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]