ni un solo caso que involucre la intervención injustificada de comunicaciones por correo electrónico, correo postal o teléfono, el monitoreo de redes sociales y de la actividad en internet, la grabación encubierta de audio y video, o la vigilancia física ha dado lugar a procedimientos legales o sanciones a los responsables. En cualquier sociedad, tales poderes irrestrictos de vigilancia tendrían seguramente un efecto negativo en las voces disidentes y organizaciones de la sociedad civil; más aún cuando están acompañados, como ha sido recientemente el caso en Rusia, con esfuerzos por parte de las autoridades para penalizar a una amplia variedad de actividades cívicas y políticas.

El hecho de que esto esté ocurriendo en Rusia, que nunca ha conseguido deshacerse de las estructuras del estado de vigilancia soviético, plantea desafíos particulares para afrontar esta nueva ola de vigilancia incontrolada y arbitraria hacia millones de residentes rusos. En muchos países, las revelaciones de Edward Snowden provocaron una seria reflexión y debate sobre los límites de la intrusión del Estado en la vida privada y familiar. No así en Rusia. De hecho, a pesar de que a Snowden se le concediera asilo provisional en Rusia en julio de 2013, en una encuesta realizada por la Fundación de Opinión Pública, el 41% de los rusos confesó que nunca había oído hablar de Snowden o de sus revelaciones. Y las noticias sobre casos específicos de vigilancia por motivos políticos en Rusia a menudo son recibidas con un encogimiento de hombros; un legado de la era soviética que se caracterizó por las actitudes de “todos están bajo vigilancia” y “no tengo nada que ocultar”. Incluso la reciente noticia de que una gran cantidad de información personal sobre propiedades, estados de salud, documentos personales, comunicaciones, viajes y transacciones financieras que se encuentran en las bases de datos controladas por el Estado también están disponibles en el mercado negro, ha hecho poco para cambiar esas actitudes profundamente arraigadas. Pero cuando un gobierno acumula más y más datos personales y ni siquiera tiene la voluntad de almacenarlos de forma segura, ya no son solo los opositores políticos los que deberían estar preocupados por su mirada indiscreta.

notas

-

1. Todos los viajeros de Moscú a Samara en la víspera de la Cumbre estaban bajo sospecha. Algunas personas fueron detenidas. Ver NEWSru.com 17 de mayo, 2007. Disponible en: http://www.newsru.com/russia/17may2007/samara_zaderj.html [28/10/2016].
2. Una ley de 2001 promulgada por la Federación de Rusia ordenó que los pasajes de tren solo podían venderse presentando un pasaporte válido y con el registro de los datos personales del viajero. En 2004 esta exigencia se amplió a los viajes aéreos y, en 2012, al servicio de autobuses interregionales. Por lo tanto, cada vez que alguien en Rusia compra un pasaje doméstico, su información personal y su itinerario quedan a disposición de las autoridades. Para Shimovolos y otros activistas de derechos humanos, así como para la oposición y los periodistas, estos requisitos suponen que a menudo se vean obligados a cancelar y comprar pasajes a último momento con la esperanza de llegar a destino sin detenciones ni interrupciones.
3. “Estrasburgo admitió la existencia de ‘listas negras’”, por Alexandra Koshkina, *Gazeta.ru* (21 de junio, 2011). Disponible en: https://www.gazeta.ru/social/2011/06/21/3670661.shtml [28/10/2016].
4. “MI negó la existencia de la Base de datos de vigilancia”, por Anna Pushkarskaya, *Kommersant* (23 de junio, 2011). Disponible en: http://www.kommersant.ru/doc/1664976 [28/10/2016].
5. Ley Federal No114-FZ. Disponible en: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102108221&backlink=1&&nd=10207922 [28/10/2016]
6. Disponible en: http://www.cdep.ru/index.php?id=79 [28/10/2016].
7. “El Tribunal determinó que la orden de búsqueda en la Asociación Agora es legal”, *Open Information Agency* (18 de agosto, 2009). Disponible en: http://openinform.ru/news/pursuit/19.08.2009/13402/ [28/10/2016].
8. “Encontraron más dispositivos de interceptación y una cámara oculta en la oficina de Navalny”, Radio Svoboda (6 de agosto, 2012). Disponible en: http://www.svoboda.org/a/24668525.html [28/10/2016].
9. “El canal de televisión NTV mostró imágenes tomadas por una cámara oculta de líderes de la oposición”, RBC (1 de abril, 2016). Disponible en: http://www.rbc.ru/rbcfreenews/56fe9b1a9a794742ee8a7f90 [28/10/2016].
10. “‘Una anatomía de la protesta - 2’: NTV sospecha de S. Udaltsov por alta traición”, RBC (5 de octubre, 2012). Disponible en: http://www.rbc.ru/politics/05/10/2012/673004.shtml [28/10/2016].
11. “Life News publica la correspondencia entre ‘Golos’ y el Departamento de Estado de EE.UU.”, *Lifenews.ru* (8 de diciembre, 2011). Disponible en: http://lifenews.ru/news/76604 [28/10/2016].
12. “‘Golos’ llevará el caso a la corte”, *Interfax* (9 de diciembre, 2011). Disponible en: http://www.interfax.ru/russia/220999 [28/10/2016].
13. “Cómo se obstruye el trabajo de los abogados en Rusia. Un informe de defensores de los derechos”, *Novaya Gazeta* (23 de septiembre, 2013). Disponible en: https://www.novayagazeta.ru/articles/2013/09/23/56486-kak-v-rossii-meshayut-rabotat-advokatam [28/10/2016].
14. “El caso ‘ZOV’” (del grupo de acción por el referéndum), Centro de derechos humanos Memorial (29 de octubre, 2015). Disponible en: http://memohrc.org/special-projects/delo-igpr-zov [28/10/2016].
15. Informe de la Radio Estatal de Chechenia y de la emisora de televisión de Grozni (16 de marzo, 2016). Disponible en: https://www.youtube.com/watch?t=185&v=-oHQNsK6E5I [28/10/2016].
16. Informe de Pyatiy Kanal (6 de marzo, 2016). Disponible en: https://www.youtube.com/watch?v=0I_MmETZgms [28/10/2016].

Un vistazo a la vigilancia en Rusia

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
No.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia?
A los rusos no parece importarles en absoluto las revelaciones de Snowden. La discusión alrededor del caso Snowden se centró principalmente en la relación entre Rusia y Estados Unidos y la decisión de darle asilo.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de las dos opciones?
Han aumentado.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No, a pesar de la sentencia del Tribunal Europeo de Derechos Humanos en el caso *Roman Zakharov v. Rusia*.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Lo ampliaría. Desde 2012 el Parlamento ruso ha adoptado docenas de leyes que limitan los derechos y las libertades civiles.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia del gobierno, ¿dicha legislación impondría nuevos controles estructurales?
No. En el Parlamento ruso no hay ningún partido político que se centre en controlar a los servicios de seguridad.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional gubernamental han sido objeto de litigio interno, incluso en los tribunales constitucionales?
No.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
Sí. El 22 de marzo de 2016 uno de los tribunales de distrito de Moscú rechazó la decisión de multar a una compañía llamada de Yandex por negarse a darle al Servicio Federal de Aduanas los datos personales de sus usuarios, incluyendo mensajes electrónicos.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
Más. Entre 2013 y 2015 el número de quienes confían en el servicio de seguridad del Estado se incrementó del 36% al 50%.

El caso Re (X) y los sujetos invisibles de la vigilancia digital

4
CANADÁ

Richard Mosley, juez federal canadiense. Foto: Couvrette/Ottawa

CANADÁ

El caso Re (X) y los sujetos invisibles de la vigilancia digital

el caso

A fines de 2013, el juez federal canadiense Richard Mosley emitió un fallo que sacudió a la sigilosa comunidad de seguridad nacional de Canadá.

Cuatro años antes, en 2009, el Servicio de Inteligencia y Seguridad Canadiense (CSIS) se presentó en una audiencia secreta *ex parte* ante el juez Mosley para solicitar un permiso para interceptar y monitorear las comunicaciones electrónicas de dos ciudadanos canadienses. El CSIS ya tenía una orden para vigilarlos dentro de Canadá; ahora el servicio pedía que se lo habilitara para trabajar con la Agencia de Seguridad en las Comunicaciones (CSE), la agencia de inteligencia de señales de Canadá, para monitorearlos cuando estaban fuera del país. Normalmente, la CSE no está autorizada legalmente para interceptar comunicaciones de canadienses, pero en el así llamado "mandato de asistencia" puede utilizar su equipo y experiencia para ayudar a otra agencia con una investigación autorizada. Los tribunales habían mostrado cierta cautela en la aprobación de estas operaciones conjuntas CSE-CSIS. Un intento anterior de obtener una orden judicial para operar en el extranjero había sido rechazada con el argumento de que la Ley CSIS, que define el alcance de las actividades y los poderes del CSIS, no autoriza investigaciones de inteligencia en el extranjero, en particular las que, debido a su naturaleza intrusiva, podrían violar leyes de otros países.[1] Pero ante el juez Mosley, el CSIS argumentó que esta solicitud era diferente: en este caso, la vigilancia de los dos objetivos se llevaría a cabo y se controlaría desde el interior de Canadá, lo que significaba que la información de vigilancia recolectada estaría sujeta a garantías legales. Mosley autorizó la orden judicial expresamente por esa garantía, y durante al menos un año el CSIS llevó a cabo la vigilancia electrónica de los dos individuos.

Todavía no se sabe quiénes eran estos "sospechosos": ni sus nombres, ni su sexo, ni cualquier otro detalle sobre sus vidas. Tampoco conocemos la naturaleza de sus acciones que, al parecer, se consideraron lo suficientemente suspicaces como para asegurar la orden de vigilancia interna en primer lugar. El carácter secreto de los casos de seguridad nacional que requieren órdenes judiciales invisibiliza a los sujetos. El proceso se lleva a cabo con tanto secretismo que lo más probable es que quienes estén siendo vigilados nunca se enteren de ello. Y, a diferencia de la vigilancia relacionada con las investigaciones criminales, no es obligatorio que nadie por fuera de estos procedimientos ocultos sepa que se produjo el espionaje. En pocas palabras, los canadienses rara vez saben que están siendo sometidos a vigilancia electrónica, o por qué.

Para asegurar una orden judicial como la que se le pidió al juez Mosley, el CSIS tiene que convencer al tribunal de que la operación de vigilancia prevista es necesaria y proporcionada y que se llevará a cabo conforme a la ley, incluida la Carta Canadiense de Derechos y Libertades. Pero debido a que los procedimientos son secretos, y porque tienen muy poco control externo o supervisión, los jueces que oyen estas solicitudes dependen de la información que los mismos servicios de seguridad proveen, y son totalmente incapaces de evaluar si estos retienen información. El juez Mosley aceptó la solicitud de 2009 para vigilar a los dos sospechosos fuera de Canadá porque estaba convencido de que, al garantizársele que la vigilancia sería recolectada y controlada desde dentro de Canadá, el CSIS y la CSE aseguraban que las comunicaciones privadas de los canadienses interceptados se utilizarían solo si eran esenciales para fines de seguridad nacional. Fue un importante precedente para el CSIS: en los siguientes cuatro años, el Tribunal Federal emitió 35 órdenes similares en base a la decisión del juez Mosley.[2]

Después, en junio de 2013, Mosley leyó algo que le pareció alarmante.

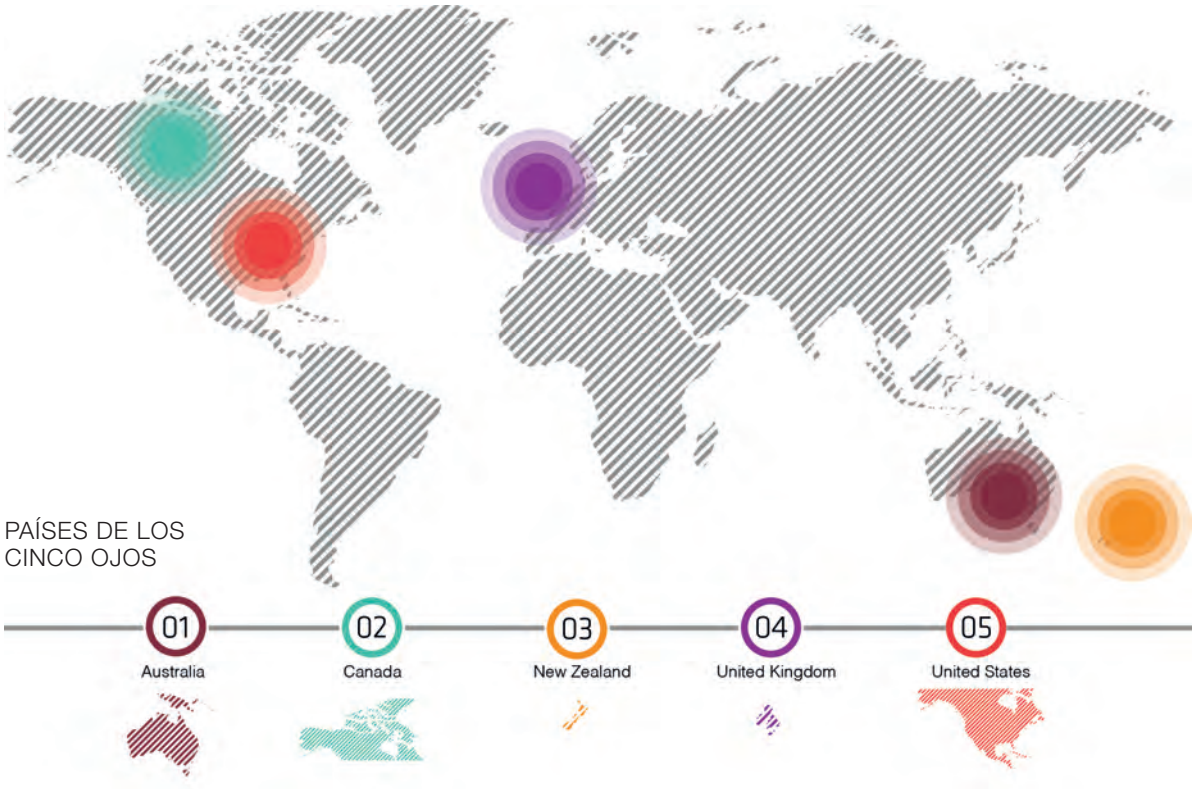
Cada año, la CSE es revisada por un comisionado de la CSE, por lo general un juez retirado que es designado para examinar sus actividades y evaluar si cumple con la ley, y para investigar cualquier queja contra la agencia. El comisionado de la CSE debe escribir un informe sobre esa revisión. La versión pública del informe es extremadamente prudente y

> “El juez Mosley emitió una sentencia pública contundente del caso, que se había dado a conocer como *Re (X)*, declarando enfáticamente que el Servicio de Inteligencia de Canadá y sus asesores legales habían cometido ‘un incumplimiento del deber de sinceridad debida a la corte’.”

cuidadosamente redactada para revelar muy poco sobre el funcionamiento real de la CSE, y rara vez atrae la atención más allá de un pequeño círculo de estudiosos y observadores de la política. Pero para el juez Mosley, algo saltó a la vista: en una discusión sobre el tipo particular de orden judicial que él había aprobado, el comisionado recomendaba que la CSE le dijera a su socio CSIS que “proveyera a la Corte Federal de Canadá de cierta evidencia adicional sobre la naturaleza y el alcance de la asistencia que la CSE puede brindar a CSIS”.[3]

La recomendación encendió las alarmas de Mosley: sugería que había algo que el tribunal –y, por extensión, él mismo– necesitaba saber acerca de cómo se estaban utilizando las órdenes judiciales que había concedido inicialmente. Decidió entonces tomar la inusual medida de llamar a los abogados del CSIS y la CSE para que se presentaran ante él y le explicaran qué era exactamente lo que estaba pasando. Específicamente, quería saber si había información o pruebas que le hubiesen sido retenidas durante la solicitud de la orden judicial, y si estas hubieran hecho una diferencia en su decisión de emitir la orden y permitir la vigilancia.

Puesto que tales procedimientos también son secretos, no conocemos todos los detalles de ese encuentro, o de las audiencias posteriores que el juez Mosley pidió en base a lo que descubrió ese día. Sin embargo, la versión pública del documento que resume los procedimientos reveló que la CSE no fue la única agencia que recolectaba información sobre los dos individuos vigilados; y que había pedido a sus homólogos de otros organismos, sus aliados de los Cinco Ojos, ayuda para llevar a cabo la vigilancia electrónica digital. Esto violaba claramente la letra y el espíritu de las garantías originales de la CSE. La orden fue concedida bajo el entendimiento específico de que el CSIS y la CSE controlarían la información sobre los dos objetivos canadienses, y de que la información reunida se quedaría en Canadá. Esa garantía era crucial. Cuando la información se recolecta y se conserva en Canadá, está protegida por las leyes



canadienses y es utilizada solo para los intereses de Canadá. Cuando es recolectada por otros, no existen tales protecciones. Hay acuerdos –de nuevo, completamente secretos– entre los aliados que se supone regulan este tipo de recolección e intercambio de información, pero no hay ninguna garantía de que esos acuerdos se respetarán si otro país decide que es de interés nacional utilizar la información reunida en operaciones conjuntas para sus propios fines.

El documento también revelaba que la omisión del CSIS y la CSE de su intención de pedir ayuda de aliados no fue accidental. Por el contrario, el empleado de la CSE que se presentó ante el juez admitió explícitamente que la presentación inicial había sido cuidadosamente "moldeada" con un asesor legal para dejar de lado la mención de terceras partes a las que se les podría pedir ayuda con la vigilancia.

Cerca del final de 2013, el juez Mosley emitió una sentencia pública contundente del caso, que se había dado a conocer como *Re (X)*, declarando enfáticamente que el Servicio de Inteligencia de Canadá y sus asesores legales habían cometido "un incumplimiento del deber de sinceridad debida a la corte". Denunciando el engaño del Servicio, Mosley escribió que "la corte debe estar preocupada de que la autoridad que le otorga el Parlamento para autorizar actividades de investigación intrusiva del Servicio pueda ser percibida en el ámbito público como una aprobación para vigilar e interceptar las comunicaciones de la población canadiense por parte de agencias extranjeras". [4]

El gobierno apeló la decisión de Mosley, pero el Tribunal Federal de Apelación confirmó la sentencia en julio de 2014. El CSIS se preparó para llevar su caso al Tribunal Supremo de Canadá, alegando que "el CSIS debe ser capaz de llevar a cabo su importante papel de recolección de inteligencia sobre amenazas a la seguridad de Canadá confiando en que está actuando dentro de la ley, y la población también tiene derecho a conocer qué limitaciones se le imponen al CSIS en este sentido". La Canadian Civil Liberties Association (CCLA) se preparó para presentar una moción para intervenir en esta apelación en nombre del interés público. Pero en 2015, el Parlamento canadiense aprobó dos proyectos de ley, C-51 y C-44, concediendo explícitamente al CSIS mayores poderes para vigilar fuera de Canadá. Como muchas de las cuestiones jurídicas cruciales dejaron de tener sentido a causa de las nuevas leyes, el gobierno retiró su apelación del caso *Re (X)* ante la Corte Suprema, lo que supone, al final, una rara derrota del gobierno y una oportunidad aún más rara para que las prácticas de vigilancia de Canadá fueran puestas bajo escrutinio público.

el contexto

Gracias a los esfuerzos de Edward Snowden y de otros informantes, contamos con mucha más información de la que alguna vez tuvimos acerca de las capacidades de las agencias de inteligencia de Canadá, y las formas en que el aparato de seguridad nacional canadiense trabaja con Estados Unidos, Reino Unido, Australia y

Maher Arar inclina la cabeza durante una conferencia de prensa a propósito de la disculpa y compensación del gobierno canadiense, Ottawa, el 26 de enero de 2007. Arar fue errónea e injustamente deportado a Siria, donde fue detenido y torturado. Foto: Tom Hanson/AP

Nueva Zelanda –sus socios internacionales en la alianza de los Cinco Ojos. Por ejemplo, por un memorando altamente confidencial publicado por Snowden, sabemos que la CSE ofrece "acceso geográfico único a áreas inaccesibles para los EE.UU." y ha "abierto sitios secretos a petición de la NSA". La NSA, a cambio, comparte tecnología de "recolección, procesamiento y análisis, y capacidades para asegurar la información".[5] Según una estimación, participar en los Cinco Ojos le da a Canadá acceso a una "asociación global de un valor de 15 mil millones de dólares canadienses", ampliando sensiblemente su capacidad de vigilancia.[6]

Cuanto más sabemos acerca de las capacidades técnicas de los servicios de inteligencia canadienses y de sus socios de los Cinco Ojos, parece más probable que el intercambio de información a través de las fronteras se utilice para eludir la legislación canadiense. Mientras que el CSIS no puede acceder a las comunicaciones de los canadienses dentro de Canadá sin una orden judicial,[7] y a la CSE se le prohíbe dirigir sus actividades hacia los canadienses salvo excepciones,[8] los organismos aliados no tienen prohibiciones en sus leyes que les impidan vigilar a los canadienses. Por el contrario, las comunicaciones exteriores son el blanco típico de la vigilancia, y ha habido sospechas –y de vez en cuando pruebas–, de que los aliados recolectan intencionadamente información unos de otros y luego encuentran maneras de compartirla –como cuando la inteligencia británica compartió voluntariamente con la NSA información recopilada a través del programa "Tempora", tal como informó el periódico *The Guardian*.[9]

El gobierno canadiense insiste en que los acuerdos entre los socios de espionaje prohíben este tipo de arreglos, pero no hay suficiente transparencia para confiar en tales garantías, y parece poco probable que Canadá pueda permanecer totalmente desacoplada de las actividades practicadas por sus aliados más cercanos. De hecho, el entonces comisionado de la CSE Robert Décary indicó de manera explícita en un informe recientemente desclasificado que no puede determinar si los socios de los Cinco Ojos cumplen con sus promesas de proteger la información acerca de los canadienses. Lo que encontró fue que más allá de "ciertas declaraciones y garantías generales" entre la CSE y sus socios, era "incapaz de evaluar en qué medida" los Cinco Ojos siguen los acuerdos con la CSE y protegen las comunicaciones privadas y la información sobre los canadienses que la CSE comparte con sus socios".[10]

Los canadienses tienen buenas razones para temer el intercambio de inteligencia entre los socios de los Cinco Ojos. En septiembre de 2002, Maher Arar, un ciudadano con doble nacionalidad sirio-canadiense, fue interceptado en el aeropuerto JFK de Nueva York en su camino de regreso a Canadá tras unas vacaciones familiares. Primero fue detenido en Estados Unidos bajo sospecha de que pertenecía a Al Qaeda, y posteriormente fue entregado por los Estados Unidos a Siria, donde fue torturado. Una comisión de investigación canadiense determinó que era una víctima inocente y que los inexactos informes de inteligencia y comunicaciones que los servicios de inteligencia de

Un vehículo pasa delante de la oficina central del Servicio de Inteligencia y Seguridad Canadiense (CSIS) en Ottawa, el 5 de noviembre de 2014.
Foto: Reuters/Latinstock

Canadá habían compartido con Estados Unidos, sin chequeo ni reservas apropiadas, condujeron al error. Por otra parte, al darle la información a Estados Unidos, la inteligencia canadiense había perdido el control tanto de la información como de la capacidad de influir en las acciones de su socio. Canadá, finalmente, se disculpó con el señor Arar y llegó a un acuerdo económico sustancial por su complicidad en su entrega y tortura, pero ninguna disculpa ni cantidad de dinero pueden reparar el daño que se le hizo a su vida.

Las historias de vigilancia más impresionantes refieren a personas –gente real, específica, con familiares, amigos, empleos– que han vivido la experiencia personal de ser vigiladas y que pueden hablar de los efectos que la vigilancia ha tenido en sus vidas, de las oportunidades de viaje o de trabajo perdidos, de los familiares implicados o amenazados, y de la sensación de violación y el miedo que engendra ser observado. Son historias que muestran el profundo costo humano de las leyes y prácticas que subvierten los derechos individuales en nombre de la seguridad nacional. También suelen ser historias que salen a la luz debido a que los individuos se dieron cuenta de que estaban siendo observados, a menudo porque la información obtenida por los vigilantes fue utilizada de una manera que dañó a estas personas –por entrar a una lista de exclusión aérea, prohibirle un cruce de frontera o, en casos extremos como el de Maher Arar, experimentando la entrega y la tortura.

Pero el caso *Re (X)* nos recuerda que mucha gente no sabrá nunca que está siendo observada, nunca sabrá que su privacidad está siendo tan profundamente invadida y, al final, puede que nunca llegue a ser detenida o acusada de un delito de terrorismo. Es bastante probable que haya muchos, muchos casos en los que la vigilancia sea errónea o esté injustificada –o, como en el caso *Re (X)*, se despliegue bajo órdenes judiciales basadas en hechos manipulados– y que no llamen la atención ni generen ninguna protesta porque quienes están siendo vigilados permanecen en la invisibilidad.

Edward Snowden ha descrito los mecanismos de Canadá para regular y controlar la vigilancia de sus agencias de inteligencia como “uno de los marcos de supervisión más débiles de cualquier agencia de inteligencia occidental del mundo”.[11] Si no hubiera sido por un juez que defendió la integridad de la orden judicial secreta, los canadienses todavía no sabrían que dos de sus conciudadanos habían sido arrastrados por la red de vigilancia digital transnacional. El juez Mosley quiso revisar su decisión de emitir la orden judicial solo porque estudió el informe anual del comisionado de la CSE, en el que daba a entender que había algo en la forma en que la CSE estaba colaborando con el CSIS que el Tribunal Federal necesitaba saber. Para entonces, habían transcurrido cuatro años desde la emisión de la orden original, y esa orden, establecida sobre la base de información engañosa, había servido como precedente para asegurar muchas otras órdenes similares.

> *Re (X)* nos recuerda que el secretismo que las agencias de inteligencia necesitan para realizar su trabajo debe complementarse con mecanismos apropiados para rendir cuentas y proteger a la población frente a abusos y errores.

conclusión

El juez Mosley defendió la ley y a los canadienses que están protegidos por ella. Su valentía e iniciativa ayudaron a visibilizar y salvaguardar a algunos de los sujetos invisibles de la vigilancia de seguridad. Desafortunadamente, el conocimiento no ha conducido a la reforma en Canadá. En lugar de responder al caso *Re (X)* y los problemas que plantea mediante la revisión y restricción de la autoridad legal de las agencias y agentes de seguridad canadienses para actuar fuera de Canadá, el gobierno aprobó dos proyectos de ley, el C-44 y el C-51, que amplían la autoridad de los organismos de inteligencia.

El proyecto C-51, la más radical de estas medidas, se introdujo en enero de 2015 y recibió sanción efectiva en junio siguiente; una progresión muy rápida para un proyecto de ley que hace grandes cambios a la ley de seguridad nacional de Canadá. En el caso particular de los términos de vigilancia, la ley C-51 permite un aumento exponencial del intercambio de información entre organismos e instituciones gubernamentales y potencialmente también con poderes extranjeros, sin reforzar las medidas de transparencia. Además da al CSIS nuevos poderes para llevar adelante acciones encubiertas, incluso acciones que van en contra de las leyes internacionales, una vez más, sin supervisión adicional. Que el proyecto de ley haya sido aprobado tan rápidamente es desconcertante dada la intensidad de las reservas y críticas recibidas, no solo por parte de la sociedad civil, sino por expertos en derecho jurídico y civil, prominentes funcionarios públicos, académicos, antiguos jueces del Tribunal Supremo y ex primeros ministros de Canadá, y dado el hecho de que el apoyo público pasó de una mayoría a favor cuando se introdujo el proyecto de ley, a una mayoría en contra cuando las características de la nueva ley se difundieron. La CCLA fue activa en los debates en torno a la ley C-51, argumentando que es fundamentalmente defectuosa e inconstitucional en secciones específicas, y que no hay ninguna evidencia de que los grandes cambios que introduce para distintos poderes de inteligencia –incluyendo posibilidades ampliadas de vigilancia– sean siquiera necesarios.[12] La CCLA se centra ahora en prevenir que esta legislación sea utilizada para privar a las personas de sus derechos, protegidos en nuestra *Carta de Derechos y Libertades*, y ha presentado una solicitud ante la Corte Superior de Ontario para que ciertas disposiciones de la ley antiterrorista C-51 de 2015 sean declaradas inconstitucionales.

Ciertamente no debería haber ninguna ampliación de las competencias digitales de vigilancia e intercambio de inteligencia en Canadá sin estructuras nuevas y más eficaces de supervisión. *Re (X)* nos recuerda que el secretismo que las agencias de inteligencia necesitan para realizar su trabajo debe complementarse con mecanismos apropiados para rendir cuentas y proteger a la población frente a abusos y errores. Los informes anuales cuidadosamente redactados por órganos consultivos, y de vez en cuando complementados por

documentos censurados obtenidos por periodistas en respuesta a una petición FOIA, simplemente no son suficientes. *Re (X)* también pone de relieve la necesidad de que los tribunales y otras autoridades de supervisión tengan acceso suficiente a la información sobre las operaciones de inteligencia en general y sobre las peticiones específicas de vigilancia, con el fin de comprobar la veracidad de las declaraciones y afirmaciones que hacen los servicios de seguridad en las solicitudes de vigilancia. En la medida en que sea posible, esa información debe hacerse pública, y se debe desafiar la retórica oficial, que a menudo intenta convencernos de que cuanta más información se recolecta y se comparte, más seguros estaremos, y contrarrestarla con la advertencia de que es peligroso para nosotros compartir demasiado con las personas equivocadas. Debemos asegurarnos de que la promesa de que nuestras agencias de inteligencia actúan proporcional y legalmente esté respaldada por leyes fuertes y apropiadas que rijan la recolección e intercambio de información. Por último, debemos asegurarnos de que todas las leyes que rigen a nuestras agencias nacionales de seguridad y sus actividades reflejen –no rechacen– nuestras garantías del derecho humano al debido proceso, a la intimidad y a la dignidad de cada individuo.

notas

-

1. Para una descripción detallada de las complejidades legales de las sentencias, véase Craig Forcese, "Triple Vision Accountability and the Outsourcing of CSIS Intercepts" (6 de diciembre, 2013). Disponible en: http://craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html [28/10/2016].
2. Comité de Revisión de Inteligencia de Seguridad. *SIRC Annual Report 2012–2013: Bridging the Gap*, p. 18. Disponible en: http://www.sirc-csars.gc.ca/anrran/2012-2013/index-eng.html [28/10/2016].
3. Robert Décary. *Communications Security Establishment Commissioner: 2012-2013 Annual Report*. Disponible en: https://www.ocsec-bccst.gc.ca/s21/s46/s18/eng/2012-2013-annual-report [28/10/2016]. Nótese que la Agencia de Seguridad en las Comunicaciones (CSE) se llamaba entonces Agencia de Seguridad en las Comunicaciones Canadá (CSEC).
4. 2013 FC 1275, párr. 97.
5. Agencia Nacional de Seguridad/nota de información del Servicio Central de Seguridad, "Relación de Inteligencia de la NSA con la Agencia de Seguridad en las Comunicaciones (CSEC)" (2013). Disponible en el Archivo Snowden en: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH1ee3.dir/doc.pdf [28/10/2016].
6. Canadá, Parlamento, Senado, Comité del Senado sobre Seguridad y Defensa [SSCNSD] (2012). Transcripción de Procedimientos. 41° Parl., 1° ses. Meeting No. 15. Disponible en: http://www.parl.gc.ca/Content/SEN/Committee/411/secd/10ev-49784-e.htm?Language=E&Parl=41&Ses=1&comm_id=76 [28/10/2016].
7. Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23), Sección 21. Disponible en: http://laws.justice.gc.ca/eng/acts/C-23/ [28/10/2016].
8. National Defence Act (R.S.C., 1985, c. N-5), Sección 273.64 (2)(a). Disponible en: http://laws.justice.gc.ca/eng/acts/n-5/fulltext.html [28/10/2016].
9. "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian* (21 de junio, 2013). Disponible en: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [28/10/2016].
10. "CSEC commissioner calls for safeguards on Five Eyes data sharing", *The Canadian Press* (14 de julio, 2014). Disponible en: http://www.cbc.ca/news/politics/csec-commissioner-calls-for-safeguards-on-five-eyes-data-sharing-1.2706911 [28/10/2016].
11. Edward Snowden. Entrevista de CBC News video (4 de marzo, 2015). Disponible en: http://www.cbc.ca/news/canada/edward-snowden-says-canadian-spying-has-weakest-oversight-in-western-world-1.2981051 [28/10/2016].
12. En apoyo a la CCLA en los debates sobre la Ley C-51, ocho miembros de INCLO firmaron una carta conjunta que fue presentada a la Comisión del Senado el 23 de abril, para mostrar apoyo internacional a la posición de la CCLA y hacer hincapié en la importancia de la Ley Internacional de Derechos Humanos y los derechos a la privacidad en las iniciativas mundiales antiterroristas.

Un vistazo a la vigilancia en Canadá

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
Sí.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No (académicos, la sociedad civil e individuos los discutieron pero el gobierno aprobó una legislación ampliando los poderes de vigilancia).

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional gubernamental se han reducido, han aumentado o ninguna de los dos opciones?
Han aumentado.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
La legislación más reciente bajo el anterior gobierno canadiense (proyecto de ley C-51, Ley contra el terrorismo, 2015) amplió los poderes de vigilancia; a partir de octubre de 2015 tenemos un nuevo gobierno cuya plataforma sugiere que puede reducir estos poderes, pero aún no está del todo claro qué va a hacer, ya que también apoyó la legislación original.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia del gobierno, ¿dicha legislación impondría nuevos controles estructurales?
Hay indicios de que lo hará, sí.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No. Sin embargo, la CCLA tiene un recurso de inconstitucionalidad activo ante la Corte Superior de Justicia de Ontario.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
Menos.

El caso AMIA, el poder judicial y los servicios de inteligencia

5
ARGENTINA

Una imagen de las ruinas que quedaron después del atentado a la AMIA en Buenos Aires el 18 de julio de 1994.
Foto: Julio Menajovsky

ARGENTINA

El caso AMIA, el poder judicial y los servicios de inteligencia

el caso

En la mañana del 17 de julio de 2015, sobre un pequeño escenario montado en una plaza del centro de Buenos Aires, un hombre y una mujer leen 85 nombres. Después de cada nombre, las personas reunidas en el lugar gritan "¡Presente!". Detrás, la rutina diaria del Palacio de Justicia de la Nación sigue su curso: los automóviles tocan bocina, los oficinistas entran y salen de los edificios.

Veintiún años antes, a las 8.42 am del 18 de julio de 1994 –en un día que había comenzado muy parecido a este– una bomba terrorista explotó en el centro comunitario de la Asociación Mutual Israelita Argentina (AMIA). El edificio de seis pisos se derrumbó en una montaña de escombros. Ochenta y cinco personas perdieron la vida y 300 resultaron heridas: trabajadores, gente haciendo mandados, transeúntes, jóvenes y ancianos. ¿Por qué? ¿Por acción de quiénes? ¿Cómo? La investigación judicial oficial sobre el ataque terrorista más grave de la historia argentina se ha extendido por más de dos décadas, y aún no arrojó respuestas.

Incluso después del regreso a la democracia en la Argentina, la Secretaría de Inteligencia del Estado (SIDE) y su sucesora, la Secretaría de Inteligencia, existían en las sombras, operando de forma encubierta; nadie explicaba lo que hacían, ni qué sabían o no sabían exactamente. Los agentes estatales y para-estatales utilizaban identidades falsas. Sus agencias recogían datos sobre los ciudadanos argentinos, en algunos casos pertinentes y en otros meros chismes, sin supervisión alguna. Gastaban sus presupuestos secretos sin rendir ningún tipo de cuentas; toda una estructura dedicada a servir a propósitos políticos. Intervenían teléfonos de hombres de negocios, periodistas, funcionarios y miembros de la oposición, produciendo información que los funcionarios políticos utilizaban para desacreditar a sus adversarios, a menudo con la participación de periodistas influyentes y medios de comunicación. Y cuando el tráfico de información no era suficiente, los agentes de la SIDE tenían acceso a fondos reservados para el soborno y el tráfico de influencias, con el fin de torcer las decisiones a su voluntad.

Las agencias de inteligencia también se las arreglaron para dominar el sistema judicial, en particular durante la década de 1990. Los tribunales eran tan dependientes de la información de los servicios de inteligencia que la relación entre el poder judicial y la comunidad de inteligencia se invirtió: más que un colaborador en las investigaciones criminales, la Secretaría de Inteligencia se adueñó de los procesos judiciales más relevantes, que incluyeron casos de corrupción política y empresaria y delitos graves que involucraban a organizaciones complejas. Al igual que en el ámbito político, los vínculos entre los servicios de inteligencia y el poder judicial se consolidaron a través de sobornos procedentes de los fondos reservados de la SIDE.

Esta red de relaciones que vinculaban al sistema político, el poder judicial, el Ministerio Público Fiscal y el sistema de inteligencia estaba bien consolidada en el momento en que la Argentina sufrió dos ataques terroristas devastadores: un atentado el 17 de marzo de 1992 en el que una camioneta explotó en la Embajada de Israel en Buenos Aires, y mató al menos a 22 personas e hirió a más de 350, y, dos años más tarde, el aún más letal atentado a la AMIA.

La primera investigación judicial del atentado a la AMIA fue manejada por el juez federal de instrucción Juan José Galeano. Durante los cruciales primeros meses, su trabajo estuvo plagado de irregularidades; entre las más graves, el hecho de que la SIDE participara en la investigación. Y para mediados de 1996, dos años después del ataque, su trabajo todavía no había arrojado ningún resultado significativo, ni tampoco la investigación paralela sobre el atentado a la Embajada israelí. La población se impacientaba: conformada poco después del atentado a la AMIA, una agrupación llamada Memoria Activa comenzó a reunirse todos los lunes frente al Palacio de Justicia para leer los nombres

Pocos días después del atentado a la AMIA, más de 150.000 personas se reunieron bajo la lluvia en la Plaza de los Dos Congresos de Buenos Aires para condenar el ataque terrorista, el 21 de julio de 1994. Foto: Eduardo Longoni

de las 85 personas que habían muerto en el ataque, y su demanda de verdad y justicia fue consiguiendo el apoyo cada vez más fuerte de los argentinos. Tanto el juez Galeano como el gobierno necesitaban un chivo expiatorio.

De manera que el juez y la SIDE conspiraron para construir una explicación basada en declaraciones de Carlos Telleldín, un vendedor de automóviles que había sido detenido por ser el último propietario registrado de una camioneta que se encontró en medio de los escombros de la AMIA. Telleldín, en la cárcel desde 1994, había sido acusado de entregar el vehículo a los terroristas, pero hasta mediados de 1996 no había revelado la identidad de esas personas. La información proporcionada por los servicios de inteligencia extranjeros a los investigadores judiciales tras el ataque sugirió que este había sido orquestado por la República Islámica de Irán. Pero en julio de 1996, pocos días antes del segundo aniversario del atentado, Telleldín declaró ante el juez Galeano que le había dado la camioneta a un grupo de policías de la provincia de Buenos Aires. Le dijo que esos agentes solían extorsionarlo y que les había entregado el vehículo a cambio de protección para su empresa ilegal de venta de vehículos robados. Galeano ordenó la detención de 15 agentes de policía, entre ellos Juan José Ribelli, jefe de la Brigada de Investigación del municipio de Lanús de la provincia de Buenos Aires. En el segundo aniversario de la explosión, con esta “conexión local” tras las rejas, las autoridades estatales aseguraron a la sociedad argentina que la célula terrorista responsable de la bomba había sido desmantelada. Debido a que las fuerzas policiales de la provincia de Buenos Aires eran conocidas por su violencia y sus vínculos con redes ilegales, la historia era creíble.

Pero menos de un año después, en abril de 1997, los medios argentinos emitieron un video de una reunión entre el juez Galeano y Telleldín. Allí, los dos parecían discutir la compra de los derechos de autor de un libro que supuestamente Telleldín estaba escribiendo. Después de la divulgación del video, ambos negaron que la conversación se refiriese a un pago por el último testimonio de Telleldín. A fines de 2001, con la declaración de Telleldín como única prueba, comenzó el juicio contra los policías acusados de participar en el ataque a la AMIA.

En 2003, nueve años después del atentado y durante los primeros días del gobierno de Néstor Kirchner, un sector de la Secretaría de Inteligencia reveló información que corroboraba que varios agentes habían sido parte de una operación de soborno relacionada con la investigación del atentado a la AMIA, y que el mismo día en que Telleldín había acusado por primera vez a la policía en 1996, empleados de inteligencia se habían reunido con su esposa en un banco. En ese momento, el gobierno tomó una decisión política fundamental: emitió un decreto relevando a los agentes

Un hombre toca el shofar, el antiguo cuerno musical judío, durante un acto conmemorativo de Memoria Activa en Buenos Aires el 17 de julio de 2015. Foto: Santiago Cichero

> “La investigación judicial oficial sobre el ataque terrorista más grave de la historia argentina se ha extendido por más de dos décadas, y aún no arrojó respuestas.”

de inteligencia de su deber de mantener sus actividades en secreto, y permitió así que en el juicio en curso declararan que se había utilizado dinero secreto de la agencia de inteligencia para pagar a Telleldín a cambio de que acusara a agentes de policía de la provincia de Buenos Aires como la “conexión local” del ataque. Los agentes de inteligencia declararon que en julio de 1996, con el conocimiento del entonces presidente Carlos Menem y a petición del juez Galeano, Hugo Anzorreguy, por entonces secretario de Inteligencia, ordenó a sus subordinados entregar 400.000 dólares a la esposa de Telleldín en pago por la declaración de su marido.

El dinero provino de fondos reservados que la SIDE administraba sin ningún tipo de supervisión o transparencia, y la naturaleza secreta del presupuesto permitió que se utilizara para fabricar una historia que descarriló la investigación de los hechos durante años. Pero ahora las consecuencias de una práctica notoriamente común –el uso de los fondos reservados para comprar o fabricar información– quedó expuesta y a la vista de todos. El pacto entre el gobierno argentino, la Secretaría de Inteligencia del Estado, agencias de inteligencia extranjeras, el juez Galeano y Telleldín había producido una pista falsa en la investigación, desviándola de pistas legítimas y poniendo la legitimidad y la legalidad de toda la investigación del atentado en tela de juicio.

El pago de un soborno que se había decidido en el nivel político más alto no era la única ilegalidad cometida durante la investigación judicial del juez Galeano. En los hechos, la SIDE y un sector de la policía federal eran los dueños de la investigación; agentes de inteligencia llevaron a cabo registros e interrogatorios de testigos, y el juez y los fiscales respaldaron sus acciones. La SIDE también se involucró en escuchas telefónicas: durante un año intervino los teléfonos de las embajadas de Cuba e Irán en Buenos Aires sin una orden judicial, así como las líneas telefónicas pertenecientes a otras personas bajo investigación. Aunque agentes de la SIDE han admitido desde entonces que en efecto hacían esas escuchas ilegales, las grabaciones en casete de las conversaciones nunca salieron a la superficie.

En octubre de 2004, el tribunal a cargo del juicio contra Telleldín, Ribelli y los otros agentes de policía dictaminó que las acusaciones contra la “conexión local” se basaban en irregularidades judiciales, declaraciones compradas y el uso ilegal de los recursos del Estado. Los jueces determinaron que la investigación no había tenido como fin descubrir la verdad, sino más bien legitimar un engaño construido por altos funcionarios de los diferentes poderes del Estado; que era “un armado al servicio de políticos inescrupulosos”. Todos los acusados fueron absueltos y el tribunal ordenó una nueva investigación, declarando nula toda la investigación realizada hasta ese punto. Al año siguiente, los fiscales que habían participado en la investigación renunciaron y el juez Galeano fue removido de su cargo por sus actos ilegales; estos ex funcionarios están en juicio actualmente. Habían pasado diez años desde el atentado, y la única respuesta a las demandas de justicia había sido la exposición de una poderosa maniobra de encubrimiento.

Después de que el juez Galeano fuese removido de su cargo, el presidente Néstor Kirchner designó a Alberto Nisman para presidir una nueva investigación como fiscal federal especial. Pero Nisman no era nuevo en el caso: había estado en el equipo de investigación inicial que había colaborado con la Secretaría de Inteligencia, y él también basaría gran parte de su investigación en la información proporcionada por la Secretaría, la mayoría de la cual no se podría utilizar como prueba en los tribunales. Por caso, en 2005 Nisman anunció que había identificado al conductor suicida de la camioneta; una afirmación que nunca fue respaldada ni demostrada en los procedimientos judiciales.

En 2006, dos años después de hacerse cargo de la investigación y 12 años después del atentado a la AMIA,

el fiscal Nisman emitió una acusación de 800 páginas acusando a ocho altos ex funcionarios iraníes, entre ellos el ex presidente Ali Akbar Rafsanjani y el ex ministro de Inteligencia Ali Fallahian, de orquestar el ataque. Un año más tarde INTERPOL emitió un "alerta roja" para cinco de los ocho funcionarios acusados e instruyó a los Estados miembros a detenerlos para que pudieran ser enviados a la Argentina para testificar en la corte.[1] El gobierno iraní se negó a entregar a sus ciudadanos a la justicia argentina, lo que originó un callejón sin salida en el caso, que se prolongó durante varios años.

Luego, en marzo de 2012, los gobiernos de la Argentina e Irán firmaron un Memorándum de Entendimiento para crear una comisión que permitiese a los jueces argentinos viajar a Teherán para realizar entrevistas, y posiblemente incluso entrevistar a los acusados nombrados, pero que no aseguraba que estos se presentarían ante un tribunal argentino. En los diez años que transcurrieron desde el momento en que Nisman asumió como fiscal especial en 2004 hasta finales de 2014, la investigación había estado casi en un punto muerto. Sin embargo, el 14 de enero de 2015, el fiscal presentó una denuncia alegando que el Memorándum de Entendimiento era una maniobra de la por entonces presidenta de la Argentina, Cristina Fernández de Kirchner, y otros funcionarios para encubrir el atentado y proteger a los iraníes. La acusación se basaba en intervenciones de teléfonos de personas que no tenían un papel central en el sistema político nacional; las conversaciones grabadas supuestamente implicaban un acuerdo para beneficiar a los iraníes. Nisman iba a presentarse ante el Congreso de la Nación el lunes 19 de enero para exponer los detalles de su denuncia a los legisladores del partido gobernante y de la oposición. El fin de semana, según informaciones que después aparecerían en la prensa, Nisman intentó sin éxito ponerse en contacto con la persona que, como jefe operativo de los servicios de inteligencia hasta diciembre de 2014, había tenido el control de la investigación de la AMIA durante años y había facilitado la intervención telefónica en la que se basó la acusación contra el gobierno de Fernández de Kirchner. A última hora de la tarde del domingo 18 de enero, Nisman fue encontrado muerto en su domicilio con una bala en la cabeza.

La investigación judicial sobre la muerte de Nisman permanece abierta y, por el momento, la teoría de que la muerte fue un suicidio prevalece. Mientras tanto, la denuncia de Nisman contra la ex presidenta argentina no ha prosperado: dos autoridades judiciales determinaron que no había pruebas suficientes para abrir un caso judicial, dado el hecho de que no se podían sacar conclusiones a partir de las conversaciones grabadas. La muerte de Nisman y el contexto en el que se produjo tuvieron un impacto significativo en la opinión pública y, después de años de una lucha a menudo solitaria por parte de las víctimas, el caso AMIA ha pasado a convertirse en un tema clave de la agenda política.

En agosto de 2015, comenzó en Buenos Aires el juicio para determinar las responsabilidades penales individuales de los funcionarios políticos y judiciales en el encubrimiento del atentado a la AMIA. Las víctimas y amplios sectores de la opinión pública argentina esperan que el juicio finalmente revele la verdad de lo sucedido.

el contexto

La investigación judicial irregular puede explicarse por la debilidad del sistema de investigación criminal de la Argentina, el funcionamiento histórico oscuro e ilegal de los servicios de inteligencia y el hecho de que a lo largo de los años los políticos dependieron de la matriz de relaciones espurias entre los servicios de inteligencia y el sistema judicial federal.

Al sostener una historia fabricada, el Estado argentino no estuvo obligado a dar seguimiento a otras pistas. Por ejemplo, el tribunal nunca profundizó en la hipótesis de que un grupo de ciudadanos sirios con supuestas conexiones con el entonces presidente Carlos Menem estuvo involucrado en el ataque. Ni siquiera investigó si los servicios de inteligencia tenían sospechas o indicios previos al atentado a la AMIA de que un ataque terrorista podría tener lugar en la Argentina. Además, la hipótesis de que los servicios de inteligencia locales tenían información sobre otro posible ataque no fue bien investigada. En 2004, diez años después del atentado, se reveló que la presión internacional también había desempeñado un papel en el encubrimiento. Cables diplomáticos de la Embajada Argentina en Israel, emitidos solo unas horas después de la explosión, mostraron que un funcionario del gobierno de Yitzhak Rabin había viajado inmediatamente a la Argentina para coordinar una "versión unificada" del atentado, por el que se culpaba a Irán por el ataque.[2]

Desde un punto de vista más amplio, también se plantea la cuestión de la motivación detrás del encubrimiento. En las dos décadas desde el ataque, los cálculos geopolíticos, las relaciones de la Argentina con otros países –Siria e Irán entre ellos– y la política interna de cada momento histórico durante el transcurso de la investigación han conspirado para ocultar la verdad.

El caso AMIA ha puesto de relieve las peligrosas conexiones subterráneas entre los servicios de inteligencia de la Argentina y sus esferas políticas y judiciales, y subrayó la importancia que tiene el control de las operaciones de inteligencia y vigilancia para el estado de derecho y la democracia.

En 1999 Memoria Activa, representada por el Centro de Estudios Legales y Sociales (CELS) y el Centro por la Justicia y el Derecho Internacional (CEJIL), denunció a la Argentina ante la Comisión Interamericana de Derechos Humanos (CIDH) en relación con el atentado a la AMIA por violación del derecho a la vida y a la integridad física. Citando las irregularidades cometidas por el poder judicial, la policía federal y los servicios de inteligencia también presentaron una denuncia contra el país por violar su obligación de realizar una investigación efectiva. En marzo de 2005 el Estado argentino reconoció su responsabilidad: "existió un incumplimiento de la función de prevención por no

> “También es necesario que el sistema político, el poder judicial y otros poderes, incluyendo los medios de comunicación, reconozcan y confronten el tóxico y a menudo irreparable impacto que el uso irresponsable y arbitrario de los servicios de inteligencia ha tenido en la democracia y la protección de los derechos humanos.”

haber adoptado las medidas idóneas y eficaces para intentar evitar el atentado, teniendo en cuenta que dos años antes se había producido un hecho terrorista contra la embajada de Israel en Argentina”. En el mismo documento, también reconoció que “existió encubrimiento de los hechos y medió incumplimiento grave y deliberado de la función de investigación adecuada del ilícito, lo cual produjo una clara denegatoria de justicia”. El Estado se comprometió a reformar sus organismos de inteligencia.[3]

Sin embargo, durante más de diez años, el gobierno argentino no ha adoptado medidas para cumplir su compromiso con la CIDH de transparentar el funcionamiento interno de los servicios de inteligencia. En lugar de ello, las autoridades políticas y judiciales siguieron tolerando el poder encubierto de los agentes de inteligencia con el fin de beneficiarse de los despojos de ese poder. Las relaciones irregulares entre jueces, abogados, grupos de presión y agentes de inteligencia afectaron el funcionamiento del sistema judicial federal, lo que posibilita alianzas entre entidades políticas (tanto del gobierno como de la oposición), empresas, sindicatos y sectores de la iglesia, entre otros. El potencial de extorsión y desestabilización continuó siendo enorme.

Después de la muerte de Nisman –y en medio de las sospechas de que esta red subterránea estaba tratando de desestabilizar al gobierno en respuesta a una reciente reorganización de la agencia de inteligencia– la presidenta Fernández de Kirchner decidió llevar a cabo una reforma del sistema de inteligencia. A fines de enero de 2015 se envió un proyecto de ley al Congreso para disolver la Secretaría de Inteligencia y crear la Agencia Federal de Inteligencia (AFI) en su lugar. El proyecto de ley contenía elementos valiosos, como la exigencia de que los cargos de director y subdirector de la AFI fuesen aprobados por el Senado, y la colocación de la oficina encargada de las escuchas telefónicas bajo la autoridad de la Procuraduría General de la Nación. Sin embargo, la propuesta inicial no incluía los tipos de cambios sustanciales necesarios para abordar los temas críticos que contribuyeron al fracaso de la investigación del atentado a la AMIA, como poner fin al secreto absoluto del sistema, replantear los criterios para la clasificación y desclasificación de la información, establecer la supervisión de los fondos reservados e imponer límites a la participación de los agentes de la AFI en las investigaciones criminales.

Fuertes críticas y sugerencias concretas del CELS[4] y otras organizaciones dieron lugar a importantes modificaciones al proyecto de ley que finalmente fue aprobado por el Congreso. Con el fin de eliminar las fronteras borrosas y las relaciones impropias entre funcionarios judiciales y espías, la ley prohibió a la nueva agencia de inteligencia participar en investigaciones criminales en el lugar de la policía y de las fuerzas de seguridad. Para abordar el problema del excesivo secretismo, el principio general del secreto como regla del trabajo de inteligencia fue reemplazado por el requisito de que solo debe mantenerse si está en juego la integridad física de un analista o de valores sociales fundamentales como la vida democrática (si bien, y en

Un hombre con un shofar, el antiguo cuerno musical judío, durante un acto conmemorativo de Memoria Activa en Buenos Aires el 17 de julio de 2015.
Foto: Santiago Cichero

una redacción imprecisa, se establece que el interés del Estado puede justificar la limitación de este principio, lo que podría dar lugar a denegaciones arbitrarias de acceso a la información).

Por otra parte, la nueva ley creó un mecanismo para desclasificar documentos y ofrecer a los ciudadanos acceso a la información. En el caso del presupuesto de inteligencia, se estableció que todos sus gastos son de carácter público y por lo tanto sujetos a la supervisión contemplada en las leyes sobre administración financiera. En el caso de que la publicación de los presupuestos pudiese afectar una operación de inteligencia en curso, la ley establece que dichos presupuestos pueden ser mantenidos en secreto pero deben ser registrados en documentos oficiales firmados por el director de la AFI y accesibles a la Comisión Bicameral encargada de supervisar a los organismos de inteligencia.

Esta reforma legislativa fue una iniciativa política importante para mejorar la legitimidad democrática de las agencias de inteligencia. Sin embargo, para que la reforma sea eficaz y los mecanismos de supervisión funcionen, los cambios deben ir acompañados por la voluntad del gobierno de habilitar y hacer cumplir el cambio.[5] En diciembre de 2015, un nuevo gobierno asumió la presidencia de la Argentina. Esta administración se enfrenta al reto de imponer firmemente este enfoque nuevo y transparente; la reorientación de los objetivos del sistema de inteligencia, su profesionalización y la realización de acciones dirigidas a la implementación de las reformas que mejoren la transparencia del sistema deben ser prioridades para el nuevo gobierno.*

Al mismo tiempo, así como la Argentina ha aprendido en sus esfuerzos para hacer frente a las violaciones de los derechos humanos en el pasado, también es necesario que el sistema político, el poder judicial y otros poderes, incluyendo los medios de comunicación, reconozcan y confronten el tóxico y a menudo irreparable impacto que el uso irresponsable y arbitrario de los servicios de inteligencia ha tenido en la democracia y la protección de los derechos humanos.

Hasta ahora hemos visto retrocesos bajo la nueva administración. El director designado de la AFI es un hombre de negocios cercano al presidente que no tiene experiencia conocida en asuntos de inteligencia. Muchos de los nuevos funcionarios de alto rango de la agencia tienen estrechos vínculos con los responsables de las irregularidades y abusos mencionados anteriormente. La primera medida concreta que el presidente Mauricio Macri tomó sin consultar al Congreso fue trasladar la unidad de intervención telefónica de la Oficina del Procurador General (con quien Macri mantiene una puja política) a la esfera de la Corte Suprema. Esto ha alimentado los temores de que ex agentes de la SIDE pudieran ser llamados para realizar escuchas telefónicas debido a la falta de personal capacitado en la corte. En el mes de mayo de 2016, el presidente Macri emitió una orden

ejecutiva que invalidó las normas que se pusieron en vigor durante 2015 y que aclaraban qué tipo de gastos podrían ser clasificados y cuáles no, y establecían un procedimiento de registros para los gastos reservados para facilitar su supervisión y revisión futura. Esta orden ejecutiva desconoce el compromiso firmado entre el Estado argentino y las familias de las víctimas de la AMIA y se remonta al antiguo sistema de administración de fondos reservados que fue utilizado por la SIDE para comprar testigos. En respuesta a una nota enviada por el CELS y Memoria Activa a la Jefatura de Gabinete de Ministros, el director de la AFI, Gustavo Arribas, respondió con evasivas y se negó a revelar el sistema utilizado actualmente para reportar el uso de los fondos reservados. El Estado argentino, en respuesta a una pregunta formulada por el Consejo de Derechos Humanos de la ONU, reconoció que la falta de un registro y de un sistema de supervisión de los gastos de inteligencia podría ser considerado "un retroceso en materia de transparencia".

conclusión

Sin una base de principios democráticos o supervisión, la capacidad de los servicios de inteligencia para hacer daño fue enorme; de hecho, el ataque terrorista más grave de la historia argentina se mantiene hasta nuestros días sin explicación y sin castigo.

El funcionamiento opaco de los servicios de inteligencia afectó durante décadas a muchas capas del sistema político: las fuerzas de seguridad, el sistema judicial y diversas esferas de gobierno. A menudo justificadas como necesarias para mantener y consolidar la gobernabilidad, estas relaciones solo sirvieron para socavar la democracia. El caso de la AMIA es un ejemplo concreto de las graves consecuencias de esos pactos ilegítimos. Es esencial que los poderes ejecutivo, legislativo y judicial y las organizaciones de la sociedad civil actúen juntos para construir sistemas democráticos fuertes que gobiernen las estructuras de seguridad e inteligencia y eviten que se vuelvan autónomas en sus objetivos y operaciones. Es fundamental que estas instituciones trabajen juntas para garantizar la responsabilidad por las actividades de los organismos de inteligencia y evitar cualquier retroceso en las reformas ya aplicadas.

Un viernes de julio de 2016 por la mañana, después de la lectura tradicional de los 85 nombres de quienes murieron hace 21 años en la explosión, la miembro de Memoria Activa, Diana Malamud, cuyo marido murió en el atentado a la AMIA, tomó el micrófono en el escenario improvisado ante el Palacio de Justicia:

Durante 21 años estuvimos y seguimos en búsqueda de una verdad que aún desconocemos: quiénes decidieron el atentado que asesinó a nuestros familiares, quiénes lo ejecutaron, quiénes los apoyaron, quiénes los ocultaron, quiénes los encubrieron. De esta última pregunta, quiénes los encubrieron, conocemos la respuesta.

Impulsadas en gran medida por las consecuencias de la muerte del fiscal Nisman, por fin se han adoptado algunas medidas concretas para que quienes conspiraron para crear una falsa narrativa de las responsabilidades del atentado rindieran cuentas. Después de años de retrasos y resistencias por parte del poder judicial, el 6 de agosto de 2015 un tribunal de Buenos Aires escuchó los argumentos iniciales en el juicio de quienes están acusados de orquestar el encubrimiento, entre ellos el ex presidente Carlos Menem, el juez Galeano y altos funcionarios de inteligencia. Después de un año de juicio, algunas verdades han comenzado a salir a la luz. Los testimonios de los policías federales y empleados de la corte han confirmado que la llamada "pista siria", que conducía a personas vinculadas a Menem, no se investigó. Telleldín mismo reconoció que el dinero que recibió de la SIDE fue para incriminar al grupo de Ribelli. Los acusadores en el primer y frustrado juicio son hoy en día los acusados.

Las víctimas y toda la sociedad merecen respuestas.

notas

-

1. Los buscados por la INTERPOL son: el ex ministro de Inteligencia iraní, Ali Fallahian; el ex comandante de la Fuerza QUDS, el brazo de élite de la Guardia Revolucionaria de Irán, Ahmad Vahidi; el ex comandante de la Guardia Revolucionaria, Mohsen Rezai; el ex agregado cultural de la embajada de Irán en Argentina, Moshen Rabbani; y el ex tercer secretario de la embajada de Irán en Argentina, Ahmad Reza Asghari. El ex jefe de Asuntos Exteriores de Hezbolá, Imad Fayez Mughniyah, fue incluido en la lista original, pero el 12 de febrero 2008 su vehículo explotó mientras conducía por las calles de Damasco, Siria. Fuentes de los servicios de inteligencia afirmaron en un informe publicado por la revista *Newsweek* en marzo del año 2015 que el asesinato de Fayez Mughniyah fue coorganizado y ejecutado por agentes de inteligencia del Mossad y la CIA.
2. Los documentos fueron puestos de manifiesto por el periodista Horacio Verbitsky, presidente del consejo directivo del CELS, en su artículo "La InfAMIA", *Página/12* (18 de julio, 2004). Disponible en: http://www.pagina12.com.ar/diario/elpais/1-38318-2004-07-18.html [28/10/2016]. La llamada "pista iraní" y el posterior abandono de la pista siria eran convenientes tanto para el gobierno argentino como para los israelíes. En el caso de la Argentina, porque desviaba la investigación de un grupo de residentes sirios en el país con lazos económicos con la familia del presidente Menem. Al mismo tiempo, era útil para el gobierno de Rabin "dado que partidos oposición y algunos medios de prensa están utilizando el hecho para atacar duramente la política de paz gobierno Rabin", como se evidencia en los cables diplomáticos.
3. Decreto 812/05. Disponible en: https://www2.jus.gov.ar/amia/pdf/decreto_812.pdf [28/10/2016].
4. Documento de análisis presentado por el CELS cuando se anunció que un proyecto de ley para reformar el sistema de inteligencia estaba siendo enviado al Congreso (1 de febrero, 2015). Disponible en: www.cels.org.ar.
5. Análisis del CELS de la modificación introducida por el Senado al proyecto de ley para reformar el sistema de inteligencia (12 de febrero, 2015). Disponible en: www.cels.org.ar

   *Sin embargo, luego de la salida de la versión en inglés de este informe, el gobierno nacional cambió aspectos centrales de la ley de inteligencia. Entre las medidas más regresivas se encuentra la decisión de que los fondos vuelvan a ser secretos. Ver análisis del CELS en www.cels.org.ar y de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia en: www.iccsi.com.ar

Un vistazo a la vigilancia en la Argentina

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
No. La gran mayoría de la población desconoce las actividades de las agencias de inteligencia.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
Sí. Sin embargo, el debate se limita a pequeños grupos especialmente preocupados por las implicaciones de las revelaciones de Snowden.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Se han reducido, pero solo hasta cierto punto. La agencia nacional de seguridad ya no controla la oficina a cargo de las escuchas legales.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
Sí. A principios de 2015 el Congreso aprobó un proyecto de ley para disolver la antigua Secretaría de Inteligencia y crear un nuevo organismo. La legislación incorporó nuevas normas en pos de la transparencia y el acceso público a la información, y limitó los poderes del sistema de inteligencia.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
N/A.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
N/A.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí. Los tribunales están investigando varias denuncias penales contra agentes y ex agentes por espionaje ilegal, contrabando de equipos de comunicaciones y obstrucción de la justicia, entre otros delitos. En marzo de 2015 dos oficiales navales de alto rango fueron condenados a prisión con libertad condicional por haber ordenado inteligencia política ilegal.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No. (Sin embargo, en el caso "Halabi c/P.E.N." de 2009, la Corte Suprema de Argentina falló que una ley que obligaba a las compañías de comunicaciones a mantener los metadatos del tráfico de teléfono e internet afectaba el derecho a la privacidad y la declaró inconstitucional.)

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
No ha modificado su percepción. La población nunca ha confiado en las agencias de inteligencia de la Argentina.

De los pasillos del Parlamento a los cubículos de los cibercafés: el gobierno indio está observando

6
INDIA

Un cibercafé en Bangalore, Karnataka, India. Foto: Alamy/Latinstock

INDIA

De los pasillos del Parlamento a los cubículos de los cibercafés: el gobierno indio está observando

el caso

En 2008, el Parlamento de la India estaba en el momento más álgido de una batalla de nueve meses sobre un acuerdo de energía nuclear con Estados Unidos. Había mucho en juego: bajo los términos del acuerdo, la India abriría 14 de sus reactores atómicos civiles a las inspecciones internacionales y, a cambio, se le permitiría ampliar su programa nuclear civil sin firmar el Tratado de No Proliferación Nuclear.

El país estaba dividido y el clima político era tenso. El gobierno del primer ministro Manmohan Singh presionaba en favor del acuerdo, insistiendo en que mejoraría la situación de la India como superpotencia mundial, mientras que los críticos y la oposición cuestionaban las intenciones del gobierno de los Estados Unidos en la negociación y alertaban sobre el daño que el acuerdo podría provocar en las relaciones de larga data con otros aliados importantes, especialmente Irán. Los críticos, además, acusaban a Singh de corrupción y de jugar cartas sucias en sus esfuerzos para convencer a los legisladores de apoyar el acuerdo. Gritando "avergüéncese" y "ladrón", los opositores marcharon al Parlamento llevando bolsas de lona llenas de dinero para simbolizar lo que describían como un plan para comprar votos, y lograron forzar una convocatoria a un voto de confianza al gobierno de Singh. Singh sobrevivió a esa votación y, en julio de 2008, el Parlamento de la India aprobó el acuerdo nuclear por un margen muy delgado.[1]

Un año más tarde, en un incidente sin relación alguna, el periodista Saikat Datta notó que un automóvil sin señas particulares lo seguía cuando se dirigía a su casa desde su trabajo en Delhi. Trató de pasar por alto su preocupación, pero el mismo vehículo lo siguió al día siguiente. Así que Datta anotó el número de la matrícula y llamó a la policía, que le informó que el número era falso. Las fuerzas del orden interceptaron el vehículo y detuvieron al conductor y dos pasajeros, descubriendo que los hombres eran funcionarios de la Oficina de Inteligencia de la India.[2]

Para el periodista, no fue una gran sorpresa enterarse de que estaba siendo vigilado por la inteligencia de la India. Después de todo, Datta reporteaba principalmente sobre seguridad nacional y había estado observando de cerca a los servicios de inteligencia.

Sin inmutarse, Datta continuó siguiendo pistas de fuentes confidenciales y en la primavera de 2010 publicó una serie de artículos en la revista *Outlook* que revelaban que el gobierno indio estaba empleando una nueva tecnología de vigilancia para interceptar y grabar conversaciones telefónicas de móviles de la India.

Las fuentes de Datta revelaron numerosos casos en los que la Organización Nacional de Investigación Técnica del gobierno (NTRO) había escuchado conversaciones privadas de líderes políticos, burócratas y dignatarios extranjeros. En 2007, la NTRO interceptó y grabó una conversación entre el secretario general del Congreso, Digvijay Singh, y un político de Punjabi en relación con la posible participación de ese político en las siguientes elecciones. En otro caso, los espías de la NTRO grabaron una llamada telefónica entre el jefe de gobierno de Bihar, Nitish Kumar, y sus colegas en materia de financiación estatal.[3] Además, informó Datta, en los agitados meses anteriores a que se aprobara el acuerdo nuclear de 2008, la NTRO había interceptado y registrado las conversaciones móviles de una serie de políticos que se oponían al acuerdo, entre ellos Prakash Karat, secretario general del Partido Comunista de la India y uno de los líderes de más alto perfil en oponerse al acuerdo.[4]

En su serie de revelaciones, Datta declaró que la NTRO estaba utilizando un nuevo tipo de tecnología de vigilancia para interceptar esas conversaciones, así como conversaciones telefónicas privadas de muchos otros ciudadanos y residentes de la India. Según fuentes anónimas gubernamentales y documentos filtrados, la intervención de teléfonos fue posible gracias a dispositivos de interceptación pasiva de telefonía celular que el gobierno de la India

comenzó a importar desde Europa del Este en 2005. A principios de 2006, la NTRO probó la tecnología en el propio supervisor de la agencia, el entonces asesor nacional de seguridad, M. K. Narayanan. Se le pidió a Narayanan que hiciera una llamada a su secretaria, que los funcionarios de inteligencia interceptaron, grabaron y transcribieron. Narayanan, quien solo respondía al primer ministro, quedó impresionado con la nueva tecnología y decidió invertir en ella.

Esta forma de interceptación celular se conoce como GSM *off-the-air* y monitoreo CDMA (o *stingrays*), y está diseñada para apuntar a las dos redes móviles más comunes de la India.[5] La tecnología funciona interceptando llamadas y mensajes mientras estos viajan entre los teléfonos y torres de telefonía móvil, lo que permite a los interceptores escuchar y grabar las comunicaciones sin ayuda de los proveedores de telecomunicaciones.[6] Como un funcionario de inteligencia de alto rango dijo a Datta: "[El sistema] puede ser desplegado en cualquier lugar. No necesitamos mostrar ninguna autorización ya que no estamos interviniendo ningún número de teléfono en el intercambio, sino interceptando señales entre el teléfono y la torre de telefonía celular y grabándolas en un disco rígido. Si se hacen demasiadas preguntas, podemos quitar el disco y borrar la conversación. Nadie se entera".[7]

El trabajo de Datta mostró cómo la NTRO había utilizado esa tecnología para monitorear a los opositores políticos del gobierno de Singh, pero también reveló las formas en que el gobierno estaba usándola contra grandes sectores de la población de la India. Además de intervenir números individuales de teléfono, la tecnología permitió llevar a cabo una vigilancia masiva, incluyendo filtrarse en las comunicaciones de toda una región. En algunos casos, el gobierno indio usó la tecnología para intervenir en ciertas regiones geográficas sobre la base de sus características demográficas, étnicas o religiosas. Datta informó que la NTRO suele intervenir en barrios predominantemente musulmanes de ciudades como Delhi, Lucknow y Hyderabad, "sintonizando conversaciones aleatorias de los ciudadanos, en un intento de localizar terroristas".[8]

el contexto

El sistema indio de interceptación celular *off-the-air* es solo una de las muchas herramientas del régimen de vigilancia masiva cada vez más empoderado y opaco del gobierno.

Ese régimen se conoce como Sistema de Control Centralizado (CMS). El gobierno indio anunció en 2009 que estaba desarrollando un sistema electrónico de recolección de inteligencia que permitiría a las agencias supervisar todas las comunicaciones telefónicas y de internet en el país.[9] Se esperaba que el CMS, que fue diseñado para reemplazar el sistema más descentralizado y privatizado del pasado, estuviera en pleno funcionamiento en marzo de 2016.[10] Como informó Reuters, el CMS permite al gobierno "escuchar y grabar conversaciones telefónicas, leer correos electrónicos y mensajes de texto, monitorear publicaciones de Facebook, Twitter o LinkedIn y rastrear búsquedas en Google".[11] En efecto, el CMS le da al gobierno acceso directo a las comunicaciones de mil millones de abonados móviles y fijos de la India y de 108 millones de abonados a internet, pasando por alto a los proveedores de telecomunicaciones e internet.[12] Este sistema masivo de recolección de datos fue concebido, diseñado y hoy opera por completo sin la aprobación ni supervisión del Parlamento.

El CMS es impresionante en su alcance y falta de control, y funciona casi totalmente al margen de las leyes pertinentes de la India.

Históricamente, dos leyes importantes han limitado la capacidad del gobierno para interceptar comunicaciones: la Ley de Telégrafos de la India, de 1885, y la Ley de Tecnología de la Información, de 2000 y modificada en 2008. Ambas leyes permiten

> “CMS le da al gobierno acceso directo a las comunicaciones de mil millones de abonados móviles y fijos de la India y de 108 millones de abonados a internet (...) Este sistema masivo de recolección de datos fue concebido, diseñado y hoy opera por completo sin la aprobación ni supervisión del Parlamento.”

una vigilancia específica y limitada en el tiempo y requieren la autorización individualizada de cada solicitud de intervención, ya sea del ministro del interior o del secretario del departamento de tecnología de la información.[13]

La Ley de Telégrafos de la era colonial restringe la interceptación de las comunicaciones a los casos en los que se la utilice en respuesta a una emergencia pública o para proteger la seguridad pública. En estas circunstancias, al gobierno se le permitía interceptar y recoger datos en el interés de “la soberanía y la integridad de la India, la seguridad del Estado, las relaciones amistosas con Estados extranjeros u orden público, o para prevenir la incitación a la comisión de un delito”.[14]

A lo largo de la década de 1990, la tendencia se orientó hacia la reducción de los poderes de vigilancia que el gobierno reivindicaba bajo la Ley de Telégrafos. En 1996, la *People’s Union for Civil Liberties*, una organización india de libertades civiles, se alzó con una demanda para impugnar las leyes de vigilancia de la India con el argumento de que violaban el derecho a la privacidad de los ciudadanos indios. Si bien la Constitución de la India no establece ningún derecho específico a la privacidad, el poder judicial ha interpretado que otros derechos constitucionales, como el derecho a la vida y la libertad, protegen la privacidad individual. *La People’s Union for Civil Liberties* argumentó que los tipos de monitoreo de las comunicaciones que estaban permitidos bajo la Ley de Telégrafos y otras leyes de la India infringían esos derechos básicos. El Tribunal Supremo de la India acordó ampliar el derecho a la privacidad para incluir las comunicaciones, emitiendo una serie de directrices para las escuchas telefónicas legales que incluían el requisito de que toda vigilancia fuese autorizada por un secretario de origen federal o estatal. Las directrices tenían como objeto proporcionar garantías temporales contra la vigilancia intrusiva hasta que el Parlamento pudiese diseñar y poner en práctica la nueva legislación de privacidad que articulara la protección legal para las comunicaciones privadas. Esto nunca ocurrió.

En cambio, a lo largo de la década de 2000, el péndulo se apartó de la protección de la privacidad y hacia poderes aún más expansivos de vigilancia. La Ley de Tecnología de la Información (IT), modificada después de los ataques terroristas de noviembre de 2008 en Bombay, debilitó considerablemente incluso a la Ley de Telégrafos, de 130 años de antigüedad. La Ley IT más reciente no requiere un estado de excepción o una amenaza a la seguridad pública para activar la interceptación de comunicaciones, y amplía específicamente las categorías de justificaciones que el gobierno puede utilizar para “interceptar, supervisar o descifrar” información a incluir en “la investigación de cualquier delito”.[15] La Ley IT básicamente le da al gobierno central la capacidad ilimitada para determinar a quiénes se le aplicará, para acceder a toda su información privada y comunicaciones y para procesarlos.[16]

Militantes del Partido Comunista de la India levantan los brazos mientras gritan consignas durante una manifestación contra el acuerdo nuclear India-Estados Unidos en Nueva Delhi, India, el 18 de septiembre de 2007. Foto: Gurinder Osan/AP

La Ley IT encendió las alarmas de organizaciones de libertades civiles y privacidad de la India. Incluso preocupó a un grupo de expertos establecido por la Comisión de Planificación del Gobierno para crear un marco para una nueva ley de privacidad, que arribó a la conclusión, en un informe de 2012, de que la combinación de la vieja Ley de Telégrafos y la recién acuñada Ley IT había "creado un confuso régimen regulador no transparente, propenso al mal uso, y que no facilita una solución para las personas agraviadas".[17]

Por otra parte, si bien tanto la Ley del Telégrafo como la IT técnicamente exigen que la interceptación de las comunicaciones de los ciudadanos sea de duración limitada y específica, otras normas y reglamentos entran en contradicción directa o debilitan esas restricciones.[18] Por ejemplo, para operar en la India, las empresas de telecomunicaciones deben obtener licencias del Departamento de Telecomunicaciones; esos permisos requieren que los proveedores de telecomunicaciones permitan al gobierno tener acceso directo a todos los metadatos y el contenido de las comunicaciones, independientemente de si el gobierno tiene o no una orden. Lo que es más: los certificados expedidos por el Departamento de Telecomunicaciones restringen el cifrado masivo de información de los usuarios a 40 bits, un nivel extremadamente débil de cifrado. Dado que las redes GSM generalmente emplean un cifrado masivo fijo de 64 bits, los proveedores de la India a menudo eliminan por completo el cifrado, dejando las comunicaciones de los usuarios sin protección alguna, tanto del gobierno como de privados.[19]

Las empresas de telecomunicaciones no son las únicas empresas privadas obligadas a ayudar al gobierno en su vigilancia. Normativas establecidas en 2011 obligan a los cibercafés a recolectar registros detallados de la identidad, dirección y número de teléfono de cada cliente, así como su historial de navegación y la cantidad de tiempo que cada usuario pasa en internet. Esta información, que los cibercafés deben conservar durante un año, debe ser presentada al gobierno todos los meses.[20] Debido a que la mayoría de los indios acceden a internet exclusivamente a través de cibercafés, esta supervisión del uso *in situ* es para el gobierno una ventana abierta a las actividades expresivas privadas de un gran porcentaje de los ciudadanos del país.[21]

Estas licencias y acuerdos con empresas privadas le dan al gobierno la capacidad no solo de interceptar y grabar conversaciones telefónicas y mensajes, sino, en efecto, de acceder a todas las comunicaciones y actividades en internet, desde correos electrónicos a búsquedas en Google y contenidos en redes sociales.[22] Es claro que se están utilizando esos poderes: en los últimos años el gobierno ha detenido a numerosas personas que lo han criticado en las redes sociales y ha presionado cada vez más a los sitios web, incluyendo a Google y Facebook, para censurar la expresión y actividad de sus usuarios.[23]

Militantes del Partido Comunista de la India gritan consignas contra el gobierno durante una manifestación contra el acuerdo nuclear India-Estados Unidos en Nueva Delhi, India, el 27 de noviembre de 2007. Foto: Manish Swarup/AP

Darle a las entidades de vigilancia interna semejante acceso amplio y directo a las comunicaciones privadas y actividades de internet sería preocupante incluso si hubiese controles efectivos sobre las agencias de inteligencia y sobre el uso que hacen de sus poderes de vigilancia. Pero en la India, la falta de transparencia de estas agencias, junto con la ausencia casi absoluta de una supervisión judicial o independiente, pone a los ciudadanos y residentes en una situación especialmente vulnerable.

Al igual que la Ley de Telégrafos, la inteligencia interna de la India tiene raíces coloniales. En 1887 Gran Bretaña estableció la Oficina de Inteligencia de la India, diseñada para investigar distintos tipos de actividad criminal.[24] El organismo, creado por el poder ejecutivo, es ahora una de las al menos diez agencias del gobierno central autorizadas para interceptar las comunicaciones de los ciudadanos.[25] Las otras agencias de inteligencia, establecidas de manera similar por dictado ejecutivo, siguieron el modelo establecido por su antepasado colonial e ignoraron los requisitos constitucionales de aprobación parlamentaria.[26]

En la realidad, no existe ningún mecanismo legal en funcionamiento a través del cual la población pueda hacerle rendir cuentas al gobierno por las violaciones de su derecho a la privacidad (que no está explícitamente reconocido por la ley de la India), o por las leyes que oficialmente rigen las prácticas de vigilancia. En el marco del Sistema de Control Centralizado, no solo las agencias gubernamentales encabezan vigilancias sin autorización judicial, sino que no existe un mecanismo de compensación legal para que las personas denuncien la interceptación ilegal de sus comunicaciones. Lo máximo que una parte perjudicada puede hacer es presentar una demanda ante un tribunal, pero lograrlo es difícil por el extremo secreto que rodea las actividades gubernamentales de inteligencia, y el hecho de que ni el gobierno ni sus intermediarios, en particular las empresas de telecomunicaciones, tengan obligación legal alguna de dar aviso a los sujetos vigilados.[27]

Esta falta de transparencia se ve agravada por la Ley de Derecho a la Información, de 2005, la cual, a pesar de que técnicamente da a los indios el derecho legal de solicitar información gubernamental, eximió de su adhesión a todas las agencias de inteligencia y de seguridad.[28] Esto hace que sea casi imposible para los ciudadanos de la India llevar pruebas de vigilancia ilegal del gobierno ante un juez. Por otra parte, varias sentencias del Tribunal Supremo tras su decisión de 1996 de establecer un limitado derecho constitucional a la privacidad han erosionado los derechos de privacidad individuales. El derecho a la privacidad está severamente limitado por un conjunto de excepciones en virtud, por ejemplo, de “un importante interés compensatorio superior”, “un imperioso interés del Estado” o una ley “justa, imparcial y razonable”.[29]

> “En los últimos años el gobierno ha detenido a numerosas personas que lo han criticado en las redes sociales y ha presionado cada vez más a los sitios web (...) para censurar la expresión y actividad de sus usuarios.”

En ausencia de controles judiciales efectivos, la supervisión de las agencias y poderes de vigilancia de la India queda en gran medida en manos de la rama ejecutiva. Bajo las directrices de 1996, el ministro del Interior tiene la responsabilidad de revisar personalmente cada solicitud individual federal de una agencia gubernamental para interceptar comunicaciones. Para asegurarse de que no haya fallos, otros tres burócratas –el secretario del gabinete, el secretario de Justicia y el secretario de Telecomunicaciones– constituyen un “comité de seguimiento”, que se reúne periódicamente para revisar las órdenes aprobadas por el ministro del Interior. El número de solicitudes que el ministro del Interior y el comité están revisando es asombrosa: 7000 a 9000 escuchas telefónicas estaban siendo autorizadas a nivel federal cada mes, desde 2013.[30] Esto significa que el ministro del Interior autoriza alrededor de 100.000 solicitudes cada año. Como han señalado los críticos, si le tomara solo tres minutos considerar cada solicitud, tardaría 15 horas al día (incluyendo fines de semana y días festivos) para evaluar 9000 solicitudes por mes. Los números por sí solos sugieren que este proceso es poco más que un sello de goma mecánico.[31]

conclusión

En su importante exposición de 2010 en la revista *Outlook*, Saikat Datta reveló que el gobierno de la India se ha movilizado agresivamente en los últimos años para adquirir y desplegar nuevas y potentes tecnologías de vigilancia digitales como el monitoreo celular GSM *off-the-air* y CDMA, y que esas tecnologías ahora se entretejen en el que posiblemente sea uno de los regímenes de vigilancia masiva más intrusivos y opacos del mundo. Por otra parte, según ha informado Datta, el gobierno indio está dirigiendo los poderes de vigilancia no solo hacia amenazas externas, sino también internas: hacia algunos de los políticos más prominentes del país, activistas, disidentes y minorías desfavorecidas y, como él mismo notó al mirar en el espejo retrovisor de su vehículo el año anterior a la publicación, a los periodistas que tratan de echar luz sobre el funcionamiento interno de los servicios de inteligencia que no rinden cuentas.

En cierto modo, los servicios de inteligencia operan como sus antepasados de la época colonial, sin una supervisión independiente y con un reconocimiento limitado de los derechos de privacidad de los ciudadanos de la India. Las herramientas que se manejan, sin embargo, son cada vez más herramientas de vigilancia masiva; el monitoreo GSM y CDMA son solo un aspecto de un sistema nuevo, más centralizado y universal de vigilancia que incluye todo, desde escuchas telefónicas a redes sociales, y que ha expandido notablemente el alcance y la cantidad de información que el gobierno puede recolectar. Desde los pasillos del Parlamento al cibercafé más modesto y alejado, el gobierno indio está observando.

notas

-

1. "India's Government Wins Parliament Confidence Vote", *The Washington Post* (23 de julio, 2008). Disponible en: http://www.washingtonpost.com/wp-dyn/content/article/2008/07/22/AR2008072200161.html [28/10/2016]
2. "Outlook Journalist Nabs Tailing IB Men", *Outlook* (11 de abril, 2009). Disponible en: http://www.outlookindia.com/newswire/story/outlook-journalist-nabs-tailing-ib-men/657969 [28/10/2016]
3. "We, The Eavesdropped", *Outlook* (3 de mayo, 2010). Disponible en: http://www.outlookindia.com/magazine/story/we-the-eavesdropped/265191 [28/10/2016]
4. *Ibíd*.
5. "Phone tap technology widely available; both GSM & CDMA phones easy to tap", *The Economic Times* (16 de diciembre, 2010). Disponible en: http://articles.economictimes.indiatimes.com/2010-12-16/news/27610363_1_interception-phone-sim-card [28/10/2016]
6. Ver "Phone Monitoring", *Privacy International*. Disponible en: https://www.privacyinternational.org/node/76 [28/10/2016]
7. "We, The Eavesdropped", *op. cit*.
8. "A Fox On A Fishing Expedition", *Outlook* (3 de mayo, 2010). Disponible en: http://www.outlookindia.com/magazine/story/a-fox-on-a-fishing-expedition/265192 [28/10/2016]
9. Human Rights Watch. "India: New Monitoring System Threatens Rights" (7 de junio, 2013). Disponible en: https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights [28/10/2016]; e "India's Snooping and Snowden", *The Wall Street Journal* (5 de junio, 2014): http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snooping-and-snowden/ [28/10/2016]
10. "India's surveillance project may be as lethal as PRISM", *The Hindu* (21 de junio, 2013). Disponible en: http://www.thehindu.com/news/national/indias-surveillance-project-may-be-aslethal-as-prism/article4834619.ece [28/10/2016]
11. "India sets up elaborate system to tap phone calls, e-mail", *Reuters* (20 de junio, 2013). Disponible en: http://www.reuters.com/article/us-india-surveillance-idUSBRE95J05G20130620 [28/10/2016]
12. Addison Litton. "The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression", *Washington University Global Studies Law Review*, Volume 14, Issue 4 (2015). Disponible en: http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1556&context=law_globalstudies [28/10/2016]; ver también "State of Surveillance in India", *Privacy International.* Disponible en: https://www.privacyinternational.org/node/818 [28/10/2016]
13. "How Surveillance Works in India", *The New York Times* (10 de julio, 2013). Disponible en: http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=0 [28/10/2016]
14. Disponible en: http://www.dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf [28/10/2016]
15. "India: New Monitoring System Threatens Rights", *op. cit.*
16. Addison Litton, *op. cit.*
17. "India: New Monitoring System Threatens Rights", *op. cit.*
18. "How Surveillance Works in India", *op. cit.*
19. *Ibíd.*
20. "Internet Privacy in India", *The Centre for Internet & Society*. Disponible en: http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india [28/10/2016]
21. Addison Litton, *op. cit.*
22. "How Surveillance Works in India", *op. cit.*
23. Ver, por ejemplo, "A Mumbai Student Vents on Facebook, and the Police Come Knocking", *The New York Times* (20 de noviembre, 2012). Disponible en: http://www.nytimes.com/2012/11/21/world/asia/india-police-arrest-student-over-facebook-post.html [28/10/2016]; "PUCL leader Jaya Vindhayala sent to judicial custody for objectionable Facebook post on Tamil Nadu Governor K. Rosaiah", *India Today* (13 de mayo, 2013). Disponible en: http://indiatoday.intoday.in/story/pucl-leader-jaya-vindhayala-remanded-judicial-custody-objectionable-posts-tn-governor-india-today/1/270867.html [28/10/2016]; e "India professor held for cartoon 'ridiculing Mamata'", *BBC News* (13 de abril, 2012). Disponible en: http://www.bbc.com/news/world-asia-india-17699304 [28/10/2016]
24. "Created by telegram, IB finds itself standing on thin legal ground", *Hindustan Times* (14 de noviembre, 2013). Disponible en: http://www.hindustantimes.com/india/created-by-telegram-ib-finds-itself-standing-on-thin-legal-ground/story-UFrue3ywW4P96DhvQFtadM.html [28/10/2016]; ver también "Ex-officer questions Intelligence Bureau's legal status", *The Times of India* (26 de marzo, 2012). Disponible en: http://timesofindia.indiatimes.com/city/chennai/Ex-officer-questions-Intelligence-Bureaus-legal-status/articleshow/12407777.cms [28/10/2016]
25. "'DNA' Exclusive: Raw Invades Your Privacy", *DNA* (17 de diciembre, 2011). Disponible en: http://www.dnaindia.com/india/report-dna-exclusive-raw-invades-your-privacy-1626874 [28/10/2016]
26. "Created by telegram, IB finds itself standing on thin legal ground", *op. cit.*
27. Addison Litton, *op. cit.*
28. Ver el sitio web gubernamental de Derecho a la Información: http://www.righttoinformation.gov.in/rtiact.asp [28/10/2016]
29. "State of Surveillance in India", *op. cit.*
30. "Can India Trust Its Government on Privacy?", *The New York Times* (11 de julio, 2013). Disponible en: http://india.blogs.nytimes.com/2013/07/11/can-india-trust-its-government-on-privacy/?_r=0 [28/10/2016]
31. *Ibíd.*

Un vistazo a la vigilancia en la India

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
No.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos?
Aumentado.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Lo ampliaría.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
No.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
Más.

Las cámaras
están prendidas,
y saben lo que
están mirando

7
HUNGRÍA

Cámaras de seguridad contra el fondo de una valla publicitaria en la que puede verse un ojo humano. Foto: Mark Lennihan/AP

HUNGRÍA

Las cámaras están prendidas, y saben lo que están mirando

el caso

Durante la campaña para las elecciones nacionales de 2014, el alcalde del distrito 8 de Budapest hizo una revelación explosiva: su gobierno estaba instalando 180 nuevas cámaras de circuito cerrado de televisión con capacidad de reconocimiento facial, un sistema que, prometió, proporcionaría una completa cobertura de vigilancia en esa parte de la ciudad.

No fue solo el plan en sí el que encendió las alarmas, sino la poderosa figura detrás del mismo. Máté Kocsis no era solo el alcalde por segundo término consecutivo de un distrito pobre pero en alza del centro de Budapest, también era miembro del Parlamento y uno de los líderes políticos del partido gobernante, el Fidesz, ocupando los cargos de vicepresidente del partido en Budapest y de director de comunicaciones del Fidesz a nivel nacional. En la municipalidad de Budapest era comisionado del gobierno y de las fuerzas policiales y en el Parlamento se desempeñó en la Comisión de Seguridad Nacional y dirigió la Comisión de Seguridad Nacional y Aplicación de la Ley. También formó parte de un comité *ad hoc* sobre crímenes cometidos por la policía ("crimen de uniforme") y de un comité de investigación para sondear las consecuencias del escándalo de vigilancia de la NSA para Hungría y la soberanía húngara. También fue presidente de la Asociación de Balonmano Húngara y vicepresidente del club deportivo Ferencvárosi Torna: cargos de patrocinio de un partido gobernante conocido por vender influencias a través de donaciones deportivas y lucrativos proyectos de construcción de estadios.

Para vender su plan, Kocsis puso en marcha una campaña de "consulta social", una estrategia de propaganda que el Fidesz emplea a menudo para reunir "descubrimientos" que sirven para justificar medidas controvertidas. El distrito 8 de Budapest es el hogar de una gran población romaní, y por décadas, durante y después del régimen soviético, ha sufrido de una alta pobreza, crimen y abandono. Para promocionar los beneficios de las cámaras no solo para la investigación del delito sino también para prevenirlo, el gobierno local envió cartas a los residentes del distrito solicitando propuestas sobre dónde ubicarlas. Combinando "investigación" con campaña, Kocsis montó su plan para la victoria: en abril de 2014 fue reelegido para un tercer mandato, y se movió rápidamente para instalar la amplia red de cámaras digitales.

Desde entonces, Kocsis ha logrado llevar a cabo su objetivo al tiempo que elude casi cualquier escrutinio público significativo. El plan tuvo un presupuesto anunciado de 300 millones de florines (HUF) –alrededor de 1 millón de dólares–, de los que dos tercios serían proporcionados por el Ministerio Federal del Interior y el tercio restante, por el gobierno local, que compraría oficialmente las cámaras. La ley húngara requiere un proceso de contratación pública obligatoria para todos los proyectos con presupuestos superiores a HUF 250 millones, pero Kocsis hizo que elevaran ese techo a HUF 300 millones para eludir esa obligación y, a pesar de ser financiado con dinero público, los detalles del proyecto quedaron envueltos en el secretismo. Cada solicitud de información sobre la licitación de las cámaras ha sido denegada por el gobierno local, que afirma que la información es confidencial por razones de seguridad nacional. El gobierno local ha declarado que el software de reconocimiento facial instalado en las cámaras es "mundialmente conocido", pero el nombre exacto y su marca también son confidenciales.

Mientras las cámaras de reconocimiento facial eran instaladas en lugares secretos en todo el distrito, una nueva sede se estaba preparando para ejecutar el sistema de vigilancia. Las cámaras eran oficialmente propiedad del gobierno local, pero los datos generados por las cámaras serían procesados por el Servicio Especial para la Seguridad Nacional, una de las agencias de seguridad nacional de Hungría. La principal función, vagamente definida, del Servicio Especial de Hungría es apoyar la recolección de información secreta de otras agencias gubernamentales. Más allá de una revelación filtrada de 2013, en la que se supo que el gobierno húngaro había adquirido y desplegado

> “Lo que se promociona como una herramienta de prevención del delito en un área particular de Budapest es en realidad un modelo para un sistema mucho más grande.”

el controvertido software de vigilancia FinFisher, poco se sabe acerca de lo que implica esa recolección de información secreta o qué métodos y procedimientos utiliza el Servicio Especial para hacer su trabajo.

Lo que está claro es que el Servicio Especial es en gran medida la agencia detrás de las cámaras de reconocimiento facial del distrito 8, y que lo que se promociona como una herramienta de prevención del delito en un área particular de Budapest es en realidad un modelo para un sistema mucho más grande. Al Servicio Especial se le ha encargado testear la nueva tecnología y, si declara que el experimento ha sido un éxito, las cámaras de reconocimiento facial serían instaladas al lado de todas las estaciones de metro de Budapest.

el contexto

Los ciudadanos húngaros están muy familiarizados con la vigilancia. La interceptación de llamadas telefónicas, la instalación de micrófonos ocultos en los hogares y la recolección de información a través de agentes de inteligencia fueron prácticas generalizadas durante el régimen comunista, un régimen contra el que el partido Fidesz, formado en 1998 por un grupo de jóvenes liberales que promovían la democracia parlamentaria y el Estado de Derecho, nació para oponerse. En la década posterior a la transición a la democracia y la economía de mercado, esos valores se arraigaron y emergió un efectivo sistema democrático multipartidista con diversos gobiernos locales, un poder judicial independiente y un claro enfoque hacia la integración europea.

Pero tras los decepcionantes resultados de las elecciones de 1994, el Fidesz viró de liberal a reaccionario y escaló, primero en las elecciones municipales y luego en las nacionales. Atrás quedaron sus compromisos democráticos fundacionales: una vez en el poder, el Fidesz ha erosionado o desmantelado muchos de los avances democráticos de Hungría de los últimos años, debilitando los gobiernos locales, remodelando el sistema de votación y socavando la

Oficiales de policía observan una prueba del sistema de vigilancia recién instalado desde la nueva sala de monitoreo de la comisaría de policía del distrito 8 de Budapest, Hungría, en 2014. Foto: Orsi Ajpek/Index

independencia de las instituciones judiciales (incluido el Tribunal Constitucional) y la de órganos de supervisión esenciales tales como la defensoría del pueblo, la autoridad de protección de datos y las agencias con autoridad sobre instituciones económicas y financieras y medios públicos de comunicación.

También ha mostrado hostilidad hacia la sociedad civil húngara. En un discurso de 2014, el primer ministro Viktor Orbán declaró que las organizaciones no gubernamentales son "activistas políticos pagados por grupos de intereses extranjeros" que "desean utilizar este sistema de instrumentos para influir en la vida política húngara". También dijo que crearía una comisión parlamentaria para revelar "quiénes son los personajes reales que están detrás de las máscaras de las ONG en Hungría". La Oficina de Control del Gobierno inició auditorías específicas de las organizaciones consideradas críticas del gobierno –incluyendo la Hungarian Civil Liberties Union (HCLU)– sin justificación legal adecuada, y para septiembre de 2014 las oficinas de dos organizaciones que estaban ayudando a distribuir fondos de una ONG noruega fueron ilegalmente allanadas por la policía.

Esta clara hostilidad hacia las actividades de las organizaciones de la sociedad civil se está produciendo en un contexto de una re-emergente y cada vez más opaca cultura de la vigilancia.

Hoy hay dos categorías de poderes de vigilancia en Hungría: la vigilancia secreta para fines de investigación criminal y la vigilancia secreta por razones de seguridad nacional. Agencias independientes llevan a cabo estas dos categorías de vigilancia y, legalmente hablando, hay diferencias en los requisitos de autorización externas y órdenes judiciales y en los mecanismos de supervisión y control que rigen sus operaciones. Pero poco se sabe realmente acerca de la naturaleza y el alcance de estos poderes de vigilancia, de su marco normativo y de si sus actividades reales cumplen con las leyes y reglamentos.

En las investigaciones criminales, la policía, las aduanas y las autoridades del Ministerio Público están autorizadas a llevar a cabo operaciones secretas de vigilancia dentro de los límites más restrictivos de la legislación húngara. Sin embargo, estas entidades reciben el apoyo del Servicio Especial para la Seguridad Nacional, que les proporciona las herramientas y los conocimientos técnicos para recolectar información de inteligencia y adquirir datos de forma encubierta. El Centro contra el Terrorismo de la policía húngara también está facultado para emplear la vigilancia secreta, tanto para fines de investigación penal como no penal. Cuando se está reuniendo inteligencia relacionada con una investigación criminal, el Centro contra el Terrorismo está obligado a solicitar una autorización judicial, pero las investigaciones para prevenir actos terroristas o aquellas que revisten interés de la seguridad nacional pueden eludir este control

Nueva sala de monitoreo de las cámaras de vigilancia de la comisaría de policía del distrito 8 de Budapest, Hungría, en 2014. Foto: Orsi Ajpek/Index

> “Designar al Servicio Especial para la Seguridad Nacional para que opere circuitos cerrados de televisión es una clara violación del principio de separación entre la policía y los servicios de seguridad nacional.”

judicial y ser autorizadas directamente por el ministro de Justicia. Los poderes del Centro contra el Terrorismo son extensos e incluyen registros secretos de hogares, grabaciones de vigilancia, la apertura de cartas y paquetes y la inspección y registro de los contenidos de las comunicaciones electrónicas o informatizadas, todo ello sin el conocimiento de los objetivos de la vigilancia.

En 2012, dos abogados que creían que estaban siendo monitoreados por el Centro contra el Terrorismo llevaron sus preocupaciones al Tribunal Europeo de Derechos Humanos (TEDH), denunciando la norma que faculta al Centro para espiar a cualquier persona sin una orden judicial, citando preocupaciones de seguridad nacional. Los abogados denunciaron esa vigilancia, que requiere solo de la firma del ministro de Justicia, con el argumento de que había una motivación política y se trataba de una violación injustificada y desproporcionada de su derecho a la privacidad. La sentencia de la TEDH sostuvo que la legislación húngara relevante no proporcionaba salvaguardias suficientemente precisas, eficaces y completas sobre el pedido, la ejecución y el potencial de reparación de tales medidas de vigilancia. El Tribunal consideró que el alcance de la medida podría incluir prácticamente a cualquier persona, en particular dada la nueva tecnología que permite al gobierno interceptar fácilmente grandes cantidades de datos fuera del rango original de operaciones. Además, sobre la base

de que el pedido se desarrolla íntegramente dentro del ámbito del poder ejecutivo, sin una evaluación de estricta necesidad y en ausencia de cualquier medida judicial eficaz o de reparación, el Tribunal concluyó que la ley violaba el derecho al respeto de la vida privada y familiar.[1]

Si los límites y las operaciones de las agencias policiales y de seguridad no quedan claros para la mayoría de los húngaros, el panorama de la vigilancia se ve ensombrecido aún más por indicios de que las empresas privadas han cooperado con el gobierno y entidades cuasi-gubernamentales en actividades ilegales de vigilancia doméstica. Una investigación de 2008 de la Oficina de Seguridad Nacional descubrió que una empresa privada llamada UD Zrt, cuyos propietarios incluían a miembros del aparato de seguridad nacional de Hungría, había espiado a políticos mediante el mapeo de sus estilos de vida, hábitos y el historial de sus actividades financieras y llamadas telefónicas.

En resumen, la nebulosa red húngara de organismos y poderes de vigilancia crea una atmósfera de malestar, sobre todo para las ONG y los activistas políticos de la oposición en Hungría. Más de 25 años después del fin del régimen comunista, hay una vez más una preocupación generalizada de que los aparatos de investigación criminal y de vigilancia en pos de la seguridad nacional están siendo desplegados para fines políticos, de una manera que recuerda a la era comunista.

conclusión

Bajo la ley húngara, solo la policía y la "autoridad de seguridad pública" están autorizadas a instalar cámaras de vigilancia; designar al Servicio Especial para la Seguridad Nacional para que opere circuitos cerrados de televisión es una clara violación del principio de separación entre la policía y los servicios de seguridad nacional. Pero la cuestión del control va mucho más allá de quién está instalando y monitoreando las cámaras. Las cámaras de reconocimiento facial dependen de una base de datos de imágenes faciales en la que se busca y compara. Al igual que con todos los demás aspectos del proyecto, no ha habido ninguna información oficial sobre cómo se está construyendo esa base de datos ni de quiénes son las imágenes que incluye.

En una reunión de junio de 2014 de una comisión parlamentaria, Kocsis declaró que el objetivo no era construir una base de datos que contuviera las imágenes de todos los húngaros; el objetivo es encontrar criminales, insistió, por lo que la base de datos se extrae de los antecedentes penales oficiales. Pero incluso limitar la base de datos a los antecedentes penales plantea graves problemas legales y del debido proceso: por empezar, el sistema de antecedentes penales de Hungría está notoriamente plagado de errores y es anticuado. Además, contiene registros no solo de aquellos que han sido condenados por delitos, sino de aquellos que se enfrentan a procedimientos penales o tienen restricciones de viajar al extranjero. Incluso en el caso de aquellos que han sido condenados por delitos, nada en el Código Penal de Hungría o en sus apartados habilita a su vigilancia permanente y sin orden judicial.

Depender de una base de datos extraída de registros oficiales es particularmente problemático en zonas como el distrito 8, que tiene una significativa población romaní. La policía húngara tiene un largo historial de discriminación en las comunidades romaníes, donde los ciudadanos han sido multados de manera desproporcionada por delitos menores, tales como no tener una campana en una bicicleta o empujar un carrito de bebé por la calle. La HCLU ha denunciado tales prácticas en los tribunales y recientemente ganó un fallo afirmando que las sanciones desproporcionadas de la población romaní por infracciones menores son discriminatorias. Sin embargo, los antecedentes penales que producen estas conductas discriminatorias son pasibles a permanecer en los archivos oficiales que alimentan la base de datos del circuito cerrado de televisión, garantizando que los residentes romaníes sean sometidos de manera desproporcionada a la vigilancia de reconocimiento facial.

De hecho, hay indicios de que el gobierno tiene la intención de construir una base de imágenes mucho más amplia. En virtud de un proyecto de ley actualmente pendiente, un registro de búsquedas por imágenes de todos los ciudadanos de Hungría estaría en funcionamiento a partir de 2016. El Servicio Especial para la Seguridad Nacional tendría amplias facultades para solicitar datos de ese archivo, lo que le daría poder para hacer identificaciones secretas, a distancia y al por mayor de todos los ciudadanos húngaros.

Bajo la ley húngara, la ubicación y la capacidad del circuito cerrado de televisión no pueden ser secretas, y gracias a una sentencia judicial a partir de una solicitud de acceso a la información presentada por la HCLU hace una década, que obligó al Departamento de Policía de Budapest a revelar dónde se había instalado una generación anterior de cámaras de vigilancia, sabemos que la nueva generación de cámaras de reconocimiento facial también ha sido instalada. La página web de la policía del distrito 8 cuenta con un mapa repleto de puntos rojos que marcan la ubicación de las cámaras de vigilancia. Pero nadie sabe a ciencia cierta lo que está sucediendo con las imágenes que las cámaras en el distrito 8 de Budapest están viendo, o a quiénes exactamente esas cámaras están reconociendo. Lo que sí sabemos, según el propio Kocsis, es que las cámaras están encendidas, en "modo de prueba", y que la falta de un marco legal para regular su uso, o la falta total de transparencia en la forma en que el sistema está siendo probado y evaluado, no han impedido su instalación y puesta en operación.

"La reglamentación puede esperar", declaró Kocsis hace poco, "hasta que las cámaras estén realmente en funcionamiento".

Un vistazo a la vigilancia en Hungría

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
No.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
No.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Han aumentado.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Lo ampliaría.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
No.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
No ha modificado su percepción.

notas
-

1. Caso *Szabó y Vissy v. Hungría*, aplicación no. 37138/14, dictamen 12 de enero, 89.

Humo y espejos: la ley irlandesa de vigilancia y la ilusión de transparencia

8
IRLANDA

Comisión del Ombudsman de la Garda Síochána, 8 de febrero de 2013. Foto: The Irish Times

IRLANDA

Humo y espejos: la ley irlandesa de vigilancia y la ilusión de transparencia

el caso

El 10 de febrero de 2014 apareció un artículo en la edición irlandesa de un periódico dominical británico muy conocido bajo el sencillo título: “GSOC bajo vigilancia de alta tecnología”. El artículo describía una serie de acontecimientos que, de no haber ocurrido en realidad, bien podrían haber servido como argumento para un thriller político.

El escenario de la historia era un modesto edificio de oficinas de tres pisos, no muy lejos de la animada zona comercial de la ciudad de Dublín, que alberga la oficina de la Comisión del Ombudsman de la Garda Síochána (GSOC). La GSOC es un órgano de supervisión independiente financiado por el Estado, que recibe y revisa las quejas sobre la Garda –la policía nacional de Irlanda– y funciona como uno de los pocos órganos de supervisión policial verdaderamente independientes en el mundo. En palabras de la GSOC, la responsabilidad principal de la Comisión es ocuparse de las “denuncias formuladas por la población en relación con la conducta de los miembros de la Garda”. Bajo la ley irlandesa, la comisión tiene amplios poderes para investigar y procesar acusaciones de mala conducta contra agentes en servicio, incluyendo –con el consentimiento del ministro de Justicia e Igualdad– al comisionado de la Garda, o jefe de policía.

La GSOC es un cuerpo de tres miembros que se estableció en diciembre de 2005 para sustituir a la antigua Junta de Denuncias de la Garda Síochána, un mecanismo interno de quejas contra la policía. La Comisión tiene más poderes que su predecesora: puede investigar las quejas formuladas contra agentes de la policía por parte de la población e iniciar investigaciones por su propia voluntad cuando considere que un agente de policía ha cometido una infracción o actuado de una manera que justifique medidas disciplinarias. Desde su creación, la GSOC ha estado involucrada en una serie de investigaciones de alto perfil sobre alegaciones de faltas graves y comportamiento criminal por parte de miembros de la Garda en servicio. La relación de trabajo entre la GSOC y la policía a veces ha sido áspera.

En su artículo, el periodista del *Sunday Times* John Mooney contaba que, hacia el final del verano de 2013, la GSOC había contratado a una empresa británica de seguridad privada, experta en contravigilancia, para que buscara en sus oficinas rastros de actividad de vigilancia en su contra. En su declaración ante un comité de supervisión parlamentaria compuesto por todos los partidos, que convocó a una serie de audiencias sobre el asunto, el entonces presidente de la GSOC, Simon O’Brien, señaló que fue la preocupación por la posible fuga o robo de información sensible de sus oficinas la que había impulsado inicialmente el pedido de rastreo. Como resultado de los hallazgos de la empresa de seguridad, la GSOC, sin el conocimiento del ministro de Justicia e Igualdad, puso en marcha su propia investigación de interés público bajo la sospecha de que estaba siendo vigilada por miembros de la Garda Síochána.

La particularidad de las modernas técnicas de vigilancia encubierta –al menos según Verrimus, la empresa de seguridad y contravigilancia del Reino Unido contratada por la GSOC para llevar a cabo la investigación– es que son, por diseño, muy difíciles de detectar con algún grado de certeza. Verrimus no pudo descubrir ninguna evidencia concreta que apuntara definitivamente a una actividad de vigilancia. Sin embargo, durante las pruebas llevadas a cabo en las oficinas de la GSOC en distintas ocasiones, la empresa identificó tres anomalías técnicas independientes que, en su evaluación profesional, apuntaban a posibles intentos de acceso a los sistemas de comunicaciones, incluyendo dispositivos móviles de personas dentro o cerca de las oficinas de la GSOC.

La primera anomalía destacada por Verrimus se relacionaba con un dispositivo WiFi sin utilizar en la oficina de reuniones de la GSOC que, según el informe, se había conectado sin autorización a una red externa de WiFi. Más tarde se demostró que esa red

externa provenía de una cafetería del mismo edificio. En su declaración ante la comisión parlamentaria, el ministro de Justicia e Igualdad se esforzó en minimizar la importancia de esa anomalía, en parte porque el dispositivo, al parecer, nunca había sido utilizado por la GSOC. Pero en su propia declaración sobre el asunto, Verrimus sostuvo que esa anomalía sigue siendo un motivo de preocupación creíble, ya que cualquier intento de una red interna de WiFi de conectarse externamente sería altamente irregular y poco probable que se tratase de un simple error.

La segunda anomalía tenía que ver con un sistema telefónico poli-conferencia ubicado en la oficina del presidente de la GSOC, el Sr. O'Brien. Un hecho inexplicable, detectado después de una prueba nocturna del sistema telefónico, sugirió que este podía estar comprometido. La anomalía se registró durante una prueba nocturna del sistema llevada a cabo por los investigadores. La prueba consistía en el envío de una señal de alerta a la línea de teléfono para comprobar posibles amenazas a la seguridad. El procedimiento está dirigido a "limpiar" a un potencial intruso. En su informe, Verrimus señaló que momentos después de que la señal enviara una prolongada descarga de música, el mismo teléfono recibió una llamada entrante. En su evaluación, la empresa de seguridad llegó a la conclusión de que "la probabilidad de llamar a un 'número equivocado' a esa hora, a ese exacto número y en el mismo momento en que se estaba realizando una prueba de seguridad es tan pequeña que prácticamente se reduce a cero". En otras palabras, la recepción de una llamada momentos después de que una señal de audio inusual e inesperada fuese enviada a través de la línea telefónica sugiere una conducta deliberada por parte de alguien que estaba escuchando esa línea, tal vez para comprobar la integridad de la conexión sin sospechar que una operación de contravigilancia estaba en marcha.

La tercera amenaza identificada por Verrimus estaba relacionada con la posible intervención de telecomunicaciones de forma remota. Verrimus informó que, después de las pruebas, detectó una "estación base" de GSM/3G falsificada, configurada para una empresa de telefonía móvil del Reino Unido que opera en el entorno de las oficinas. La estación base era capaz de conectarse a cualquier teléfono suscripto a ese operador o incluso, como se confirmó más tarde, a otros operadores de telefonía, dependiendo de las especificaciones. Cualquier teléfono conectado a la falsa estación base habría sido susceptible de tener su información comprometida, incluyendo los datos de las llamadas telefónicas. En su informe, Verrimus llegó a la conclusión de que la tecnología utilizada para simular una red de este tipo era posiblemente un IMSI Catcher o "stingray": un dispositivo que se utiliza para adquirir los códigos de hardware de los teléfonos móviles y tarjetas SIM utilizadas en la conexión a una red en particular. Las pruebas realizadas para detectar la estación de base falsificada coincidieron con lo visto por personal de Verrimus en el lugar: un vehículo sin identificación y con ventanas oscurecidas estacionado cerca de las oficinas de la GSOC, que la empresa concluyó sugería la posibilidad de vigilancia móvil. Verrimus señaló que debido a que los IMSI Catchers generalmente están a disposición únicamente de entidades gubernamentales, el dispositivo detectado indicaba una vigilancia sofisticada intencional. Sin embargo, no hubo evidencia de que ninguno de los teléfonos de la GSOC hubiese sido comprometido como resultado de la anomalía.

En una serie de informes sobre sus investigaciones, Verrimus no concluyó de manera definitiva que hubiera habido un ataque de vigilancia contra las oficinas de la GSOC. En base a la evidencia disponible, la empresa concluyó una serie de hechos. En primer lugar, el fenómeno del dispositivo WiFi en la sala de reuniones "evidenció que estaba actuando de manera insegura". En segundo lugar, "una estación base falsa o falsificada de 3G fue detectada localmente". Por último, en relación al sistema de conferencias en el despacho del director, que recibió una llamada entrante en el momento en que la línea se puso a prueba, la empresa llegó a la conclusión de que la prueba "pudo haber desencadenado la respuesta de un atacante/puesto de escucha/monitoreo". Verrimus llegó a afirmar que, en tal

Miembros de la Garda Síochána (servicio de policía de Irlanda), 2013. Foto: Brenda Fitzsimons/The Irish Times

caso, era "probable que el 'oyente' haya considerado que el audio intermitente en la línea telefónica a las 01.40 horas fuese extraño y, sin pensar o considerar la posibilidad de una operación [de contravigilancia], decidiera poner a prueba la línea para asegurarse de que estaba funcionando […] suponiendo que no habría nadie en las oficinas en ese momento". Estas conclusiones dejaron pocas dudas de que Verrimus creía que las anomalías detectadas representaban una amenaza clara y que la GSOC podría haber sido sometida a una vigilancia o intento de vigilancia. Por otra parte, a juicio de la empresa, al menos una de las anomalías era tan tecnológicamente compleja que habría sido difícil de desplegar para cualquier entidad que no fuese de la policía o de un servicio de inteligencia del Estado.

Que el informe Verrimus arrojase sospechas sobre el Estado provocó indignación en el gobierno, y la resistencia interna desaceleró significativamente una investigación oficial. El entonces ministro de Justicia e Igualdad, Alan Shatter TD (de la Teachta Dála[1]) hizo una aparición desafiante ante la comisión parlamentaria, criticando la noción de que él (como se había sugerido) o la policía estuviesen bajo sospecha. "Mi único interés es llegar a la verdad", dijo a la comisión, al tiempo que afirmaba que la insinuación de que él podría haber autorizado dicha vigilancia se encontraba en el reino de la "fantasía total". Sin embargo, al ser interrogado por los miembros de la comisión parlamentaria, el ministro reveló que ni siquiera le había preguntado al comisionado de la Garda si la policía había llevado a cabo una actividad de vigilancia contra la GSOC. Tampoco le había preguntado a la división de Inteligencia de las Fuerzas de Defensa (conocida como G2), otro organismo con autoridad de vigilancia legal, si había participado en el control del órgano de supervisión de la policía. En opinión del ministro, no había "evidencia" que requiriera una investigación interna de la policía o de los servicios de inteligencia militar –una posición repetida en varias ocasiones por altos funcionarios irlandeses, incluso mientras crecían las preocupaciones sobre lo que se dio a conocer como el "escándalo de escuchas de la GSOC".

En vez de apoyar una investigación sustancial, la respuesta del gobierno a la tormenta política se centró en los mensajeros: los funcionarios cuestionaron la credibilidad de Verrimus en relación con su evaluación de que las anomalías suponían una amenaza, cuestionaron el comportamiento de la GSOC por iniciar su propia investigación de interés público sobre la posible participación de la policía en la vigilancia de sus oficinas y criticaron a su director por no haber informado al ministro de Justicia e Igualdad sobre la investigación. La GSOC admitió que, en última instancia, aunque su sospecha del involucramiento de la policía se basara en una causa noble, no encontró evidencias de mala conducta por parte de la Garda y que si bien, en virtud de la legislación irlandesa, la GSOC no está obligada a

“Sobre la base de las opiniones técnicas y la información disponible, es imposible descartar categóricamente toda posibilidad de vigilancia encubierta.”

informar al ministro de sus investigaciones, lamentaba no obstante su decisión de no mantener informado al ministro sobre su investigación de las escuchas. La muy seria posibilidad de que la GSOC hubiera sido sometida a una vigilancia poderosa, intrusiva e ilegal se perdió casi por completo entre las disputas políticas internas.

Pero fuera del gobierno, la preocupación por el escándalo de las escuchas de la GSOC creció día a día, y el 18 de febrero de 2014, ocho días después de que el artículo del periodista John Mooney apareciera por primera vez en *The Sunday Times*, el gobierno cedió a la presión de los partidos de la oposición, medios de comunicación independientes y expertos legales, incluyendo el Irish Council for Civil Liberties (ICCL) y el público en general, y estableció una investigación judicial. Esa investigación fue dirigida por un juez retirado del Tribunal Supremo, el Honorable Sr. Juez John Cooke. Dieciséis semanas después, el 10 de junio de 2014, el juez publicó un informe parcialmente redactado de 64 páginas.

Los términos de referencia para la investigación judicial fueron fijados por el gobierno. Como cuestión esencial, se le pidió al juez Cooke que determinara la secuencia de eventos que llevaron a la GSOC a iniciar su propia investigación de interés público, que examinara todos los informes y documentos relevantes a esa investigación y que revisara y evaluara cualquier evidencia de violación de la seguridad o intento de violación de la seguridad de la GSOC. En sus conclusiones, el juez no descartó la vigilancia de manera concluyente. En su lugar, ofreció una serie de explicaciones inocentes acerca de las anomalías encontradas. Teniendo en cuenta las limitaciones derivadas de la “fundamentación *ad hoc* y no estatutaria de la investigación” el juez señaló que no se le había concedido ninguna autoridad “para dirimir en la disputa de los hechos” y que las conclusiones alcanzadas en el informe dependían de la cooperación voluntaria de los interesados y de aquellos a quienes el juez consideraba conveniente contactar. Después de haber limitado su opinión a la documentación relacionada con las sospechas de la GSOC, el juez concluyó que:

Sobre la base de las opiniones técnicas y la información disponible, es imposible descartar categóricamente toda posibilidad de vigilancia encubierta.

Sin embargo, agregó que:

En las tres amenazas identificadas por Verrimus, resulta evidente que las pruebas no apoyan la tesis de que el tipo de vigilancia señalada en el artículo del Sunday Times *se llevara a cabo, y mucho menos que se llevara a cabo por miembros de la Garda Síochána.*

El informe pasaba a ofrecer una serie de explicaciones alternativas y más bien inocentes sobre las anomalías descubiertas por Verrimus que, el juez concluyó, debían ser consideradas plausibles. El juez señaló que la conexión de datos en relación con el sistema WiFi de la sala de reuniones no podría haber sido utilizado para activar un micrófono capaz de escuchar conversaciones, ya que el dispositivo en cuestión no estaba habilitado para la microfonía. Por lo tanto, no podría haber ocurrido ninguna vigilancia real. De igual modo, la estación base falsa de 3G que Verrimus dijo haber detectado podría explicarse por la actividad de empresas de telefonía móvil probando redes de 4G en la zona, aunque el informe no presentó pruebas concluyentes para apoyar esa suposición. Por último, si bien el hecho de que hubiera una llamada entrante en el sistema de comunicaciones sigue sin explicación, el juez señaló que no hay pruebas de que la “reacción de realizar una llamada sea atribuible necesariamente a una infracción o mala conducta por parte de un miembro de la Garda”. Esta explicación es tan curiosa como desorientadora, ya que una respuesta a la pregunta de si alguien estaba escuchando o era capaz de escuchar es muy distinta a la pregunta de quién estaba escuchando.

El informe del juez Cooke fue inmediatamente criticado, tanto por su metodología como por sus conclusiones. En reacción a las conclusiones del informe, el director ejecutivo del ICCL, Mark Kelly, señaló que dadas las limitaciones impuestas por los términos de referencia del gobierno para su investigación, Cooke encontró precisamente lo que parece haber sido predeterminado a encontrar: que es imposible descartar categóricamente toda posibilidad de vigilancia encubierta. Kelly dijo que era sorprendente que el juez no hubiera hecho el más mínimo intento de impulsar una investigación independiente para establecer objetivamente si la Garda Síochána había o no autorizado una vigilancia sobre la GSOC. También señaló que ni un solo miembro de la Garda o de las Fuerzas de Defensa había sido entrevistado, y que

no parecía haber habido ninguna inspección de los registros de uso de equipamientos de vigilancia por parte de la policía o de los servicios de inteligencia militar. Las actividades de "supervisión" de los "jueces designados" bajo la legislación pertinente tampoco fueron sometidas a ningún tipo de revisión.

En lugar de entrevistar a miembros de la división Garda Special (Seguridad y crimen), o de la división de inteligencia de las Fuerzas de Defensa (G2), o a funcionarios de la Administración Fiscal, el juez Cooke se centró en la cuestión de si las sospechas de la GSOC estaban bien fundamentadas, dejando por completo de lado la cuestión central de si alguna agencia del Estado buscó u obtuvo permiso para vigilar al órgano de supervisión policial independiente. Al dejar sin respuesta la pregunta de si la GSOC había sido sometida a espionaje, el juez Cooke evitó asimismo las preguntas cruciales que surgirían si se determinaba que se había producido dicho espionaje, a saber: ¿quién hizo las escuchas?, ¿se autorizó el espionaje?, ¿por qué?

En su respuesta pública a la publicación del informe del juez, Kelly opinó que un informe que simplemente revisita una serie de explicaciones más o menos plausibles a las anomalías de las comunicaciones, sin siquiera intentar compararlas con información a disposición de la policía y de los servicios de inteligencia militar, solo puede ser calificado como un ejercicio de "humo y espejos".

el contexto

Hasta el año 2009 la vigilancia en Irlanda se regía en gran medida por la Ley de Interceptación de Paquetes Postales y Mensajes de Telecomunicaciones de 1983, en su versión modificada. La legislación daba a la policía y a las Fuerzas de Defensa poderes limitados para escuchar llamadas telefónicas, abrir y leer correos y, si estaban equipados para hacerlo, leer correos electrónicos. El Estado solo podía invocar las disposiciones en circunstancias excepcionales y únicamente con una autorización –solicitud mediante–, al más alto nivel: el ministro de Justicia e Igualdad. Sin embargo, la legislación más reciente ha ampliado esas facultades a un grado sin precedentes.

La Ley de Justicia Penal (Vigilancia) de 2009 reglamentó una serie de facultades legales relativas a la actividad de vigilancia por parte de agentes del Estado. Su puesta en vigencia coincidió con el fortalecimiento del sistema de tribunales penales especiales sin jurado de Irlanda, originalmente establecidos para juzgar a miembros de organizaciones subversivas, pero utilizados cada vez más –a pesar de las considerables críticas por parte de los organismos de supervisión de tratados internacionales– para juzgar a personas sospechosas de crimen organizado. La Ley de 2009 no solo autoriza a la policía y a las Fuerzas de Defensa a llevar a cabo operaciones de vigilancia, sino también, en ciertas circunstancias, a las autoridades fiscales. La Ley incluso amplió la definición legal de vigilancia, por lo que esta se define ahora como:

Monitorear, observar, escuchar o hacer una grabación de una persona o grupo de personas o de sus movimientos, actividades y comunicaciones, o monitorear o hacer una grabación de lugares u objetos, a través de o con la ayuda de dispositivos de vigilancia.[2]

Bajo los nuevos poderes, las autoridades pueden solicitar autorización para realizar vigilancias encubiertas de hasta tres meses de duración mediante una petición secreta remitida a un juez del Tribunal de Distrito (el nivel judicial más bajo de Irlanda), enviada por un oficial de policía, un miembro de las Fuerzas de Defensa o un funcionario fiscal de rango apropiado. En circunstancias consideradas de urgencia, cuando no se puede obtener una autorización judicial, la Ley prevé la autorización por un período de hasta 72 horas de las solicitudes presentadas por un oficial de suficiente rango de agencia de investigación, sujeta a ciertas condiciones.

La Ley de 2009 dio a la policía y las agencias gubernamentales un acceso sin precedentes a la vida privada de las personas, y un nuevo e importante incentivo para empujar los límites de la legalidad. En una desviación significativa de la legislación previa, la Ley indica que una vez que se concede la autorización, los agentes pueden entrar en cualquier lugar, ya sea comercial o residencial, sin el conocimiento o consentimiento del propietario o persona encargada del local –por la fuerza, si es necesario– a los efectos de llevar a cabo una serie de actividades de vigilancia, incluyendo instalar o retirar un dispositivo de vigilancia en un sistema de telecomunicaciones interno. Cualquier evidencia obtenida a través de la vigilancia podría ser admitida como prueba en procedimientos penales, incluso si un oficial de policía no cumpliera con los requisitos para obtener la autorización, siempre que el tribunal considere que el hecho fue accidental, que el agente había actuado de buena fe y que estaba en el interés de la justicia aceptar la evidencia.[3]

Por último, la Ley de 2009 erosionó aún más los ya débiles mecanismos de supervisión destinados a mantener los poderes de vigilancia bajo control. Antes, el gobierno podía autorizar el monitoreo de comunicaciones postales y telefónicas, según fuese necesario para el "interés nacional", y podía obligar a las compañías de correo y telecomunicaciones a darle acceso a los datos conservados a través de sus servicios y ponerlos a disposición a petición. También podía obligar a dichas compañías a interceptar las comunicaciones de un cliente, ayudando con la instalación de capacidades de vigilancia en sus redes y proporcionando acceso directo a sus equipos para facilitar la vigilancia. En los casos considerados por las autoridades investigadoras como urgentes o en interés de la "seguridad del Estado", las solicitudes de cooperación podían hacerse de manera verbal por una persona con suficiente autoridad. Lo que constituía exactamente "seguridad del Estado" nunca fue definido en la legislación.

La Ley anterior a la de 2009 eximía por completo a los dispositivos de interceptación y seguimiento de la obligación de solicitar una autorización judicial.

> “Un informe que simplemente revisita una serie de explicaciones más o menos plausibles a las anomalías de las comunicaciones, sin siquiera intentar compararlas con información a disposición de la policía y de los servicios de inteligencia militar, solo puede ser calificado como un ejercicio de ‘humo y espejos’.”

Si bien el ministro de Justicia e Igualdad estaba obligado a solicitar una autorización para interceptar las comunicaciones relacionadas con investigaciones criminales o de “seguridad del Estado”, los dispositivos de localización –definidos como los equipos utilizados para brindar información sobre la ubicación de una persona, vehículo u objeto– no necesitaban dicha autorización, bajo la teoría de que los dispositivos de localización no graban conversaciones y, por tanto, son menos intrusivos que los dispositivos de monitoreo y que a menudo se despliegan en situaciones de emergencia en las que los requisitos pueden ocasionar retrasos excesivos.

En esencia, la legislación desde 2009 ha traspasado este holgado marco a la tecnología digital más reciente. Por ejemplo, la Ley de Comunicaciones (Retención de Datos) de 2011[4] permite que, sin orden judicial, un miembro de la policía en o por encima del rango de comisario solicite a los proveedores de telecomunicaciones y servicios de internet los datos retenidos, en situaciones en que esos datos son necesarios para la prevención, detección, investigación o acusación de un delito grave; para salvaguardar la seguridad del Estado; o para salvar una vida humana. En casos de urgencia, esas solicitudes pueden ser comunicadas por vía verbal.

Tanto la legislación anterior como la actualizada autorizan a un juez del Tribunal Supremo a controlar las operaciones de vigilancia para determinar si cumplen con la ley. Pero las exigencias para informar son tan débiles que es prácticamente imposible determinar qué poderes se están utilizando, con qué frecuencia y si las operaciones de vigilancia cumplen siquiera con los requisitos legales mínimos.[5] Que la policía, las Fuerzas de Defensa y las autoridades fiscales están utilizando sus poderes de vigilancia es claro: en 2014 la empresa global de telecomunicaciones Vodafone reveló que entre el 1 de abril de 2013 y el 31 de marzo de 2014 había recibido 7973 solicitudes para entregar datos de las comunicaciones.[6]

La concentración de los poderes de vigilancia en manos de la policía nacional de Irlanda, las Fuerzas de Defensa y las autoridades fiscales –todas con el poder de iniciar sus propias operaciones y solicitudes de información, y con poca supervisión independiente– es bastante preocupante. Pero además, en los últimos meses se ha hecho evidente que los ciudadanos irlandeses y los residentes también son vulnerables a la vigilancia exterior aprobada por el gobierno.

El 25 de noviembre de 2014, el diario alemán *Süddeutsche Zeitung* publicó documentos obtenidos por el informante Edward Snowden que revelaron que la agencia de inteligencia británica GCHQ pudo haber estado monitoreando las comunicaciones telefónicas y de internet irlandesas mediante la intervención de una serie de cables submarinos que se extienden desde Irlanda a los Estados Unidos y Gales.[7]

Al día siguiente, la nueva ministra de Justicia e Igualdad, Frances Fitzgerald TD, convirtió en ley un instrumento

legislativo[8] que permite a las agencias extranjeras intervenir llamadas telefónicas e interceptar correos electrónicos en Irlanda. Esa disposición puso en vigor la tercera parte de la Ley de 2008 de Justicia Penal (Asistencia Mutua), que regula la forma en que Irlanda colabora con otros gobiernos en investigaciones criminales, tanto en relación con la vigilancia por parte de Irlanda como con las solicitudes de organismos extranjeros para autorizar su propia actividad de vigilancia en ese país. Un aspecto especialmente preocupante de esta nueva ley es una cláusula que establece que las empresas que se opongan o se nieguen a cumplir con una orden de interceptación podrían ser llevadas ante una sesión privada de un tribunal, que determinará un fallo.

El espectro de abusos que resulta de los acuerdos de intercambio de inteligencia en Irlanda está lejos de ser teórico. En 1999, en una sorprendente revelación hecha por un canal de noticias del Reino Unido, salió a la luz pública que durante siete años, de 1990 a 1997, las agencias de inteligencia británicas interceptaron todas las comunicaciones telefónicas, de fax, de correo electrónico y de datos entre el Reino Unido e Irlanda, incluyendo información legalmente protegida y confidencial, y que toda esa información se había almacenado, en bloque, en un Centro de Ensayos Electrónicos operado por el ministerio de Defensa del Reino Unido.

En 2005, a raíz de estas revelaciones y de los desafíos legales posteriores, el ICCL se unió con Liberty y British-Irish Rights Watch para presentar una demanda ante el Tribunal Europeo de Derechos Humanos (TEDH), alegando que esa masiva “expedición de pesca” de datos había vulnerado la privacidad de sus comunicaciones telefónicas inter-organizacionales, en violación del artículo 8 de la Convención Europea de Derechos Humanos (CEDH), y que la interceptación en masa de todas las comunicaciones entre el Reino Unido e Irlanda entre 1990 y 1997 había sido desproporcionada y carecía de transparencia. La Corte de Estrasburgo estuvo de acuerdo, dictaminando que el gobierno del Reino Unido debe “disponer, en una forma que sea accesible a la población, cualquier indicación sobre el procedimiento a seguir para seleccionar para su inspección, intercambio, almacenamiento y destrucción material interceptado”, y que la vigilancia que se había llevado adelante durante dicho período no protegió los derechos a la privacidad de los demandantes, establecidos en el artículo 8 de la CEDH “de conformidad con la ley”.

conclusión

El posible espionaje de la GSOC expuso algunas fisuras muy significativas en el panorama de la vigilancia irlandesa y, en particular, en la capacidad y voluntad de las autoridades públicas para brindar una supervisión eficaz. La GSOC, a fin de cuentas, pudo o no haber sido objeto de vigilancia por parte de agentes del Estado. Sin embargo, como demostró el informe del juez que tuvo una mirada acotada sobre el asunto, se hicieron pocos esfuerzos para determinar si la actividad de vigilancia había tenido realmente lugar. Es perfectamente posible que la vigilancia encubierta se haya llevado a cabo e incluso que haya sido autorizada desde el más alto nivel. Nada de lo que se ha dicho, sea oficialmente o en los hallazgos posteriores de la investigación, ha invalidado esa posibilidad.

Lo que es evidente es que el juez perdió la muy significativa oportunidad de hacer las preguntas correctas a las personas adecuadas. ¿Qué se sabe acerca de la actividad de vigilancia del Estado? ¿Qué se está haciendo para garantizar que los estándares sean controlados y mantenidos? ¿Qué tipo de jurisdicción de vigilancia existe en Irlanda, y sobre quién recae la responsabilidad por las faltas cometidas? En otras palabras, ¿quién, si es que hay alguien, vigila de manera efectiva a los vigilantes?

Tanto el escándalo de las escuchas como el marco legislativo vigente en materia de vigilancia apuntan inextricablemente a la necesidad de una reforma significativa en el área. Se necesita con urgencia una revisión independiente y eficaz y una auditoría a intervalos regulares llevada a cabo por una autoridad reguladora independiente. Sin esa reforma, Irlanda seguirá siendo una “zona oscura” entre sus pares internacionales y de la UE en cuanto a la escasez de mecanismos de control interno para la supervisión y rendición de cuentas que son necesarios para asegurar el uso legítimo de la vigilancia por parte de agentes del Estado. Lo que es más, dadas las revelaciones del mal uso previo de los datos por parte de organismos tanto extranjeros como nacionales, y mientras la tecnología siga desarrollándose (generando oportunidades nuevas e innovadoras que habiliten un mayor monitoreo y vigilancia), lo que se perderá será, probablemente, la confianza de la población.

Un vistazo a la vigilancia en Irlanda

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
Sí.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
Sí.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Ninguna de las dos opciones.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Lo estrecharía.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
Sí.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí (*Maximillian Schrems v Data Protection Commissioner*).

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
No ha modificado su percepción.

notas
-

1. La denominación Teachta Dála refiere a los miembros de la cámara baja del Parlamento irlandés (N. de la T.).
2. Ley de Justicia Penal (Vigilancia) 2009, Sección 1.
3. Yvonne Daly. "Legislative Developments – Criminal Justice (Surveillance) Act 2009", *Revisión Anual de la Ley de Irlanda 2009*, 2010, p. 341.
4. *Communications* (*Retention of Data*) *Act 2011*, Sección 6. Disponible en: http://www.irishstatutebook.ie/2011/en/act/pub/0003/print.html [28/10/2016]
5. "More robust oversight of surveillance laws is 'crucial', experts warn", *Irish Examiner* (15 de junio, 2015). Disponible en: http://www.irishexaminer.com/ireland/more-robust-oversight-of-surveillance-laws-is-crucial-experts-warn-336910.html [28/10/2016]
6. Vodafone. "Country-by-country disclosure of law enforcement assistance demands" (2014). Disponible en: http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html [28/10/2016]
7. "UK Spy Base GCHQ tapped Irish internet Cables", *The Irish Times* (6 de diciembre, 2014). Disponible en: http://www.irishtimes.com/news/crime-and-law/government-accused-of-cowardice-over-tapping-of-cables-1.2022045 [28/10/2016]
8. Instrumento legislativo 541. Disponible en: www.irishstatutebook.ie/eli/2007/si/541/made/en/pdf [28/10/2016]

El caso Makaburi: el rol de la vigilancia en los asesinatos extrajudiciales

9
KENIA

El clérigo musulmán Abubakar Shariff Ahmed, también conocido como Makaburi, discute con altos oficiales de la policía fuera de la mezquita de Masjid Musa en Mombasa, Kenia, el 5 de febrero de 2014. Foto: AP

KENIA

El caso Makaburi: el rol de la vigilancia en los asesinatos extrajudiciales

Se espera que una de las prioridades predominantes de un gobierno sea proteger la seguridad nacional. En Kenia, el terrorismo se ha convertido en una de las mayores amenazas a la seguridad nacional, ya que cientos de ciudadanos y residentes del país han sido asesinados y muchos más han resultado heridos por terroristas en los últimos años. Si bien está dentro de los intereses principales del gobierno keniano hacer frente a esta amenaza con firmeza, debe hacerlo honrando los principios constitucionales del país –principios que reconocen el respeto de los derechos y libertades fundamentales del individuo como esenciales para el interés nacional. Por desgracia, Kenia parece estar en un camino que, paradójicamente, sacrifica los derechos y las libertades fundamentales en nombre de la seguridad nacional. Para enfrentar la amenaza terrorista, se han promulgado leyes que han ampliado el poder del Estado a expensas de las libertades individuales, incluyendo leyes que han eliminado cualquier límite significativo a la autoridad del gobierno para vigilar. Esto es particularmente preocupante dado el historial de abuso de los poderes de vigilancia en Kenia por parte de agentes de seguridad, que a menudo han empleado la vigilancia al servicio de graves violaciones de los derechos humanos, tales como la tortura y las ejecuciones extrajudiciales. El caso que exponemos a continuación es uno de los tantos que han profundizado la preocupación de que los poderes de vigilancia están siendo utilizados, una vez más, no para apoyar investigaciones policiales y procesos judiciales, sino para apoyar el asesinato selectivo.

el caso

Abubakar Shariff Ahmed, conocido ampliamente por su apodo “Makaburi” (que significa “tumbas” en suajili), era un clérigo musulmán que vivía en la ciudad costera de Mombasa y que predicaba en la controvertida mezquita de Masjid Musa, donde sus jóvenes y ardientes seguidores lo consideraban un jeque[1] que hablaba con valentía acerca de la opresión a la que eran sometidos los musulmanes en Kenia.

Makaburi había asumido la dirección de la mezquita después de que otros dos polémicos clérigos considerados sus allegados hubieran muerto en circunstancias turbias: Aboud Rogo, en 2012, e Ibrahim Ismail al año siguiente. Al igual que los de Rogo e Ismail, los sermones de Makaburi estaban llenos de referencias a lo que él consideraba las guerras injustas de Occidente contra los musulmanes de todo el mundo. Estos clérigos también llamaban a sus seguidores a levantarse y defender su fe, en exaltadas exhortaciones que sus críticos veían como una distorsión a los verdaderos principios de la fe musulmana, orientadas claramente hacia el extremismo y la radicalización. Para el gobierno de Kenia, estos sermones eran más que teológicos: consideraba a la mezquita de Masjid Musa como un centro de radicalización y reclutamiento de jóvenes musulmanes para la agrupación terrorista Al Shabab, en la guerra en curso en la vecina Somalia.

En 2010 y 2011 Al Shabab, cuya base está en Somalia pero opera una red de células dentro de Kenia, llevó a cabo una serie de secuestros de extranjeros en hoteles de la costa keniana y en las zonas del norte del país. En respuesta, las tropas de las Fuerzas de Defensa de Kenia (KDF) se trasladaron en octubre de 2011 a Somalia en la “Operación Linda Nchi”. La KDF y la misión de paz de la Unión Africana en Somalia (AMISOM) desalojaron con rapidez a Al Shabab de la ciudad portuaria meridional de Kismayo, pero los éxitos militares de Kenia en Somalia fueron recibidos con una escalada de ataques terroristas en el país. Desde el inicio de la Operación Linda Nchi hasta septiembre de 2014, según las estadísticas publicadas por la Unidad de Policía Antiterrorista de Kenia (ATPU), 264 personas murieron y 923 resultaron heridas en 133 ataques terroristas en Kenia.

Mientras los atentados aumentaban, Makaburi atrajo cada vez más la atención del gobierno keniano y de las agencias de inteligencia internacionales. En 2012, el Departamento del Tesoro de Estados Unidos lo designó como partidario de Al Shabab, declarando que:

Abubaker Shariff ha predicado en las mezquitas de Mombasa que los jóvenes deben viajar a Somalia, cometer actos extremistas, luchar por Al Qaeda y matar a ciudadanos estadounidenses. Abubaker Shariff Ahmed fue detenido por las autoridades de Kenia a fines de diciembre de 2010 por su presunta participación en la explosión en una terminal de autobuses de Nairobi. Abubaker Shariff Ahmed es también líder de una organización juvenil keniana en Mombasa con vínculos con Al Shabab. A partir de 2010, Abubaker Shariff Ahmed fue reclutador y facilitador para Al Shabab en la zona de Majengo, en Mombasa.

En los dos años siguientes, Makaburi fue detenido tres veces más, acusado la primera vez de haber cometido un robo violento; la segunda, de ser un miembro de Al Shabab; y la tercera, de incitar a la violencia juvenil en Mombasa. Pero el gobierno de Kenia nunca consiguió pruebas suficientes para condenar a Makaburi por ninguno de esos cargos, y el predicador expresó abiertamente que estaba siendo acosado judicialmente. "¿Cómo que soy un terrorista? ¿A quién he aterrorizado?" preguntó durante una entrevista con Al Jazeera en 2013. "Estoy ante los tribunales desde hace 3 años y no se ha demostrado nada en mi contra. Yo soy el que está siendo aterrorizado; mi vida es la que está en peligro". Llegó tan lejos como para demandar al gobierno keniano por el secuestro ilegal de su propiedad después de un registro domiciliario de 2011, recuperando satisfactoriamente 670.000 chelines kenianos (aproximadamente 6700 dólares) por daños y perjuicios. El tribunal compensó los daños una semana antes de que fuese abatido a tiros después de asistir a una audiencia en la corte el 1 de abril de 2014 en relación con un caso penal presentado contra él.

Aproximadamente seis meses antes de la muerte de Makaburi, el 21 de septiembre de 2013, un ataque terrorista en el centro comercial Westgate en Nairobi dejó al menos 50 muertos y 170 heridos. Después del atentado, Makaburi fue citado diciendo que los homicidios estaban justificados. "No es terrorismo porque en la ley islámica [sharia] tenemos la venganza", le dijo a un periodista. "El ejército de Kenia está haciendo lo mismo con la gente de Somalia […] el Corán dice ojo por ojo". En ese tiempo reconoció que las autoridades kenianas estaban cada vez más frustradas por su incapacidad para procesarlo, y comenzó a decir que era solo cuestión de tiempo para que lo ejecutaran. Hablaba más y más sobre el martirio, alegando que cualquier jeque que enseñara religión islámica, incluyendo la yihad, es asesinado en Kenia. Durante una entrevista televisiva en octubre de 2013, Makaburi fue más específico acerca del origen de la amenaza, afirmando que el "Recce", un escuadrón de élite de la Unidad de Servicios Generales (GSU) de la Policía Nacional de Kenia, tenía luz verde para asesinarlo, como había hecho antes con sus colegas. A pesar de declarar que estaba listo para morir, Makaburi comenzó a tomar precauciones de seguridad, pasando las noches en diferentes lugares y viviendo lejos de su esposa e hijos.

El 1 de abril de 2014, Abubakar Shariff Ahmed, alias Makaburi, fue asesinado a tiros por desconocidos en las inmediaciones de los tribunales de Shanzu en Mombasa, colapsando bajo una lluvia de balas en el mismo tramo de la calle en la que Aboud Rogo e Ibrahim Ismail habían sido asesinados de manera similar. Su muy pública muerte dejó en claro lo que ya para entonces era una sospecha que prevalecía: que la policía de Kenia se había embarcado en ejecuciones extrajudiciales como parte de sus esfuerzos contra el terrorismo. Y apareció una nueva e inquietante pregunta: ¿en qué medida estos homicidios fueron alentados por la información obtenida de sistemas en proliferación de vigilancia nacional e internacional?

el contexto

Como la Kenya Human Rights Commission (KHRC) y otras organizaciones de la sociedad civil kenianas han documentado, Kenia tiene un historial de ejecuciones extrajudiciales, uno en el que la GSU de la policía, en

Un policía keniano armado patrulla los alrededores de la mezquita de Masjid Musa, donde el clérigo musulmán Sheikh Ibrahim Ismail fue asesinado tras los disturbios ocurridos después de las oraciones del viernes en la zona de Mombasa, Kenia, el 4 de octubre de 2013. Foto: AP

particular, actúa con impunidad. A mediados y finales de la década de 2000, la GSU estaba vinculada a los asesinatos y desapariciones de cientos de miembros de una secta y banda criminal prohibida conocida como los Mungiki;[2] el aumento de las muertes violentas de clérigos musulmanes identificados como radicales también apuntó a un programa de eliminación similar.

Mientras que las ejecuciones extrajudiciales de miembros de los Mungiki se produjeron durante las campañas de violencia y extorsión de la organización contra otras comunidades, los asesinatos de clérigos se produjeron durante la intensificación de las actividades terroristas de Al Shabab en Kenia.[3] Estos ataques están teniendo un efecto devastador en el bienestar social y económico de la región norte del país, en particular, que está sufriendo un éxodo masivo de profesores no musulmanes y otros funcionarios que han sido blanco de ataques terroristas.

Los funcionarios del gobierno keniano han buscado hacer frente al terrorismo creciente con fuerza y decisión, afirmando que no cederán en su guerra contra el terrorismo. Inmediatamente después del lanzamiento de la Operación Linda Nchi, el presidente Mwai Kibaki declaró: “La seguridad de nuestro país es de suma importancia. Vamos a defender nuestra integridad territorial a través de todas las medidas necesarias para garantizar la paz y la estabilidad”.[4] Originalmente se entendió que el mensaje definiría la misión y las operaciones de la KDF en Somalia, pero a medida que aumentaron los ataques en Kenia, la estrategia antiterrorista fue claramente aplicada a nivel doméstico. Ya en octubre de 2011, el gobierno estaba considerando una operación de seguridad en Nairobi para purgar la ciudad de militantes y simpatizantes de Al Shabab. “[Al Shabab] es como un gran animal con su cola en Somalia”, dijo entonces el ministro asistente de seguridad interna. “Todavía estamos luchando con la cola, y la cabeza está asentada aquí [en Nairobi]”.[5]

Sobre el terreno, las operaciones de seguridad en Kenia consistieron en gran medida en redadas policiales dirigidas contra inmigrantes ilegales y personas indocumentadas, que son percibidas como la fuente de las amenazas internas. Estas operaciones han provocado acusaciones de discriminación contra los miembros de las comunidades somalíes y musulmanas, y se dice que han incluido violaciones contra los derechos humanos tales como detenciones prolongadas, extorsión y saqueo de bienes, agresiones físicas y violencia y, en algunos casos extremos, ejecuciones extrajudiciales.

Una de las redadas de seguridad más notables, la Operación Usalama Watch, ocurrió en abril de 2014 tras una serie de ataques con granadas en Nairobi y Mombasa. Las incursiones fueron tan extensas que el Estadio Nacional de Kasarani se convirtió en un centro masivo de detención de refugiados urbanos y de personas sospechosas de estar ilegalmente en el país. Las organizaciones de derechos humanos caracterizaron inmediatamente a la operación como discriminatoria e inconstitucional. La redada parecía apuntar solo a los refugiados somalíes, a los kenianos de etnia somalí, a los etíopes, a los sudaneses del sur y a otras poblaciones musulmanes de Kenia. Algunos de los detenidos acusaron a la policía de extorsión e informaron que habían sido detenidos en condiciones deplorables y sin acceso a sus familiares o representantes legales. Los refugiados de zonas urbanas fueron trasladados por la fuerza a campos de refugiados, y algunos fueron deportados sumariamente a Somalia desde Kenia, en lo que seguramente viola el principio de no devolución de la Convención de Refugiados de 1951 y de la Convención de la Organización para la Unidad Africana de 1969, que regula los aspectos específicos del problema de los refugiados en África. La comunidad de derechos civiles no fue la única en protestar. El gobierno recibió fuertes críticas de la población por las redadas indiscriminadas en sus operaciones de seguridad, que rara vez descubrían actividades terroristas o amenazas significativas. Las detenciones masivas fueron calificadas como ejercicios de propaganda y una demostración de la incapacidad del gobierno para hacer frente a la amenaza terrorista. El gobierno se encontró bajo la presión de tener que desarrollar una estrategia de seguridad basada en la inteligencia, antes que en la fuerza bruta.

> “¿En qué medida estos homicidios fueron alentados por la información obtenida de sistemas de vigilancia nacional e internacional en proliferación?”

En respuesta, la estrategia ha llegado a depender cada vez más de la vigilancia en general y de la vigilancia digital en particular. El gobierno de Kenia ha invertido mucho en tecnología de vigilancia y ha ampliado significativamente la autoridad de los organismos de seguridad del Estado, en particular del Servicio Nacional de la Policía (NPS) y del Servicio Nacional de Inteligencia (NIS), para llevar a cabo actividades de vigilancia digital. En 2012 dos leyes importantes –La Ley Nº 30 de Prevención del Terrorismo y la Ley Nº 28 del Servicio Nacional de Inteligencia– recortaron los derechos a la privacidad y ampliaron la capacidad de la policía para actuar ex parte y le dieron autoridad de emergencia para controlar comunicaciones. Otra ola de enmiendas y leyes promulgadas en 2014 continuó la tendencia, criminalizando publicaciones y demás expresiones “que pudieran entenderse como una inducción directa o indirecta a cometer un acto terrorista”,[6] autorizando a los órganos de seguridad nacionales a interceptar comunicaciones con el propósito de detectar, disuadir e interrumpir el terrorismo, sin obtener una autorización judicial y, en su lugar, siguiendo los procedimientos a ser prescritos por el secretario de gabinete encargado de la seguridad interna.

Las enmiendas de 2014 se aprobaron en circunstancias reñidas que incluyeron enfrentamientos violentos entre legisladores de la Asamblea Nacional. La KNCHR se unió a la Coalición para la Reforma y Democracia (CORD, el principal partido de la oposición) y otras organizaciones de la sociedad civil para denunciar la Ley de Leyes de Seguridad (Enmienda) ante los tribunales, y, el 23 de febrero de 2014, la Corte Suprema declaró que varias disposiciones de la Ley que restringían publicaciones y expresiones eran inconstitucionales, pero permitió que se conservara la autoridad para interceptar comunicaciones sin una orden judicial.

Estos nuevos poderes de vigilancia llegaron cuando Kenia todavía estaba luchando para reformar las estructuras de seguridad e inteligencia del Estado, que se habían utilizado con frecuencia para atacar a opositores políticos y suprimir el disenso. Un informe de 2013 de la Comisión de la Verdad, la Justicia y la Reconciliación de Kenia (TJRC) detalló de qué manera la notable Dirección Especial de la policía nacional supervisó un sistema de inteligencia que incluyó la detención y tortura de disidentes políticos durante la lucha por la democracia pluripartidista en la década de 1980. Provista de poderes de vigilancia digital mucho mayores, la Unidad de Policía Antiterrorista (ATPU) de la policía nacional está haciéndose rápidamente de una reputación similar, alimentada por las sospechas de vigilancia y ejecución de varios clérigos musulmanes de la región costera keniana. Por otra parte, en julio de 2015 se reveló que el Servicio de Inteligencia Nacional de Kenia había solicitado software de hackeo a un proveedor italiano de software de vigilancia malicioso conocido como Hacking Team, y le había pedido a la

> El vínculo entre la lucha contra el terrorismo, las ejecuciones extrajudiciales y la vigilancia digital está demostrando ser un área de creciente preocupación que requerirá de una mayor investigación o escrutinio.

compañía que cerrara una página web perteneciente a un popular bloguero, crítico del actual gobierno.[7]

Nuestra organización, KHRC, ha participado en diversas iniciativas de promoción que han intentado echar luz sobre las oportunidades y los riesgos planteados por internet en relación con las libertades civiles. Además de cuestionar los poderes de vigilancia otorgados al Estado en la guerra contra el terror, la KHRC ha mapeado el contexto legislativo y político respecto de internet en Kenia. La KHRC también ha llamado la atención y se ha manifestado en contra del acoso a los blogueros y defensores de los derechos humanos sobre la base de lo que publican *online*. El vínculo entre la lucha contra el terrorismo, las ejecuciones extrajudiciales y la vigilancia digital está demostrando ser un área de creciente preocupación que requerirá de una mayor investigación o escrutinio.

El 7 de diciembre de 2014, Al Jazeera transmitió un informe sobre el asesinato de Makaburi en el que varios agentes no identificados declararon ante cámaras que habían formado parte del escuadrón de la muerte al que se le encargó asesinar al polémico clérigo después de que los intentos de procesarlo en la corte hubieran fallado. “Makaburi en Mombasa es una persona muy peligrosa para nuestro país”, declaró en el informe un oficial identificado como “El comando”, del grupo Recce, la élite de la Unidad de Servicios Generales. “¿Qué se hace con una persona así? ¿La perdonas por estar pendiente de los derechos humanos?”.[8]

Al Jazeera informó[9] que su investigación había descubierto la colaboración entre la Unidad Antiterrorista de la policía (ATPU), el Servicio Nacional de Inteligencia (NIS), la Unidad de Radiación del servicio regular de la policía y el equipo Recce, de la GSU, para supervisar el asesinato de personas consideradas como amenazas terroristas. Su investigación reveló que individuos como Makaburi fueron colocados bajo vigilancia por el NIS, que tenía la tarea de elaborar perfiles de personas de interés, incluyendo dónde iban y con quién se reunían o visitaban. La información se usaba a continuación para decidir si la persona de interés sería eliminada. “Nos movemos tácticamente para entender lo que está ocurriendo en el terreno”, dijo a Al Jazeera un oficial del NIS identificado sencillamente como “El espía”. “Recolectamos esa información y a continuación se la damos a la fuente correcta para que se tome una acción”. De acuerdo con el informe de Al Jazeera, el NIS envía su información de vigilancia al Consejo de Seguridad Nacional de Kenia (NSC), el más alto órgano de seguridad del país, que incluye al presidente, el vicepresidente, el secretario del gabinete para el interior, el secretario del gabinete para la defensa, el procurador general, el director del NIS, el inspector general de la policía y el jefe de las Fuerzas de Defensa de Kenia. El NSC decide si emite una orden de ejecución, que llega a un escuadrón de la muerte del grupo Recce. El oficial de Recce identificado como “El comando” dijo a Al Jazeera que los asesinatos se dirigen específicamente a figuras influyentes, como clérigos radicales. “Cuando nos llega la información de que ‘tal y tal’ están organizando a un

Hombres musulmanes son detenidos en la mezquita de Masjid Musa en Mombasa, Kenia, el 2 de febrero de 2014. Hubo tiroteos dentro y alrededor de la mezquita después de una redada de policías armados, que habían recibido un aviso anónimo de que jóvenes musulmanes estaban siendo radicalizados y entrenados para llevar adelante ataques militares. Foto: Joseph Okanga/Reuters

grupo determinado que podría aterrorizar a la gente, la primera persona de la que hay que deshacerse es del líder", dijo.

Esta, informó Al Jazeera, fue exactamente la secuencia de eventos que se siguió en el asesinato de Makaburi. Una serie de cables de inteligencia obtenidos por Al Jazeera, atribuidos al Departamento de Investigación Criminal de Kenia (CID), confirmaron que Makaburi había sido objeto de una intensa vigilancia a lo largo de 2013. Aunque redactados en varias áreas, los cables indican que Makaburi se convirtió en una preocupación para los órganos de seguridad que creían que estaba planeando activamente y financiando una serie de ataques terroristas en el país, y que en abril de 2013 se había declarado a sí mismo el "Amir" de todos los agentes de Al Shabab en el país. Es esta la inteligencia que se dice que persuadió al NSC para autorizar el asesinato de Makaburi en abril de 2014. En los escalofriantes testimonios de los oficiales no identificados de las unidades de la ATPU, unidades de Recce y Radiación destacados en la investigación de Al Jazeera, los funcionarios reconocieron que la ejecución de Makaburi fue planeada en Nairobi por oficiales de alto rango de la policía y funcionarios del gobierno. También admitieron que eran responsables de la muerte de otros clérigos musulmanes.

Entre las muchas revelaciones explosivas de la investigación de Al Jazeera, hubo acusaciones de que la vigilancia detrás de las ejecuciones extrajudiciales habían sido facilitadas y apoyadas por gobiernos extranjeros que eran socios en la "guerra global contra el terrorismo". Además de recibir apoyo financiero y equipamiento, los agentes de seguridad alegaron que el gobierno británico había brindado entrenamiento sobre cómo llevar a cabo la vigilancia "de manera avanzada" para obtener información. Estas fuentes afirmaron además que la unidad Recce recibe formación de Israel, que la formación incluye instrucciones sobre cómo eliminar a personas de interés y que el escuadrón de la muerte a menudo se basaba en información de socios extranjeros para identificar sus objetivos. "Una vez que nos dan la información, mañana [el objetivo] ya no está", dijo uno de los agentes a Al Jazeera.

Cuando el informe de Al Jazeera fue transmitido, los gobiernos de Gran Bretaña e Israel negaron públicamente las afirmaciones de que eran cómplices de las ejecuciones extrajudiciales de clérigos musulmanes. El gobierno británico llegó a afirmar que le había expresado su preocupación por las ejecuciones extrajudiciales al gobierno de Kenia.

conclusión

En el momento más alto del debate público en torno a la promulgación de la Ley de Leyes de Seguridad (Enmienda) de 2014, el portavoz del

gobierno afirmó que Kenia se había unido a "la larga lista de democracias que han actualizado sus leyes de seguridad para garantizar la protección de los ciudadanos de organizaciones terroristas y criminales que operan con una creciente sofisticación y brutalidad". Pero las ejecuciones de Makaburi y de otros clérigos musulmanes han despertado el fantasma de una ilegalidad cada vez más sofisticada y brutal por parte del gobierno keniano, dirigida específicamente a los ciudadanos de Kenia; una en la que la información recabada por el espionaje digital dentro del país y compartida por gobiernos extranjeros constituye la base para emitir órdenes secretas de asesinato, sin el debido proceso constitucional o legal.

No hay dudas de que Kenia se enfrenta a problemas graves y legítimos de seguridad. Más de 300 personas han muerto en ataques terroristas cometidos en suelo keniano desde 2011. Sin embargo, la respuesta del Estado a tal terror debe acatar la Constitución de Kenia y respetar las obligaciones para con los derechos humanos, incluso al lidiar con quienes tienen puntos de vista extremos y repugnantes. A quienes son sospechosos de ser terroristas o de trabajar con terroristas se les debe conceder el debido proceso y juzgárselos en un tribunal. No hacerlo crea una cultura de la impunidad que terminará socavando las salvaguardias que garantizan que las personas son inocentes hasta que se demuestre lo contrario ante la justicia.

La ejecución de Makaburi y de otros clérigos deja en claro que las operaciones de contraterrorismo en Kenia no siempre se han ajustado a las normas de la Constitución del país. Y, al parecer, las ejecuciones extrajudiciales no han sido dirigidas solo contra clérigos. La KHRC y otras organizaciones de derechos humanos están recibiendo cada vez más denuncias de desapariciones de jóvenes de la región de la costa norte de Kenia, presuntamente detenidos por la Unidad de Policía Antiterrorista.

Al mismo tiempo, hay cada vez más indicios de que la vigilancia antiterrorista del gobierno ahora está orientada no solamente hacia los sospechosos de terrorismo, sino también a periodistas y blogueros que discuten sobre terrorismo y otros temas controvertidos. Empleando las disposiciones de una ley que penaliza "el uso indebido de un sistema de telecomunicaciones", la policía ha iniciado una vigilancia excesiva de las redes sociales, y ha habido un marcado aumento de los casos de personas que están siendo arrestadas o interrogadas sobre la base de lo que comparten en blogs y plataformas sociales. En enero de 2016 el periodista Yassin Juma fue detenido por publicar en sus redes actualizaciones sobre un reciente ataque a las Fuerzas de Defensa de Kenia (KDF) por parte de Al Shabab en Somalia. Fue más preocupante aún el caso de Judith Akolo, otra periodista que en enero de 2016 fue convocada para ser interrogada por la Dirección de Investigación Criminal por retuitear el post de un bloguero conocido por proporcionar información actualizada sobre temas de seguridad de Kenia; ese mismo bloguero fue también llevado a un interrogatorio. Y en un avance especialmente preocupante, lo que comenzó como una vigilancia en línea orientada a posibles amenazas terroristas se ha ampliado para incluir el seguimiento y la penalización de actividades expresivas que nada tienen que ver con el terrorismo, sino más bien con blogueros que están siendo detenidos por ocasionar molestias al publicar historias sobre diversos líderes políticos.[10]

La turbulenta historia de los derechos humanos en Kenia nos ha enseñado que las fuerzas de seguridad de nuestro país necesitan más, no menos, garantías para proteger la seguridad y los derechos de los ciudadanos kenianos. Pero las nuevas leyes le han dado a las fuerzas de seguridad del país, históricamente propensas a abusar de su autoridad en operaciones de seguridad, aún mayor discrecionalidad en la forma en que llevan a cabo la vigilancia. Esta vigilancia sin supervisión no ha dado lugar a procesamientos legales; en cambio, ha conducido a una cultura del miedo, el acoso, la autocensura y, al parecer, a ejecuciones extrajudiciales en manos de un escuadrón de la muerte autorizado por el Estado.

notas

-

1. En este contexto, jeque [*shayj* o *sheyj*] debe comprenderse como líder o referente religioso; no político (N. de la T.).
2. Comisión Nacional de Kenia sobre Derechos Humanos (KNCHR). El Informe "The Cry of Blood" sobre ejecuciones y desapariciones extrajudiciales (2008). El informe señala que para noviembre de 2007, la KNCHR había tenido conocimiento de 500 casos de ejecuciones extrajudiciales, donde la policía pudo haber actuado como cómplice. Disponible en: http://www.africancrisis.org/Docs/crimes-against-humanity-extra-judicial-killings-by-kenya-police-exposed.pdf [28/10/2016]
3. En 2015 la frecuencia y devastación de los ataques creció aún más. El más notable fue contra la Universidad de Garissa, donde se informó de la muerte de 147 civiles, incluyendo estudiantes y personal universitario. Otros atentados atribuidos a Al Shabab han tenido lugar en los condados de Wajir, Mandera y Lamu, buscando avivar las divisiones religiosas y étnicas en esas áreas.
4. "Kenya to target al Shabaab sympathisers in Nairobi", *BBC* (2011). Disponible en: http://www.bbc.com/news/world-africa-15384331 [28/10/2016]
5. *Ibíd.*
6. *The Security Laws (Amendment) Act* 2014, Sección 64. Disponible en: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf [28/10/2016]
7. Ver Wikileaks: https://www.wikileaks.org/hackingteam/emails/?q=kensi.org [28/10/2016]
8. *Inside Kenya's Death Squads*. Disponible en: http://interactive.aljazeera.com/aje/KenyaDeathSquads/ [28/10/2016]
9. *Ibíd.*
10. Ver Asociación de Blogueros de Kenia (BAKE): http://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/ [28/10/2016]

Un vistazo a la vigilancia en Kenia

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
Sí.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
No.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
Sí.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Han aumentado.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
Lo ampliaría.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
No.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
Sí.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
Sí.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
Menos.

Espiar para otros: casos problemáticos de vigilancia transnacional

10
SUDÁFRICA

Kumi Naidoo, entonces director de Greenpeace, habla frente a Aurora: un oso polar de dos pisos de altura, operado mecánicamente e instalado por activistas de la organización durante la Conferencia de las Naciones Unidas sobre Cambio Climático (COP21) en Le Bourget, al norte de París, Francia, el 9 de diciembre de 2015. Foto: Francois Mori/AP

SUDÁFRICA

Espiar para otros: casos problemáticos de vigilancia transnacional

el caso

Kumi Naidoo, de nacionalidad sudafricana, tiene largos antecedentes como activista. En su temprana adolescencia, durante la era del apartheid en Sudáfrica, Naidoo comenzó a organizar a su comunidad, trabajando con jóvenes del barrio y movilizando masivas manifestaciones contra el régimen. En 1980, con solo 15 años, fue detenido, expulsado de la escuela secundaria y amenazado con una pena de prisión de 15 años. Naidoo pasó a la clandestinidad durante algún tiempo y, finalmente, se exilió en Inglaterra, donde realizó estudios de postgrado en la Universidad de Oxford. Regresó a Sudáfrica un mes después de que Nelson Mandela fuese elegido presidente, y trabajó como investigador, periodista, profesor universitario y consejero juvenil, y durante diez años dirigió CIVICUS, una ONG internacional centrada en la participación ciudadana.

En 2009 Naidoo se unió a Greenpeace como director ejecutivo internacional. Persuadido para asumir el cargo por su hija Naomi, Naidoo consideró su papel en Greenpeace como formador de alianzas y agente de cambio. Es importante señalar que, comprendiendo las intrincadas conexiones entre la justicia ambiental, los derechos de la mujer y los derechos humanos, asumió su trabajo con el objetivo de reforzar los tres.

A principios de 2015, la cadena de noticias Al Jazeera consiguió una filtración de cables de inteligencia que revelaban que Corea del Sur había identificado a Naidoo como una posible amenaza a la seguridad durante la cumbre del G-20 que tuvo lugar en Seúl en noviembre de 2010. De acuerdo con los cables, Corea del Sur había pedido a Sudáfrica "evaluaciones de seguridad específicas" sobre Naidoo, vinculándolo con otros dos sudafricanos que habían sido arrestados en una redada contraterrorista en Pakistán (pero que más tarde habían sido puestos en libertad y devueltos a Sudáfrica). Sudáfrica nunca informó a Naidoo sobre la solicitud de Corea del Sur, que se enteró por una llamada telefónica de un periodista de Al Jazeera y que todavía desconoce si el Estado cumplió con la solicitud o si se ha hecho algo con la información que, como respuesta, se puede haber proporcionado.

Con toda razón, a Naidoo le preocupó el cable filtrado. Como le dijo a un periodista al enterarse sobre la posible operación de vigilancia:

Mi reacción principal cuando me contactó Al Jazeera no fue de sorpresa, frustración o enojo; fue de tristeza, dolor y decepción.[1]

Naidoo había visitado Corea del Sur varias veces, y cree que su servicio de inteligencia hizo la solicitud debido a su abierta oposición a la energía nuclear. Familiarizado con las acciones de vigilancia en su juventud, a Naidoo le preocupaba que el gobierno sudafricano estuviese revisitando viejos hábitos de la era apartheid. Por ahora, sin embargo, lo que busca son sobre todo respuestas; como comentó en el artículo:

Quiero creer que mi gobierno me confirmará que no ha sido el caso y que no ha dado información sobre mí a ningún tercero, se trate de agencias de Corea del Sur u otras.

En julio de 2015, el Legal Resources Centre (LRC) emitió un pedido de acceso a la información de parte de Naidoo a la Agencia Estatal de Seguridad por registros relacionados con la operación de vigilancia solicitada. El LRC pidió específicamente:

- la solicitud de información recibida desde Corea del Sur mencionada en los cables filtrados respecto de Naidoo, Greenpeace y sus miembros;
- la respuesta de Sudáfrica a la solicitud de información emitida por Corea del Sur sobre Naidoo, Greenpeace y sus miembros;
- cualquier acuerdo, memorando de entendimiento u otro documento que asegurara, facilitara, fomentara o contemplara el intercambio de inteligencia entre Sudáfrica y Corea del Sur;
- cualquier solicitud de información recibida desde cualquier país con respecto a Naidoo, Greenpeace y sus miembros, y la respuesta dada por Sudáfrica; y

—cualquier solicitud de una orden de interceptación solicitada o concedida bajo la legislación sudafricana pertinente.

La Agencia de Seguridad del Estado no ha emitido ninguna respuesta a esa solicitud. Tal falta de acción es considerada un rechazo a la solicitud de conformidad con la legislación sudafricana. El LRC interpuso una apelación interna, pero tampoco obtuvo respuesta. En virtud de las leyes de acceso a la información, el siguiente paso haría necesario interponer un recurso judicial en términos de la Promoción de Acceso a la Información ACT2 del año 2000, con el fin de acceder a la información solicitada.

Entretanto, la respuesta pública del gobierno sudafricano a la información filtrada que sugería que podría haber estado vigilando a un ciudadano –un activista pacífico reconocido mundialmente– ha sido particularmente preocupante. En lugar de abrir un diálogo sobre posibles actividades de vigilancia, el gobierno condenó las filtraciones e indicó que una investigación completa –sobre las filtraciones, no sobre la posible vigilancia de Naidoo– había sido puesta en marcha. En una declaración del 25 de febrero de 2015, el ministro de Seguridad del Estado declaró que:

Si bien es una práctica internacional que los países compartan información de inteligencia sobre cuestiones transversales relativas a oportunidades económicas y de seguridad, entre otros asuntos, la filtración de documentos que detallan supuestos detalles del funcionamiento de la Agencia de Seguridad del Estado se condena en los términos más fuertes posibles. Bajo el marco jurídico y normativo que rige la gestión de la información clasificada en Sudáfrica, es ilegal revelar dicha información fuera de los protocolos de clasificación imperantes. Tal conducta tiene el peligroso efecto de socavar la eficacia operativa del trabajo para asegurar este país y raya con socavar las relaciones diplomáticas con nuestros socios de la comunidad internacional. Cualquier fuga de información clasificada socava la seguridad nacional de cualquier Estado.

Se ha puesto en marcha una investigación completa sobre la presunta filtración; su veracidad y verificación serán manejadas en los términos de los protocolos que rigen la gestión de la información clasificada.[2]

Los miembros del partido de la oposición que lidera el parlamento, la Alianza Democrática, advirtieron que esas revelaciones podrían utilizarse como excusa para presionar con un proyecto de Ley de Protección de Información de Estado que contendría disposiciones que, según las advertencias de las organizaciones de la sociedad civil, podrían tener un efecto negativo sobre informantes y periodistas. La campaña Right2Know, un grupo de la sociedad civil, se hizo eco de la advertencia:

Estamos seguros de que, a nivel local, las estructuras de seguridad del Estado sudafricano pintarán esas filtraciones como un acto hostil, y utilizarán el evento para buscar un mayor control sobre el flujo de información; esas filtraciones incluso se pueden utilizar como pretexto para convertir el proyecto de Protección de Información de Estado en Ley […] Es significativo que este importante acto de periodismo caiga fácilmente bajo el secretismo de la amplia y expansiva definición de "espionaje" incluido en el proyecto de ley, que conlleva penas de hasta 25 años de prisión, y no tiene defensa del interés público.[3]

También Naidoo expresó su decepción por la respuesta gubernamental a los cables filtrados:

Lo que no veo en los cables que están disponibles es de hecho una negativa del gobierno de Sudáfrica a los surcoreanos, que diga: "Este es un ciudadano nuestro que fue parte de la lucha por la liberación y que ha estado apoyando la democracia y los derechos humanos desde la edad de 15 años, y no creemos que haya ninguna razón para que ustedes hagan esa petición".[4]

el contexto

Durante muchos años, los activistas políticos de Sudáfrica han expresado su preocupación ante la posibilidad de que las estructuras de inteligencia del

> “A principios de 2015, la cadena de noticias Al Jazeera consiguió una filtración de cables de inteligencia (...) Corea del Sur había pedido a Sudáfrica ‘evaluaciones de seguridad específicas’ sobre Naidoo.”

Estado estén vigilando y monitoreando su trabajo, incluso en la era post-apartheid, y por que las agencias de inteligencia estén abusando de sus poderes. Mientras que algunos han llamado a esta tendencia “el ascenso de los segurócratas” por la forma en que el núcleo de seguridad sudafricano está siendo percibido como más reservado, expansivo e implicado en asuntos políticos, otros[5] se preguntan si los servicios de inteligencia de Sudáfrica fueron de veras reformados en la era democrática.

Una de las sagas de vigilancia más célebres de Sudáfrica fue la de las así llamadas cintas de espionaje. Las cintas contenían grabaciones realizadas por funcionarios de inteligencia de las conversaciones entre el ex jefe de la unidad de investigación del delito (llamada en su tiempo “los Escorpiones”) y el ex director de la Fiscalía Nacional, en relación con cargos de corrupción contra el presidente Jacob Zuma en 2007, por su supuesta participación en un escándalo de venta de armas.[6] La situación tuvo grandes ramificaciones políticas para todos los involucrados, y fue quizás una de las manifestaciones más evidentes del alcance de los servicios de inteligencia en la era post-apartheid. En efecto, lo que quedó claro es que nadie estaba más allá de la vigilancia, sin importar su posición. Como parte de un proceso judicial que se oponía a la decisión de retirar los cargos penales contra el presidente Zuma, se hizo posible que las propias cintas fuesen puestas a disposición de la población, dándole a esta una idea del tipo de información en la que los servicios de seguridad estaban interesados.[7]

El impacto de la vigilancia sobre los medios de comunicación y la sociedad civil es especialmente preocupante. Por ejemplo, en octubre de 2011, el entonces Inspector General de Inteligencia (IGI) confirmó que las llamadas telefónicas de un periodista del *Sunday Times* habían sido controladas por la unidad de investigación de los Servicios de Policía de Sudáfrica.[8] El IGI insistió en que la vigilancia era “parte de un método de investigación legal” que “fue aprobado por el juez designado en relación con [el periodista] en referencia a acusaciones criminales, y no porque se tratara de un periodista”. El periodista fue posteriormente detenido en las oficinas del *Sunday Times* y se le incautaron sus anotadores, computadora y teléfono móvil. A continuación fue acusado de fraude, falsificación y puesta en circulación de documentación falsa, pero esos cargos no fueron procesados. Las acciones de la policía han sido ampliamente criticadas por ser nada más que tácticas para intimidar al periodista y evitar que revelara información que podría haber sido perjudicial para personas en el poder. También ha habido preocupaciones posteriores que plantearon que se han utilizado acciones de vigilancia para espiar a miembros de los medios involucrados en actividades periodísticas legítimas, y que eso ha sido posible gracias a los bajos niveles de supervisión de los organismos involucrados.

Estos incidentes han planteado serias inquietudes acerca de la eficacia de la legislación que autoriza la vigilancia post-apartheid, y que está destinada a garantizar que esta se lleve a cabo de manera legal y con una supervisión adecuada. Debido a que los servicios de inteligencia del régimen del apartheid sudafricano se utilizaron de manera rutinaria para hostigar a los críticos políticos del régimen, desde la transición a la democracia, en 1994, el nuevo gobierno ha tomado medidas para revisar los alcances de los servicios de inteligencia. Sin embargo, un amplio énfasis en la seguridad nacional se ha traducido en un amplio y persistente alcance de los servicios de inteligencia.

En 2002, Sudáfrica aprobó la Ley de Regulación de la Interceptación de Comunicaciones y Provisión de Información Relacionada con las Comunicaciones (RICA) para regular la vigilancia de las comunicaciones. Sujeta a ciertas excepciones, la Ley RICA requiere el permiso de un juez para interceptar comunicaciones sobre la base de “motivos razonables para creer” que un delito grave ha sido, está siendo o probablemente vaya a cometerse. La Ley RICA establece las condiciones para conceder las directivas de interceptación.

Para garantizar la capacidad de los organismos estatales pertinentes para llevar a cabo las interceptaciones, esa ley necesita que los proveedores de servicios de telecomunicaciones ofrezcan servicios de telecomunicaciones que pueden ser interceptados. La Ley RICA también requiere que todos los sudafricanos registren sus tarjetas de módulo de identidad del abonado (SIM) con sus proveedores de telefonía móvil. Mientras que la constitucionalidad de la Ley RICA aún no se ha demostrado, los expertos han señalado que algunas de sus disposiciones no pasarían el examen en caso de denuncia.

Manifestantes gritan consignas durante una concentración para denunciar la Cumbre del G-20 de Seúl, Corea del Sur, el 10 de noviembre de 2010. Foto: Lee Jin-man/AP

Es notable que no exista ninguna disposición que exija que las personas sometidas a vigilancia sean notificadas de que sus comunicaciones han sido interceptadas, incluso después de la finalización de la investigación pertinente. Esto significa que a las autoridades se les da un poder que se oculta casi por completo de la vista del público. Por ejemplo, aunque la vigilancia de Kumi Naidoo había sido autorizada bajo la Ley RICA, Naidoo nunca se hubiera enterado de ella si no se filtraba la información. E incluso ahora que sabe acerca del posible espionaje, no existe ningún recurso automático bajo la Ley RICA para que se informe qué actividades de vigilancia se llevaron a cabo y por qué. Estas debilidades violan los principios "necesarios y proporcionados" por los que las personas deberían ser notificadas de las decisiones que autorizan la interceptación de sus comunicaciones, con tiempo e información suficientes para que puedan apelar la decisión, y deben tener acceso a los materiales presentados para apoyar la solicitud de autorización.[9]

Sin embargo, la vigilancia bajo la Ley RICA es solo una parte del panorama general de la vigilancia en Sudáfrica. Por ejemplo, el Centro Nacional de Comunicaciones (NCC), que alberga las capacidades de vigilancia masiva del Estado, opina que sus actividades no están reguladas por la Ley RICA. Si esto es así, significa que sus operaciones se llevan a cabo fuera de la ley. El NCC tiene el poder de reunir y analizar "señales extranjeras", lo que incluye las comunicaciones originadas fuera de las fronteras de Sudáfrica pero que pasan a través o terminan en Sudáfrica y los metadatos de comunicaciones, todo ello con poca o ninguna supervisión o restricción. Con respecto a los metadatos, se sabe poco acerca de cómo se los recolecta y almacena, o por qué es necesario almacenarlos durante un período de 3 a 5 años. Por otra parte, una orden para acceder a los metadatos almacenados no tiene por qué ser solicitada al juez que autoriza una vigilancia bajo la Ley RICA; en cambio, se la puede solicitar a cualquier juez en funciones o de la Corte Suprema, para lo cual no se provee ningún dato estadístico informado.

La promulgación de la Ley de Protección de Datos Personales de 2013 (POPI) contiene la promesa de ser una posible garantía del derecho a la privacidad. Sin embargo, a julio de 2016 la persona que debe oficiar como Regulador de la Información todavía no ha sido designada, y varias disposiciones claves de la POPI, incluyendo las condiciones para el tratamiento legal de la información personal, aún no están en funcionamiento.[10] Por otra parte, y también para julio de 2016, el cargo de Inspector General de Inteligencia –funcionario encargado, en virtud de la Constitución sudafricana, de la supervisión civil de los servicios de inteligencia– permanece vacante desde marzo de 2015. En términos generales, la población sudafricana carece de información significativa acerca del alcance de la vigilancia en su país. El Comité Permanente Conjunto sobre Inteligencia (JSCI) –la comisión parlamentaria encargada de supervisar el trabajo de los servicios de inteligencia en Sudáfrica– tiene la obligación de elaborar informes públicos sobre la aplicación de la Ley RICA. Sin embargo, la información suele escasear en detalles. El informe más reciente de la JSCI no brinda ninguna información sobre por qué se llevaron a cabo

Activistas de Right2Know protestan fuera del recinto en el que tienen lugar las audiencias del Ente Regulador Eléctrico Nacional de Sudáfrica en Midrand el 4 de febrero de 2016. Foto: Shayne Robinson

intercepciones RICA, o su resultado y su eficacia en la prevención o investigación de delitos. Entretanto, no parece haber ninguna supervisión centralizada u obligación de informar públicamente sobre las estadísticas de recolección y uso de metadatos, y a las empresas de telecomunicaciones se les prohíbe publicar información (incluyendo estadísticas agregadas) tanto sobre la interceptación de las comunicaciones como sobre los metadatos.[11] El JSCI también sigue funcionando como un comité cerrado, a pesar de las repetidas peticiones para abrirlo al público. El resultado es que los sudafricanos siguen en gran medida sin saber cómo funcionan ni cuáles son los objetivos de los servicios de inteligencia del país.

conclusión

Es claro que al menos algunas organizaciones e individuos están siendo monitoreados por las estructuras de seguridad del Estado en Sudáfrica; sin embargo, no está claro cómo se está haciendo, las razones de la vigilancia o el uso que se hace de la información recolectada. En algunos casos, hay serias preocupaciones de que las estructuras de seguridad puedan tener un celo excesivo y extralimitarse en sus funciones. Por otra parte, también hay serias preocupaciones de que el gobierno sudafricano comparta indiscriminadamente información con gobiernos extranjeros, sin las previsiones adecuadas para que los protagonistas de dicha información sean notificados y objeten dicha información o su intercambio.

Lo que sí sabemos es que los servicios de seguridad están buscando aumentar sus capacidades. El informe más reciente de la JSCI advirtió que los criminales están utilizando tecnologías de comunicación electrónica más sofisticadas, y que la agencia de seguridad necesita de manera urgente contar con tecnología moderna para interceptar esas comunicaciones electrónicas.[12] El informe también indica que, de 202 solicitudes de vigilancia presentadas por la policía, se concedieron las 202. En la filtración de información del año 2015 de Hacking Team, se reveló que el gobierno de Sudáfrica había expresado su interés por la compra de tecnología de vigilancia y hackeo.[13] Sin embargo, la cadena de comunicación termina abruptamente, por lo que no llega a saberse si el equipamiento fue finalmente adquirido. Poco se sabe acerca de la capacidad de vigilancia que el gobierno tiene y usa en la actualidad. Pero las filtraciones pusieron de manifiesto al menos cierto grado de voluntad política del gobierno sudafricano de equiparse con esa tecnología.

Si bien los servicios de seguridad tienen un papel importante que desempeñar en las circunstancias apropiadas, la historia de Sudáfrica ha demostrado de

> “Mientras que algunos han llamado a esta tendencia ‘el ascenso de los segurócratas’ por la forma en que el núcleo de seguridad sudafricano está siendo percibido como más reservado, expansivo e implicado en asuntos políticos, otros se preguntan si los servicios de inteligencia de Sudáfrica fueron de veras reformados en la era democrática.”

qué modo los poderes de vigilancia pueden fácilmente ser empleados para infringir los derechos básicos. A la historia reciente hay que sumar el hecho de que, con nuevas tecnologías, la gente podría no enterarse nunca de que ha sido vigilada. Para los sudafricanos, esta combinación de historia y tecnología aumenta el riesgo de intimidación y la posibilidad de que la vigilancia y la perspectiva de ser vigilados tengan un efecto negativo sobre el trabajo de activistas, medios y políticos y los disuadan de realizar el importante papel que desempeñan en una democracia abierta y responsable.

un giro internacional

En Sudáfrica, como en muchas democracias emergentes del mundo actual, las organizaciones por los derechos civiles y derechos humanos, como el LRC, están dedicando más tiempo a denunciar la expansión de los poderes de vigilancia y la protección de los derechos a la privacidad. Pero las revelaciones de Edward Snowden sobre la existencia de una vasta arquitectura de vigilancia digital internacional liderada por Estados Unidos y sus socios de los llamados Cinco Ojos trajeron consigo otra preocupación: la posibilidad de que las organizaciones no gubernamentales y por los derechos civiles de cualquier lugar del planeta estén siendo vigiladas no solo por sus propios gobiernos, sino por agencias de espionaje que operan a continentes de distancia. Y así, en julio de 2014, diez organizaciones de derechos humanos[14] (seis de las cuales son miembros de la INCLO) se unieron para intentar determinar si sus organizaciones habían sido vigiladas por el Cuartel General de Comunicaciones del Gobierno (GCHQ) del Reino Unido, a través de sus programas masivos de vigilancia.

Las organizaciones presentaron una denuncia ante el Tribunal de Poderes de Investigación (IPT) para impugnar la legalidad de los programas de vigilancia masiva del GCHQ. El IPT es un tribunal especial establecido para recibir demandas por vigilancia ilegal y para determinar si esos programas son contrarios a la protección de los derechos humanos contenidos en la Ley de derechos humanos del Reino Unido y la Convención Europea de Derechos Humanos (CEDH). Se trata del único tribunal en el Reino Unido que puede juzgar casos contra los servicios de seguridad.

El caso, que tenía el objetivo de descubrir la verdad sobre los programas transnacionales de vigilancia masiva y determinar si esos programas estaban capturando las comunicaciones de esas organizaciones y clientes, planteaba desafíos enormes y únicos –en particular porque, bajo la ley del Reino Unido, el Estado no está obligado a informarte si has sido sometido a espionaje, incluso si no has hecho nada para justificar las actividades de vigilancia y si la vigilancia revela que eres irreprochable. Si no hubiera sido por las filtraciones de Snowden, que mostraron que los gobiernos del Reino Unido y los Estados Unidos estaban llevando a cabo programas masivos de interceptación y compartiendo información entre sí y con otros socios internacionales, las organizaciones

> “Las revelaciones de Edward Snowden sobre la existencia de una vasta arquitectura de vigilancia digital internacional liderada por Estados Unidos y sus socios de los llamados Cinco Ojos trajeron consigo otra preocupación: la posibilidad de que las organizaciones no gubernamentales y de libertades civiles de cualquier lugar del planeta estén siendo vigiladas no solo por sus propios gobiernos, sino por agencias de espionaje que operan a continentes de distancia.”

no habrían conocido el alcance de la vigilancia y no podrían haber superado ese primer y a menudo fatal obstáculo para quienes buscan demandar los programas de vigilancia del Estado.

Sin embargo, ese no era el único obstáculo. A lo largo del litigio, el gobierno del Reino Unido mantuvo su política de “no confirmar ni negar”; no admitía la existencia de sus programas de vigilancia masiva, ni tampoco los negaba. Esto a pesar del hecho de que el gobierno de los Estados Unidos ya había reconocido que las revelaciones de Snowden sobre su programa paralelo PRISM y de recolección “upstream” eran ciertas. La respuesta del IPT a esto fue examinar la ley sobre la base de un compromiso: la audiencia procedería sobre una premisa fáctica hipotética: que la vigilancia masiva, según lo revelado por Snowden, ocurre.

Además, y quizás lo más difícil, fue que a las diez organizaciones solo se les permitió participar en algunas de las audiencias del IPT. El IPT mantuvo al menos una audiencia a puerta cerrada, a la que solo asistieron miembros del tribunal, el gobierno y sus representantes. Las organizaciones de derechos humanos no estaban representadas en esa audiencia, ni se les proporcionó un resumen del material presentado al IPT durante esa sesión (a pesar de las repetidas peticiones al IPT de que toda la información recibida en secreto fuese revelada, todas las cuales fueron rechazadas). Más allá de la obvia injusticia de excluir a una de las partes del proceso legal, este enfoque condujo a profundas dificultades prácticas y de confusión.

Por ejemplo, después de la audiencia a puerta cerrada el IPT le dijo al gobierno del Reino Unido que una parte del material que había presentado al tribunal en secreto debía ser revelado a las diez organizaciones. El gobierno elaboró entonces una nota que parecía establecer el modo en que el gobierno del Reino Unido maneja el material interceptado que recibe de gobiernos extranjeros. Pero el estatus de la nota no estaba claro: ¿era parte de un documento normativo? y, en caso afirmativo, ¿era toda la norma o un resumen de la misma? El IPT negó una solicitud para explicar qué era el documento y cómo lo había utilizado el gobierno en la audiencia a puerta cerrada. Tres versiones diferentes del documento fueron presentadas a las organizaciones en distintos momentos, cada una con una serie diferente de correcciones. Pero no hubo explicación alguna del significado de esa nota, ni del gobierno ni del IPT.

Incluso con tales obstáculos, por primera vez en sus 11 años de historia el IPT llegó a una conclusión contra el gobierno en la denuncia presentada por las diez organizaciones de derechos humanos. Sostuvo que el procedimiento que el gobierno del Reino Unido había utilizado para recibir información que el gobierno de Estados Unidos recogía a través de PRISM o de la recolección “upstream” había sido ilegal durante años; y era ilegal porque las garantías dentro del régimen de intercambio de inteligencia no eran lo suficientemente

Manifestantes usando máscaras con el rostro del ex contratista de la NSA Edward Snowden durante la audiencia testimonial de Glenn Greenwald ante un comité del Congreso brasileño sobre los programas de vigilancia de la NSA en Brasilia, 6 de agosto de 2013. Foto: Reuters/Latinstock

conocidas por la población. Pero el tribunal acompañó esa conclusión con otra, alegando que gracias a las revelaciones que habían tenido lugar durante el litigio, las garantías eran ya lo suficientemente públicas y el régimen era compatible con los derechos humanos. Según el tribunal, esas revelaciones históricas estaban en la nota misteriosa.

Lamentablemente, el IPT decidió que los programas de vigilancia masiva del gobierno del Reino Unido no constituían una violación de los derechos humanos. Más bien, señaló que la vigilancia masiva era en realidad una consecuencia "inevitable" de la tecnología moderna, y que los poderes otorgados por la Ley de Regulación de los Poderes de Investigación de 2000 le permitió al gobierno británico espiar a ciudadanos extranjeros sin una orden que identificara al objetivo de vigilancia.

Sin embargo, en junio de 2015, el IPT pronunció un fallo adicional en el que reveló que dos de las organizaciones demandantes habían sido vigiladas ilegalmente por el GCHQ. El LRC fue una de ellas.[17] En relación con el LRC, el IPT descubrió que "las comunicaciones de una dirección de correo electrónico asociada al [LRC] fueron interceptadas y seleccionadas para su examinación de conformidad con la s 8(4) de la Ley de Regulación de los Poderes de Investigación. El [IPT] considera que la interceptación fue legal y proporcionada y que la selección de comunicaciones para examinar fue proporcionada, pero que el procedimiento establecido por las políticas internas de GCHQ para seleccionar las comunicaciones para su exanimación fue por error no seguido en este caso".

El IPT llegó a la conclusión de que se trataba de una violación del artículo 8 del CEDH, pero quedó convencido de que "la agencia interceptora no hizo uso alguno del material interceptado, ni retuvo archivos". En consecuencia, dictaminó que el LRC no sufrió ningún daño material o perjuicio, y no hubo compensación.

Como lo resumió Janet Love, directora nacional del LRC, en el momento de la decisión:[17]

[En LRC] estamos profundamente preocupados tras enterarnos de que las comunicaciones de nuestra organización han sido objeto de interceptación ilegal por parte del GCHQ. Como un estudio de abogados de interés público, nuestras comunicaciones son obviamente confidenciales, y consideramos que se trata de una violación grave de los derechos de nuestra organización y de las personas afectadas.

Ya no podemos aceptar la conducta de los servicios de inteligencia que actúan bajo un secretismo tan pernicioso, y vamos a tomar medidas inmediatas para tratar de obtener más información. Instamos al gobierno sudafricano y británico a cooperar con nosotros en este sentido.

En Sudáfrica, tras la sentencia del IPT, el LRC presentó una solicitud de acceso a la información a la Agencia de Seguridad del Estado, en busca de la siguiente información:

—cualquier solicitud de información relativa al LRC o sus miembros recibida del gobierno del Reino Unido;
—cualquier respuesta proporcionada a dicha solicitud de información;
—cualquier acuerdo, memorando de entendimiento u otro documento que asegurara, facilitara, fomentara o contemplara el intercambio de inteligencia entre Sudáfrica y Reino Unido;
—cualquier solicitud de información con respecto al LRC o a sus miembros recibida desde cualquier otro país, y la respuesta dada por Sudáfrica; y
—cualquier solicitud de una orden de interceptación solicitada o concedida bajo la legislación sudafricana pertinente.

Hasta el día de hoy esta petición no ha sido respondida.

El fallo del IPT dejó más preguntas que respuestas para el LRC, así como para las otras organizaciones involucradas en la demanda. Como actualmente no existe un derecho de apelación contra las sentencias del IPT, y teniendo en cuenta la gravedad del daño de que esas prácticas de vigilancia se consideren legales, las diez organizaciones llevaron el asunto al Tribunal Europeo de Derechos Humanos (TEDH). En diciembre de 2015, el TEDH decidió aceptar el caso, considerándolo una "prioridad". El gobierno del Reino Unido respondió en abril de 2016 y los demandantes, el 26 de septiembre 2016.

La decisión del TEDH constituirá una de las primeras veces en que un tribunal regional de derechos humanos se pronunciará sobre la legalidad de los regímenes de vigilancia masiva en la era post-Snowden. Frente a la intransigencia del gobierno y sistemas jurídicos inmóviles, esta es una oportunidad clave para que el TEDH afirme y dé contenido al derecho a la privacidad y para insistir en la transparencia de los Estados.

notas

-

1. "Greenpeace head Kumi Naidoo saddened at spying revelations", *The Guardian* (26 de febrero, 2015). Disponible en: http://www.theguardian.com/world/2015/feb/26/greenpeace-head-kumi-naidoo-saddened-at-spying-revelations [28/10/2016]
2. *Ibíd.*
3. "South Africa scrambles to deal with fallout from leaked spy cables", *The Guardian* (24 de febrero, 2015). Disponible en: http://www.theguardian.com/world/2015/feb/24/south-africa-scrambles-to-deal-with-fallout-from-leaked-spy-cables [28/10/2016]
4. "Greenpeace head Kumi Naidoo saddened at spying revelations", *op. cit.*
5. Manual de activismo de Right2Know, "Big Brother Exposed", p. 2
6. Corruption Watch. "Spy Tapes Saga: The Latest", (22 de agosto de 2013). Disponible en: http://www.corruptionwatch.org.za/spy-tapes-saga-the-latest [28/10/2016]
7. "UPDATE: NPA files 'spy tapes" papers'", *eNews Channel Africa* (3 de julio, 2015). Disponible en: https://www.enca.com/south-africa/will-npa-file-spy-tapes-papers [28/10/2016]
8. "Hawks bugged reporter's phone", *Mail & Guardian* (2 de octubre, 2011). Disponible en: http://mg.co.za/article/2011-10-02-hawks-bugged-reporters-phone [28/10/2016]
9. "International Principles on the Application of Human Rights to Communications Surveillance" (Mayo 2014). Disponible en: http://en.necessaryandproportionate.org/text [28/10/2016]
10. Incluso una vez que la POPI esté plenamente vigente, todavía habrá un período de gracia de un año antes de que se exija su cumplimiento, período que el ministro responsable podría extender aún más.
11. Vodafone. "Law Enforcement Disclosure Report: Updated Legal Annexe February 2015". Disponible en: https://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf [28/10/2016]. Para una visión general de la estructura de los servicios de seguridad, ver: http://www.ssa.gov.za/AboutUs/LegislationOversight.aspx [28/10/2016]
12. "Moderne tegnologie fnuik glo SA se spioene", *Netwerk 24* (27 de enero, 2016). Disponible en: http://www.netwerk24.com/Nuus/Politiek/moderne-tegnologie-fnuik-glo-sa-se-spioene-20160127 [28/10/2016]
13. "Hacking Team failed to crack SA", *IT Web* (14 de julio, 2015). Disponible en: http://www.itweb.co.za/index.php?option=com_content&view=article&id=144683 [28/10/2016]
14. La American Civil Liberties Union, Amnistía Internacional, Bytes for All, la Canadian Civil Liberties Association, la Egyptian Initiative for Personal Rights, la Hungarian Civil Liberties Union, el Irish Council for Civil Liberties, el Legal Resources Centre y Privacy International.
15. Curiosamente, a la misma hora, en un caso diferente ante el mismo tribunal, el gobierno tuvo que publicar lo que parecía ser el documento normativo completo en el que se basaba la nota, pero aun así el IPT no lo solicitó para este caso.
16. [2015] UKIPTrib 13_77-H_2. El IPT indicó inicialmente que la *Egyptian Initiative for Personal Rights* era la otra organización que había sido vigilada ilegalmente. Sin embargo, pocos días después de emitir su sentencia, el IPT se retractó de su declaración inicial, e indicó que la organización afectada había sido Amnistía Internacional. No queda claro cómo se cometió tal error.
17. "GCHQ's surveillance of two human rights groups ruled illegal by tribunal", *The Guardian* (22 de junio, 2015). Disponible en: https://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal [28/10/2016]

Un vistazo a la vigilancia en Sudáfrica

¿Los ciudadanos saben más ahora que hace tres años acerca de las actividades de vigilancia del gobierno?
Sí. Aunque gran parte de las actividades de vigilancia del Estado todavía se llevan a cabo en secreto, se sabe más a través del periodismo de investigación y por filtraciones de información ocurridas en los últimos años.

¿Las revelaciones de Snowden condujeron a un debate público significativo en su país acerca de los límites adecuados de la vigilancia gubernamental?
Sí. Más organizaciones se han involucrado activamente en cuestiones relativas a la vigilancia, lo que a su vez ha impulsado el debate público y demandas de una mayor apertura y transparencia.

Después de las revelaciones de Snowden, ¿ha habido otros informantes que hayan decidido filtrar información al público acerca de la vigilancia gubernamental?
Sí. Ha habido filtraciones a los medios sobre actividades de vigilancia en curso.

En los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno se han reducido, han aumentado o ninguna de los dos opciones?
Sin respuesta. Aunque ha habido un importante reestructuración de los servicios de inteligencia, es difícil determinar si esto ha reducido o aumentado el personal de vigilancia.

En los últimos tres años, ¿se han impuesto nuevos controles estructurales sobre los servicios de inteligencia (por ejemplo, nuevos requisitos de transparencia)?
No en términos de legislación nacional.

Si el poder legislativo/Parlamento considerara una nueva legislación sobre vigilancia gubernamental, ¿dicha legislación restringiría o ampliaría su poder de vigilancia?
N/A.

Si el poder legislativo/Parlamento considerara una nueva legislación relativa a la vigilancia gubernamental, ¿dicha legislación impondría nuevos controles estructurales?
N/A.

Durante los últimos tres años, ¿las autoridades a cargo de la vigilancia de seguridad nacional del gobierno han sido objeto de litigio interno, incluso en los tribunales constitucionales?
No.

Durante los últimos tres años, ¿los tribunales han rechazado algún aspecto de la vigilancia gubernamental por ser incompatible con la Constitución y los derechos humanos?
No.

Durante los últimos tres años, ¿cree que la población ha llegado a confiar más, menos o no ha modificado su percepción sobre las agencias de inteligencia?
Menos. Esto es especulativo, pero en vista de la creciente conciencia acerca de la naturaleza y la escala de las actividades de vigilancia, y de una aparente preocupación pública en este sentido, parecería que la población es más cautelosa acerca de los servicios de inteligencia.

conclusión y recomendaciones

conclusión y recomendaciones

Argentina, Canadá, Hungría, India, Irlanda, Israel, Kenia, Rusia, Sudáfrica, Estados Unidos: todos estos países son democracias, algunas establecidas desde hace tiempo, algunas emergiendo de sistemas autoritarios y todavía luchando por lograr instituciones democráticas estables y consolidadas. Todas ellas, las democracias viejas y las nuevas, han experimentado una expansión dramática de los poderes y actividades de vigilancia en los últimos años.

Como este informe ilustra claramente, esta expansión ha ocasionado daños reales: daños a las personas y a sus derechos civiles y humanos; daños a la confianza de la población y al clima necesario para ejercer el activismo político y la disidencia; y daños al estado de derecho y al propio tejido y estructuras de los estados democráticos.

Los casos de Ibraheim "Abe" Mashal de Estados Unidos, un veterano al que le fue prohibido viajar en avión en base a inocuos correos electrónicos, y de Rateb Abu-Krinat de Israel, un activista de los derechos de las minorías convocado a una reunión con agentes de seguridad del Estado que insinuaron que estaban monitoreando sus comunicaciones y actividades, parecen haber emergido desde detrás de la cortina de hierro, donde los ciudadanos se encontraron cara a cara con un estado de vigilancia vasto y subterráneo. El caso *Re (X)* –en el que dos ciudadanos canadienses cuyas identidades desconocemos probablemente nunca sepan que fueron monitoreados tanto por su gobierno como por sus socios extranjeros– sugiere de qué manera los poderes de vigilancia sin fronteras y sin rostro se comportan en la era digital. Y el caso sudafricano de Kumi Naidoo muestra cómo, en esta nueva era, tal cooperación transnacional puede convertir a un respetado activista en un objetivo de vigilancia de otro país.

Incluso en las democracias más arraigadas, las nuevas herramientas y poderosas tecnologías de vigilancia están abriendo y reabriendo resquicios en las comunicaciones e instituciones que dependen de la confidencialidad –como cuando se utilizan nuevas tecnologías para monitorear conversaciones de políticos de la oposición en la India, o cuando un defensor del pueblo facultado para supervisar

a la policía nacional de Irlanda llega a creer que su propio organismo de control es el que está siendo observado.

Entretanto, en países con democracias emergentes y el recuerdo fresco de regímenes autoritarios, los nuevos poderes de vigilancia pueden parecerse bastante a una extensión de los hábitos y estructuras represivas del pasado, en la forma de una nueva amenaza a la privacidad y a la seguridad personal. Un país como Argentina, que ha luchado para reconstruir un estado democrático después de los crímenes cometidos durante la dictadura, descubre que los poderes de vigilancia de los servicios de inteligencia continúan siendo herramientas políticas potentes y turbias. Los servicios de seguridad de Hungría, un país que solo hace poco se quitó de encima décadas de opresión política, están probando un sistema de vigilancia que todo lo ve, y que parece la encarnación moderna del estado de vigilancia de la era comunista. En una democracia emergente como Kenia, que lucha contra una grave amenaza terrorista, la inteligencia recolectada con nuevos poderes digitales no conduce a condenas ni a políticas más eficaces, sino al resurgimiento de escuadrones de la muerte y a ejecuciones extrajudiciales. Y en Rusia, el espionaje interno de activistas es un recuerdo vivo de que su transición hacia la democracia nunca fue completa.

Tanto a nivel internacional como en cada uno de esos países existen leyes que limitan los poderes de vigilancia. El derecho internacional –incluyendo, en particular, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP)– obliga a los Estados a garantizar que cualquier interferencia con el derecho a la privacidad obedezca a los principios fundamentales de la legalidad, proporcionalidad y necesidad. Y cada uno de los diez países de este informe cuenta con un cuerpo de leyes domésticas que está destinado a proteger la privacidad y mantener la vigilancia a raya. Pero al intentar asegurarse de que sus gobiernos cumplen con estos estándares cuando se embarcan en las operaciones de vigilancia descritas en este informe, los diez miembros de la INCLO y nuestros colegas en las comunidades de los derechos civiles y humanos se han encontrado con un conjunto común de desafíos. Hemos encontrado marcos legales pobremente definidos, cuya función debería ser regular la actividad de vigilancia y proteger los derechos individuales. Hemos luchado contra la falta de transparencia en relación con las leyes y prácticas que rigen la vigilancia tradicional y digital en nuestros países, y hemos lidiado con mecanismos débiles o insuficientes para la supervisión de las operaciones de espionaje. Y cuando se han violado derechos individuales, hemos tenido dificultades para encontrar las vías legales que conduzcan a una reparación y rendición de cuentas por parte del Estado.

En los casos en que las operaciones de vigilancia se han llevado a cabo extraterritorialmente, descubrimos discrepancias preocupantes en la forma en que los gobiernos protegen los derechos de privacidad de sus propios ciudadanos, pero no los de quienes viven más allá de sus fronteras. Descubrimos que el secretismo generalizado, la mediocre supervisión y la falta de transparencia plagan estos nuevos y expansivos poderes, y sin embargo, nos encontramos con que tenemos aún menos medidas para desafiar y frenar el espionaje transnacional e impedir el intercambio de inteligencia ilegal a través de las fronteras.

Para poner fin a estos abusos y evitarlos en el futuro, será necesaria la acción concertada tanto a nivel nacional como internacional. A nivel nacional, los Estados deben tomar medidas adicionales para proteger mejor el derecho a la privacidad y otros derechos humanos en sus prácticas de vigilancia; prohibir la vigilancia masiva; mejorar el control y la transparencia de los servicios de inteligencia y de los poderes de vigilancia; imponer limitaciones a la vigilancia extraterritorial y al intercambio de información; y mejorar la protección de quienes denuncian el accionar de las instituciones a cargo de la seguridad nacional. Al mismo tiempo, en un mundo en el que los poderes digitales de vigilancia suelen tener un alcance global, se debe hacer más para articular un marco sólido y transparente que proteja el derecho humano fundamental a la privacidad a nivel internacional. Con este fin, estamos instando a todos los Estados a apoyar aclaraciones adicionales y estándares internacionales para asegurar que los ciudadanos de todas las naciones disfruten de igual protección ante la vigilancia injustificada.

recomendaciones a los gobiernos de todo el mundo

Respetar y asegurar el derecho humano a la privacidad, tanto *offline* como *online*

Respetar y garantizar a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción y control el derecho a la privacidad –tanto en línea como fuera de línea– y asegurarse de que esté más plenamente articulado en las leyes nacionales e internacionales, incluido el artículo 17 del PIDCP, sin distinción alguna por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, nacimiento o cualquier otra condición.

Reconocer la obligación legal de respetar y garantizar el derecho a la privacidad y otros derechos humanos de las personas fuera de su territorio cuando se adquieren, procesan, utilizan, almacenan o comparten sus datos personales.

Respetar y asegurar el derecho a la privacidad en el intercambio de información entre gobiernos

Divulgar la información necesaria para evaluar la compatibilidad de los acuerdos y prácticas de intercambio de inteligencia con las obligaciones para con los derechos humanos, incluido el derecho a la privacidad de las personas afectadas, y prohibir todos los acuerdos o prácticas que violen estas normas.

Asegurar que la privacidad y otros principios de los derechos humanos sean la base de los acuerdos y prácticas de intercambio de información, incluyendo limitaciones en el uso, retención, difusión, acceso y destrucción de la información. El intercambio de información debe estar sujeto a advertencias escritas para garantizar el cumplimiento de estas garantías.

Reducir el alcance de los poderes de vigilancia

Revisar todas las leyes, políticas y prácticas para asegurar que todas las actividades de inteligencia, incluidas las operaciones de vigilancia, sean compatibles con las obligaciones internacionales de derechos humanos, en particular los derechos a la privacidad y la libertad de expresión.

Asegurar que la vigilancia y otras actividades de inteligencia se llevan a cabo sobre la base de un marco legal públicamente accesible, preciso y completo, no discriminatorio y claramente definido.

Asegurar que todas las operaciones de vigilancia se lleven a cabo de conformidad con leyes, políticas y prácticas públicamente accesibles y de conformidad con la autorización judicial y que, como mínimo, sean un medio necesario y proporcionado para la búsqueda de un objetivo gubernamental legítimo y sean mínimamente invasivas del derecho a la privacidad –incluso en relación con la vigilancia orientada a proteger la seguridad nacional.

Prohibir y terminar con la vigilancia masiva

Reconocer que la vigilancia masiva o indiscriminada es una interferencia ilegal y prácticamente siempre desproporcionada del derecho a la privacidad. Adoptar medidas para poner fin a tales prácticas y prohibirlas.

Mejorar el control de las agencias de inteligencia y de las operaciones de vigilancia

Asegurar el establecimiento de organismos de control y revisión eficientes, independientes, responsables y transparentes de las actividades de inteligencia, los organismos de inteligencia y otros organismos gubernamentales que participen en las operaciones de vigilancia, y asegurar que estén adecuadamente financiados.

Publicar y divulgar todas las leyes, políticas y prácticas de vigilancia y las interpretaciones legales pertinentes de dichas normativas a los órganos de control y revisión, y tomar todas las medidas necesarias para garantizar un control adecuado y eficaz de los servicios de inteligencia y de otros organismos gubernamentales que participen en las operaciones de vigilancia.

Proveer reparaciones a las violaciones del derecho a la privacidad

Proporcionar garantías legales y procesales eficaces contra la recolección y uso excesivo, inadecuado o no autorizado de información personal por parte de las agencias de inteligencia.

Proporcionar acceso a recursos judiciales eficaces y de otra índole para quienes –independientemente de su origen nacional o país de residencia– tengan un fundamento razonable para creer que han sido sometidos a actividades de vigilancia en violación de sus derechos.

recomendaciones para naciones unidas

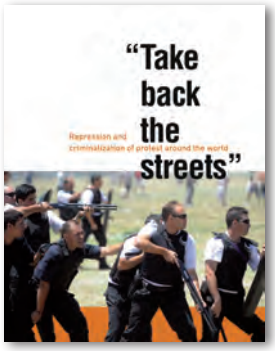
Mejorar la protección de quienes denuncien prácticas en relación a la seguridad nacional

Reforzar la protección legal para quienes denuncien prácticas en relación a la seguridad nacional y prohibir el procesamiento de quienes no sean empleados del gobierno o contratistas por revelar información que exponga irregularidades oficiales o sea de gran interés para los medios de comunicación, en los casos en que el interés público por esa información es mayor que cualquier daño específico a la seguridad nacional o a un interés estatal comparable.

El Comité de Derechos Humanos de la ONU debe revisar y actualizar la Observación General Nº 16 al artículo 17 (derecho a la privacidad) del PIDCP para brindar orientación a los Estados sobre sus obligaciones de respetar y garantizar el derecho a la privacidad informativa en virtud del PIDCP.

Apoyar al Relator Especial de Naciones Unidas sobre el derecho a la privacidad para aportar claridad sobre las normas pertinentes y el cumplimiento de dichas normas a nivel mundial, incluyendo, en particular, las normas aplicables a la vigilancia digital masiva.

OTROS INFORMES DE LA INCLO



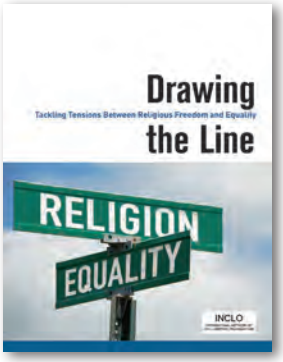
"Recuperen las calles: Represión y criminalización de la protesta en el mundo" incluye casos con ejemplos actuales de distintas reacciones estatales al activismo y la protesta en contextos nacionales únicos. Los casos muestran ejemplos de uso excesivo de la fuerza que resultaron en lesiones y muerte, y de trato discriminatorio y criminalización de líderes sociales. Todos los casos resaltan el papel integral que desempeñan las organizaciones de la sociedad civil en la protección de estos derechos democráticos fundamentales.

El informe online se encuentra disponible en español en: http://inclo.net/pdf/take-back-the-streets-sp.pdf http://www.inclo.net/pdf/take-back-the-streets.pdf

---

"Letalidad encubierta: efectos en la salud del uso de las armas 'menos letales' en las protestas" se trata de un informe conjunto entre la INCLO y Physicians for Human Rights, que documenta las consecuencias para la salud de las armas menos letales, examina su papel y sus limitaciones en contextos de protesta social y hace recomendaciones para su uso seguro. El objetivo de la publicación es concientizar sobre el uso indebido y abuso de este tipo de armas, sus efectos perjudiciales sobre la salud y el impacto de su utilización sobre el pleno disfrute de los derechos a la libertad de reunión y expresión.

El informe online en inglés se encuentra en: http://www.inclo.net/pdf/lethal-in-disguise.pdf (proximamente disponible en español)



"Libertad de culto e igualdad: Aportes para delimitar sus tensiones" se basa en la experiencia de los miembros de la INCLO en cinco continentes, en el análisis de casos en que la religión y las reivindicaciones de igualdad han competido en los tribunales. El informe propone resoluciones a las tensiones en tres áreas: derechos LGBT, derechos reproductivos y vestimenta religiosa. El informe articula un principio fundamental para resolver las tensiones entre religión e igualdad: la libertad religiosa supone el derecho a nuestras creencias, un derecho que es fundamental y debe ser defendido vigorosamente. Sin embargo, la libertad religiosa no nos da el derecho de imponer nuestros puntos de vista sobre los demás, sea discriminándolos o perjudicándolos.

El informe online se encuentra disponible en español en: http://inclo.net/pdf/drawing-the-line-sp.pdf


CELS
CENTRO DE ESTUDIOS
LEGALES Y SOCIALES


LRC
Legal Resources Centre


ACLU
AMERICAN CIVIL LIBERTIES UNION


Irish Council for
Civil Liberties


Egyptian Initiative
for Personal Rights


HRLN
Human Rights Law Network


ASZ
HCLU HUNGARIAN
CIVIL LIBERTIES UNION


AGORA


CANADIAN
CIVIL LIBERTIES
ASSOCIATION
ASSOCIATION
CANADIENNE DES
LIBERTES CIVILES


Pamoja Tuteteе Haki
KENYA HUMAN RIGHTS
COMMISSION