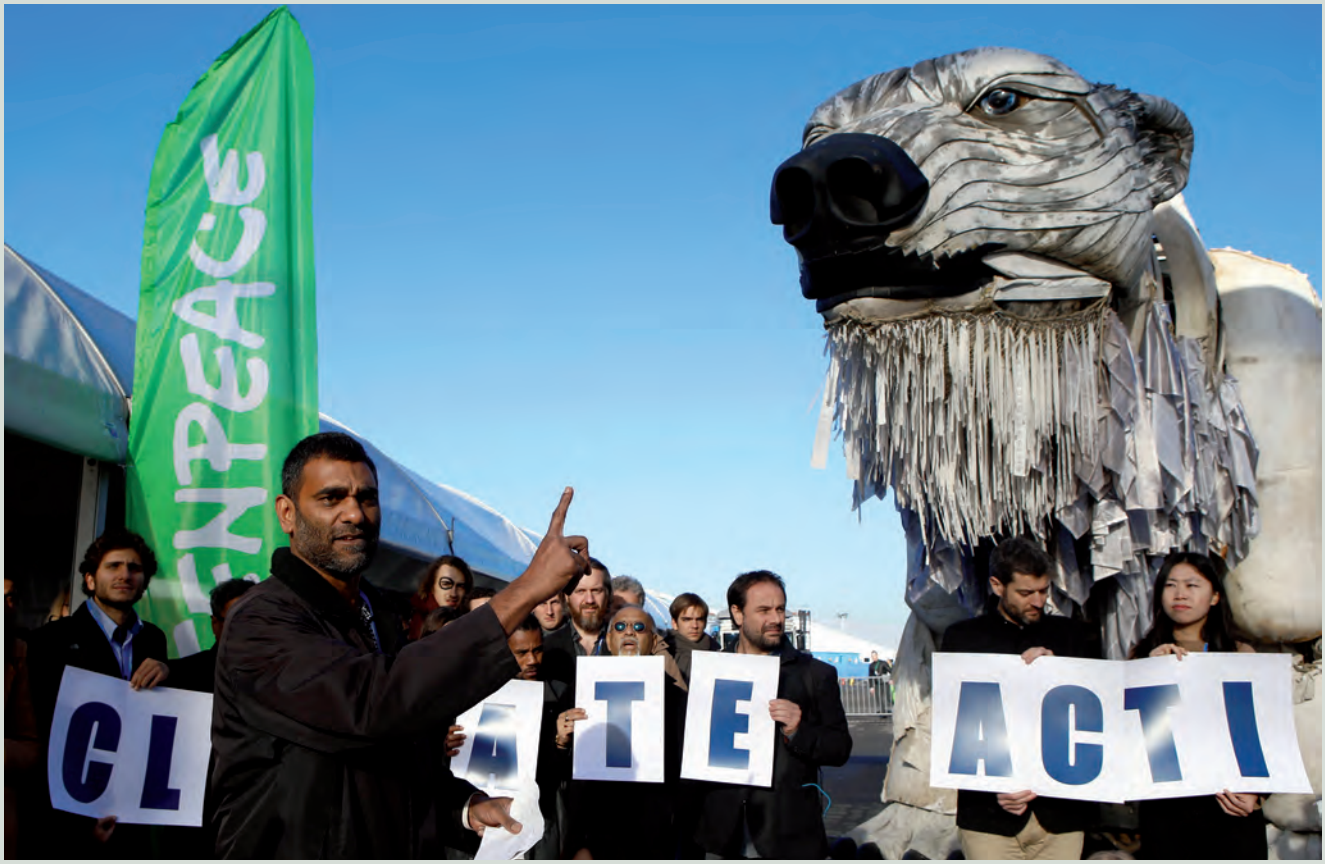
Espiar para otros: casos problemáticos de vigilancia transnacional

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.

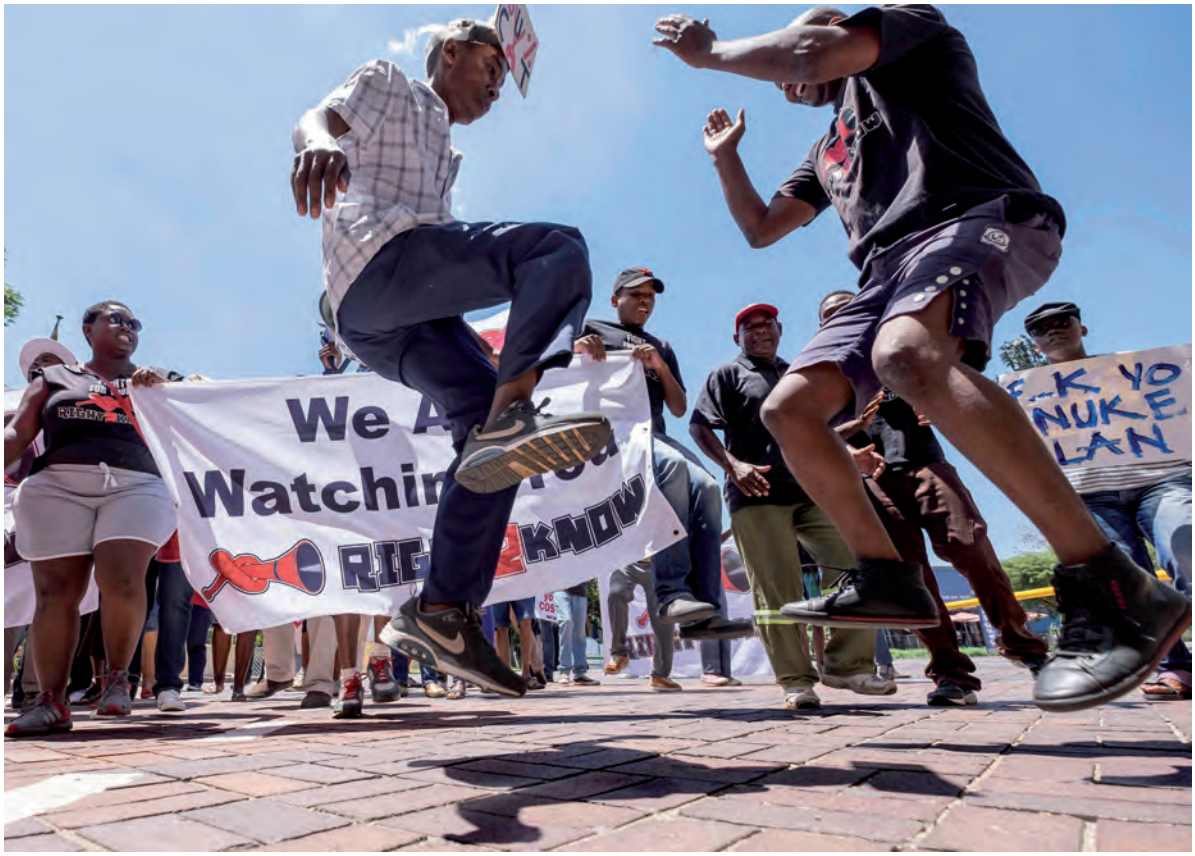
Para garantizar la capacidad de los organismos estatales pertinentes para llevar a cabo las interceptaciones, esa ley necesita que los proveedores de servicios de telecomunicaciones ofrezcan servicios de telecomunicaciones que pueden ser interceptados. La Ley RICA también requiere que todos los sudafricanos 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.”

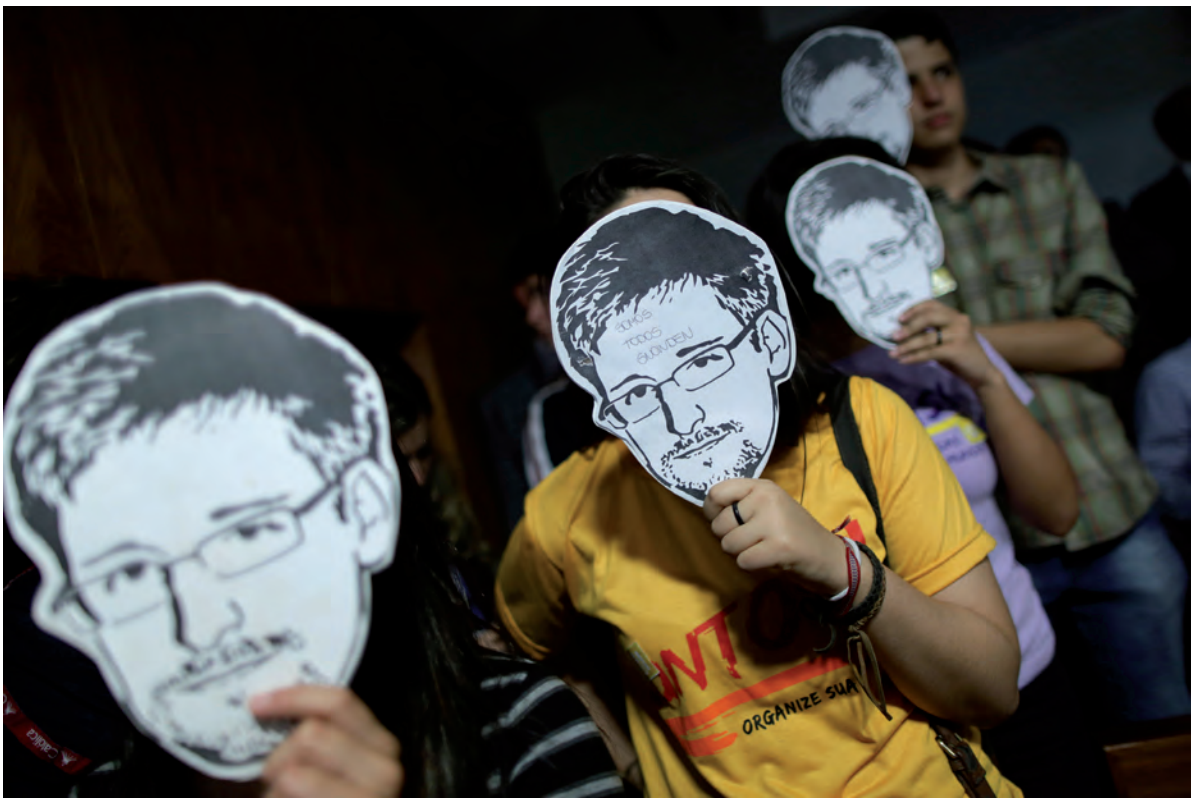
no habrían conocido el alcance de la vigilancia y no podrían haber superado ese primer y a menudo fatal obstáculo para quienes buscan demandar los programas de vigilancia del Estado.

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.