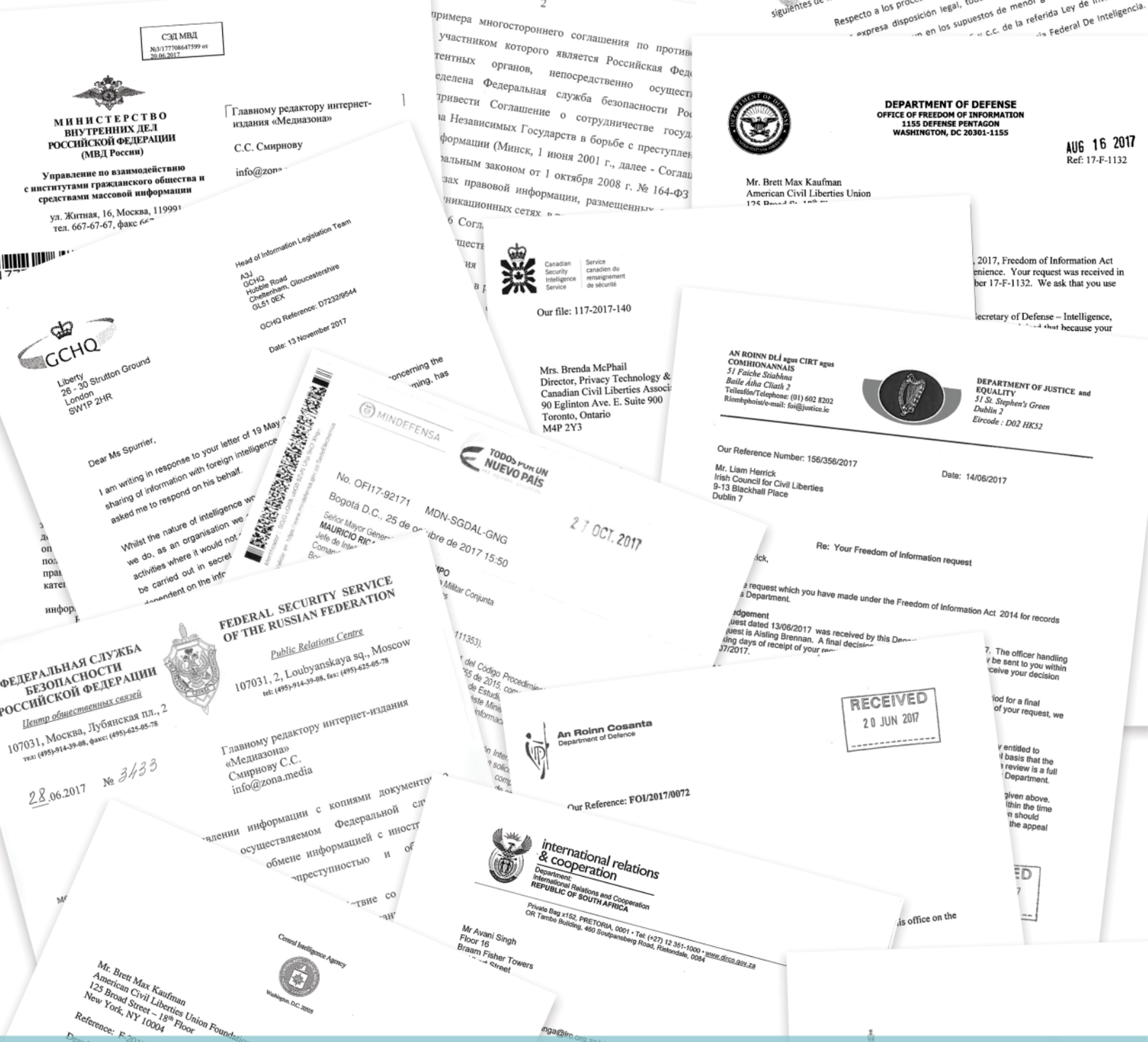

PREGUNTAS SIN RESPUESTA

INTERCAMBIO INTERNACIONAL DE INTELIGENCIA

JUNIO 2018

INCLO

INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

Sobre INCLO

Junio de 2018

Este informe fue producido por la Red Internacional de Organizaciones por los Derechos Civiles (INCLO), un grupo de 13 organizaciones nacionales e independientes de derechos humanos abocadas a promover los derechos y las libertades fundamentales mediante el apoyo y fortalecimiento mutuo 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.

Las organizaciones que componen INCLO son: Agora International Human Rights Group (Agora) de Rusia; American Civil Liberties Union (ACLU); Association for Civil Rights (ACRI) de Israel; Canadian Civil Liberties Association (CCLA); Centro de Estudios Legales y Sociales (CELS) de Argentina; Dejusticia de Colombia; Egyptian Initiative for Personal Rights (EIPR); Human Rights Law Network (HRLN) de la India; Hungarian Civil Liberties Union (HCLU); Irish Council for Civil Liberties (ICCL); Kenya Human Rights Commission (KHRC), Legal Resources Centre (LRC) de Sudáfrica y Liberty del Reino Unido.

Índice

Agradecimientos

El informe fue escrito por Elizabeth Farries y Eric King.

INCLO también agradece a Lucila Santos (INCLO), Brett Max Kaufman y Asma Peracha (ACLU), Avner Pinchuk (ACRI), Damir Gainutdinov (Agora), Brenda McPhail (CCLA), Margarita Trovato y Paula Litvachky (CELS), Vivian Newman (Dejusticia), Amr Gharbeia (EIPR), Kranti Chinappa y Devika Nair (HRLN), Márton Asbóth (HCLU), Aoife Masterson (ICCL), Andrew Songa (KHRC), Tsanga Mukumba (LRC) y Hannah Couchman (Liberty) por sus contribuciones a este informe.

Introducción

Este informe se basa en un proyecto de acceso a la información pública de INCLO. Diez miembros de INCLO presentaron solicitudes de acceso a la información pública[1] a sus gobiernos nacionales para dar luz sobre cómo funcionan las prácticas de intercambio de inteligencia tras las revelaciones de 2013 de Edward Snowden. Se trata de la primera coalición multinacional de organizaciones de derechos humanos que exige a los gobiernos divulgar información sobre acuerdos entre agencias de inteligencia y brindar respuestas sobre una práctica de la que no suelen rendir cuentas[2].

Las fuentes de este informe son nuestras solicitudes de acceso a la información pública, análisis documentales, entrevistas confidenciales con funcionarios de inteligencia y supervisión retirados o en funciones, y experiencias en trece países de INCLO. Las solicitudes se encuentran en curso, pero las tendencias emergentes incluyen exenciones legales, demoras o falta de respuestas. También hay:

- **Normas insuficientes** que rijan cómo se forman u operan las alianzas de intercambio de inteligencia;
- **insuficiente control y revisión gubernamental** de los acuerdos de intercambio de inteligencia; e
- **insuficiente transparencia** y acceso a información relacionada con dichos acuerdos.

La democracia necesita que los acuerdos internacionales de intercambio de inteligencia sean transparentes y estén guiados por leyes y controles adecuados. Se trata de una protección necesaria a nuestros derechos humanos consagrados, incluida la privacidad, la libertad de expresión, la libertad de asociación y el acceso a la información[3]. Al mantener estos acuerdos en secreto, los gobiernos han eliminado la capacidad de la sociedad para cuestionar su accionar.

La **Sección I** de este informe describe la cooperación internacional en materia de inteligencia y comparte las inquietudes de INCLO con respecto a estas prácticas. La **Sección II** detalla la legislación nacional vigente en los países miembros de INCLO, identifica los déficits de esas leyes y recomienda reglas y procedimientos claros. La **Sección III** describe prácticas de control y recomienda protocolos de supervisión más estrictos. La **Sección IV** comparte los resultados de nuestras solicitudes de acceso a la información pública y recomienda una mayor transparencia pública para garantizar el derecho de acceso a la información.

---

[1] Véase en el Apéndice de las solicitudes de acceso a la información de INCLO y sus respuestas.

[2] En 2017, Privacy International (PI) se asoció con organizaciones de la sociedad civil incluyendo miembros de INCLO y escribió a órganos de supervisión de 42 países como parte de un proyecto para aumentar la transparencia en el intercambio de inteligencia y alentar a los órganos de supervisión a analizar la ley y esta práctica en sus respectivos países. INCLO comparte la preocupación de PI de que el intercambio de inteligencia no transparente, irrestricto y sin rendición de cuentas representa riesgos sustanciales para los derechos humanos y el Estado de derecho democrático. Ver Privacy International “Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards” (abril de 2018). Disponible en: https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29.pdf

[3] Véanse los artículos 17, 19 y 22 de la Asamblea General de la ONU, "Pacto Internacional de Derechos Civiles y Políticos" (16 de diciembre de 1966); Artículos 12, 19 y 20 de la Asamblea General de la ONU, 'Declaración Universal de los Derechos Humanos' (10 de diciembre de 1948); Artículos 9, 10 y 11 del Consejo de Europa, 'Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, modificado por los Protocolos nos. 11 y 14' (1 de junio de 2010); Artículo 9 de la Carta Africana de Derechos Humanos y de los Pueblos.

I. Preocupaciones sobre el intercambio de inteligencia

En la India, la opacidad es la norma en lo que respecta a las acciones de vigilancia y al intercambio de inteligencia. Esta situación se ve reflejada en nuestros estatutos, como la Ley de Derecho a la Información de 2005 y la Ley de Tecnología de la Información de 2008. El control es mínimo y preocupante. Aadhaar, el proyecto masivo de metadatos biométricos de la India se encuentra actualmente bajo revisión judicial en nuestra Corte Suprema. Se trata del mismo tribunal constitucional que sostuvo que la privacidad es un derecho fundamental consagrado en nuestra Constitución. Lo que se decida en este caso marcará el rumbo que tomarán en la India las acciones de vigilancia ciudadana y el intercambio de inteligencia entre países.

- Kranti L Chinnapa, Director ejecutivo, Human Rights Law Network

A. Cooperación internacional de inteligencia en la práctica

Si bien sigue habiendo una alarmante falta de información acerca del intercambio de información de inteligencia entre diferentes países, esta sección detalla de qué manera el intercambio de inteligencia es una parte integral del trabajo de los servicios de inteligencia, los tipos de intercambio involucrados y de qué manera los acuerdos pueden ser construidos en torno al intercambio de recursos desiguales.

El intercambio es parte integral del trabajo de los servicios de inteligencia

Incluso antes de la llegada de Internet y de las tecnologías digitales de comunicación, las agencias de inteligencia compartían un gran volumen de sus análisis de inteligencia. Con el paso del tiempo, la cooperación internacional se ha convertido en una parte aun más integral del trabajo de los servicios de inteligencia. La mayoría –si no todas– las funciones de los servicios de inteligencia ahora incluyen una dimensión internacional. Algunas agencias tienen cientos de relaciones con contrapartes extranjeras[4]. De hecho, las necesidades específicas de un sistema nacional de inteligencia pueden resultar en que países que son potenciales adversarios firmen un acuerdo de cooperación sobre un asunto particular de interés compartido[5].

El nivel de información que estos acuerdos pueden suministrar es significativo. Ex funcionarios británicos de inteligencia han sugerido que la mayor parte de la producción occidental de

[4] Por ejemplo, el Director General de la Dirección General de Seguridad Exterior (DGSE) de Francia declaró que su servicio trabaja con más de 200 socios extranjeros. Testimonio del Director General de la DGSE Érard Corbinde Mangoux ante el Comité de Defensa de la Asamblea Nacional (20 de febrero de 2013).

[5] Véase, por ejemplo, la bien documentada cooperación de información e inteligencia entre el Reino Unido y la Libia de Gaddafi sobre el tema específico de la lucha contra el terrorismo. Véase también el llamado escándalo Irán-Contra (si bien no está relacionado con un intercambio de información, demuestra cómo la cooperación de inteligencia puede ocurrir incluso entre adversarios).

inteligencia se intercambia con al menos un socio extranjero[6]. Declaraciones de testigos proporcionadas por funcionarios de inteligencia del Reino Unido en respuesta a un litigio también han revelado que la inteligencia compartida por gobiernos extranjeros con los servicios de inteligencia del Reino Unido representa una proporción significativa de la información de inteligencia en poder de los servicios de inteligencia[7].

Intercambio depurado e intercambio en bloque

El intercambio internacional de inteligencia ha incluido tradicionalmente productos y evaluaciones de inteligencia depurados, que suelen entregarse en respuesta a la solicitud específica de un socio extranjero. El Estado puede brindar información que ya está en posesión de su agencia de inteligencia, o solicitarle a un socio que recopile la información deseada a través de sus propios sistemas de vigilancia. La inteligencia reunida podría incluir:

- **Información estratégica** como la evaluación de una situación en un país determinado o amenazas a la seguridad en sentido amplio;
- **información operativa**, como las capacidades de un actor armado no estatal; e
- **información táctica** relevante para una investigación de inteligencia en curso.

Además de la recolección de inteligencia con previa solicitud, una forma de cooperación cada vez más común es el intercambio de inteligencia de señales sin procesar, es decir, inteligencia derivada de señales electrónicas y sistemas utilizados por objetivos extranjeros ("SIGINT"). Los países entran en acuerdos de intercambio que permiten a cada socio tener acceso directo a las redes electrónicas en bloque de la otra parte[8]. Muchos servicios de inteligencia pueden tener acceso directo a bases de datos conjuntas.

No todos los intercambios son iguales

Documentos filtrados[9] nos muestran que una serie de acuerdos internacionales de cooperación de inteligencia también cubren diferentes tipos de intercambio además de productos de inteligencia depurados o en bloque. Los acuerdos de intercambio permiten el acceso a diferentes recursos tecnológicos y analíticos, a la vez que brindan soporte técnico, capacitación y recursos financieros. Cooperar con socios extranjeros permite a los gobiernos compartir las cargas de recursos y evitar la duplicación de esfuerzos al dividir el trabajo en torno a prioridades compartidas.

---

[6] Michael Herman, *Intelligence Power in Peace and War* (University of Cambridge Press 1996).

[7] Declaración testimonial de Charles Farr en Privacy International, Liberty y otros vs. Secretario del Estado para Asuntos Exteriores y de la Commonwealth y otros ante el Tribunal de Poderes de Investigación, IPT/13/92/CH, 16 de mayo de 2014. Liberty, miembro de INCLO, ha emprendido este litigio en representación de CCLA, EIPR, HCLU, ICCL y LRC cuestionando el uso que el Cuartel General de Comunicaciones del Gobierno (GCHQ), uno de los servicios de inteligencia de Reino Unido, hace del intercambio de inteligencia.

[8] La alianza de los Cinco Ojos es el ejemplo más conocido de esta práctica, pero su modelo se aplica en otras jurisdicciones. Véase, por ejemplo, una base de datos de la Agencia de Seguridad Nacional (NSA) titulada ICREACH. Se trata de un motor de búsqueda similar a Google e incluye el intercambio en bloque de SIGINT sin procesar de terceros. Véase Ryan Gallagher, "The Surveillance Engine" (*The Intercept*, 25 de agosto de 2014) disponible en: https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

[9] RAMPART-A es un programa de la NSA en el que 13 socios extranjeros "brindan acceso a cables y alojan equipos estadounidenses". El SIGINT sin procesar generado es de acceso directo para cada parte.

El intercambio, por lo tanto, no siempre es igual entre los socios y puede tener distintos valores. Estos acuerdos en particular otorgan a las agencias con mejores recursos acceso a redes y conocimiento "local" que incluso los servicios de inteligencia más grandes no podrían adquirir sin asociarse, a la vez que las agencias de inteligencia más grandes a menudo ofrecen equipamiento y entrenamiento a cambio de acceso a determinadas estaciones de aterrizaje de cables submarinos en otro país[10].

B. Problemas con estas prácticas

INCLO reconoce que los acuerdos internacionales de cooperación de inteligencia pueden significar beneficios para cada Estado y que no hay nada "incorrecto" en ellos *per se*. Sin embargo, nos preocupa el hecho de que las agencias tengan un historial de evasión de los marcos normativos existentes, para lo cual se valen de una larga lista de lagunas jurídicas y técnicas que describiremos a continuación.

Marcos normativos ausentes o ineficaces

En algunos países, los acuerdos internacionales en materia de inteligencia no están guiados o limitados por estatuto alguno. Incluso los países que cuentan con leyes que regulan el intercambio de inteligencia con gobiernos extranjeros, a menudo carecen de:

- Políticas, regulaciones o procedimientos vinculantes que las rijan o implementen;
- control y revisión legislativa independiente; e
- información clara, accesible y de carácter público.[11]

Estas omisiones dejan un espacio significativo para que las agencias de inteligencia que busquen traspasar los límites de la ley interpreten cuestiones técnicas y jurisdiccionales poco definidas de modos que afectan a los derechos humanos. Más aún, la población tiene poca o nula capacidad para cuestionar esas interpretaciones secretas.

Dada la falta de normas rigurosas, control y revisión, los acuerdos de cooperación de inteligencia suelen tomar la forma de Memorandos de Entendimiento secretos, establecidos directamente entre las agencias de inteligencia pertinentes[12]. De esta manera las relaciones de inteligencia quedan blindadas tanto frente a la sociedad civil como frente a los propios gobiernos a los que esas agencias pertenecen[13]. De hecho, los acuerdos de cooperación internacional que se han filtrado declaran

[10] Véase a Ryan Gallagher, "How Secret Partners Expand NSA's Surveillance Dragnet" (*The Intercept*, 18 de junio de 2014), disponible en: https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

[11] Panel de juristas eminentes de la Comisión Internacional de Juristas, "Evaluando el daño, instando a la acción" ("Assessing Damage, Urging Action"), 2009, p. 90.

[12] Los acuerdos de intercambio de inteligencia filtrados también sugieren que es común que el acuerdo obligue a mantener el secreto, y el texto estipula que "será contrario a este acuerdo revelar su existencia a un tercero a menos que se acuerde lo contrario". Véase el Acuerdo de UKUSA 1940-1956, disponible en el sitio web de la NSA en: https://www.nsa.gov/news-features/declassified-documents/ukusa/

[13] Los documentos filtrados explican la posición de la NSA de que "por diversas razones, nuestras relaciones de inteligencia rara vez se ven afectadas por perturbaciones políticas extranjeras, internacionales o nacionales... En muchas capitales de nuestros socios extranjeros, pocos altos funcionarios fuera del aparato de inteligencia-

expresamente que no están "destinados a crear ningún derecho exigible por ley y no deben interpretarse como un acuerdo internacional o un instrumento jurídicamente vinculante según el derecho internacional"[14]. Dichas restricciones crean un conjunto de obligaciones entrelazadas que limitan la capacidad del gobierno para intervenir y de la población para asegurar la divulgación de la información.

Legal en un país pero no en otro

Las agencias de inteligencia también pueden sacar provecho de sus alianzas internacionales de inteligencia para cosechar los beneficios de las capacidades de recolección de información por parte de otras jurisdicciones, incluso cuando se encuentran prohibidas por ley en su propio país. Para que un país emprenda una acción de vigilancia y recopile información sobre un objetivo a petición de un socio extranjero, es razonable que se apliquen los marcos y restricciones legales de ambos países. Sin embargo, de acuerdo con la información obtenida en nuestras entrevistas con personal de inteligencia retirado y en funciones[15], sospechamos que tales prácticas son inusuales. Por lo tanto, una agencia que tiene vedada por ley la recolección de determinada información, puede recibirla por parte de otra agencia en cuyo país si esté habilitado el procedimiento.

Esta cuestión ha surgido en los Países Bajos[16], donde las agencias de inteligencia tienen prohibido interceptar comunicaciones de cables submarinos de fibra óptica, pero no así recibir información de otras agencias de inteligencia extranjeras que sí lo hayan hecho. El Comité Holandés de Revisión de Inteligencia y Seguridad (CTIVD) revisó esta acción potencialmente lesiva del derecho a la privacidad y se sintió obligado a permitir que la práctica continuara[17]. El CTIVD consideró que a) en muchos casos es imposible saber cómo los socios extranjeros adquirieron el material; b) no resulta razonable que los holandeses insistan en que todo el intercambio de material esté acompañado por explicaciones que describan la técnica utilizada y las autoridades legales que permitieron la recolección; c) no hay una norma internacional consensuada que condene la interceptación de cables de fibra óptica, y d) la legislación holandesa no dice nada sobre la permisibilidad de esta práctica de intercambio internacional.

---

defensa están atentos a cualquier conexión SIGINT con los EE.UU". Véase "What Are We After With Our Third Party Relationships?" (2009), disponible en: https://edwardsnowden.com/wp-content/uploads/2014/03/third-party-relationships.pdf

[14] Memorando de entendimiento entre la Agencia de Seguridad Nacional/Servicio Central de Seguridad (NSA/CSS) y la Unidad Nacional SIGINT de Israel (ISNU), disponible en: www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf

[15] Las entrevistas de Eric King con personal de inteligencia retirado y en funciones se concedieron bajo la condición de anonimato.

[16] Comité de Revisión de los Servicios de Inteligencia y Seguridad de los Países Bajos (CTIVD), "Review Report on the processing of telecommunications data by GISS and DISS" (5 de febrero de 2014), disponible en: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss/report-38-processing-telecommunications-data.pdf

[17] Ibíd.

Sorteando órdenes judiciales

También hemos visto la burla de las órdenes judiciales en los países miembros de INCLO[18]. Los países pueden omitir información al momento de solicitar una orden o esquivar los requerimientos que éstas contengan basándose en argumentos legales estrechos y defectuosos. En Canadá, cuando el Servicio de Inteligencia de Seguridad Canadiense (CSIS) y la Agencia de Seguridad en las Comunicaciones (CSE) quisieron monitorear a dos canadienses que viajaban al exterior, se les exigió que solicitaran una orden judicial. Al presentar la solicitud, deliberadamente omitieron información clave que hacía referencia a su intención de contar con la ayuda[19] de sus socios de los "Cinco Ojos" ("Five Eyes" en inglés)[20].

Del mismo modo, mientras que el Cuartel General de Comunicaciones del Gobierno del Reino Unido (GCHQ) necesita una orden judicial para recolectar datos SIGINT en bloque sin procesar, documentos secretos sugieren que el GCHQ en cambio no necesita una orden para recibir datos en bloque sin procesar de parte de la Agencia de Seguridad Nacional de los Estados Unidos (NSA)[21]. Para ello, se basaron en acuerdos secretos que alegan que si no era técnicamente factible que el GCHQ adquiriera el material por sí mismo, la recolección de parte de terceros no activaría el requerimiento de una orden judicial[22] ni tampoco sería ilegal. De forma similar, en Estados Unidos un alto funcionario de inteligencia de ese país afirmó que, aunque las autoridades de EE.UU. pueden verse impedidas por ley para obtener una orden para vigilar a ciudadanos estadounidenses que viven en el exterior o de solicitar dicha información a otros países, nada impide que las autoridades estadounidenses la *reciban*[23].

Infraestructura en países extranjeros

Las agencias también pueden evadir leyes nacionales al establecer instalaciones o infraestructura en otros países. Cuando una agencia de inteligencia que opera en un país extranjero recolecta SIGINT,

---

[18] Este incumplimiento por supuesto no se limita a los países miembros de INCLO. Un claro ejemplo proviene de Nueva Zelanda. Allí, el Buró de Seguridad de Comunicaciones del Gobierno (GCSB) no está autorizado a vigilar a los neozelandeses. Sin embargo, informes periodísticos revelan que el GCSB le pidió a la NSA de Estados Unidos que recopilara información e interceptara llamadas telefónicas de un periodista de Nueva Zelanda. El periodista informaba sobre el manejo de detenidos en Afganistán por parte del ejército neozelandés, y el GCSB le pidió a la NSA que descubriera las fuentes confidenciales del periodista. El Inspector General de Nueva Zelandia está actualmente investigando el asunto. Véase a Nicky Hager, "US spy agencies eavesdrop on Kiwi" (*Stuff*, 28 de julio de 2013), disponible en: http://www.stuff.co.nz/national/8972743/US-spy-agencies-eavesdrop-on-Kiwi

[19] Véase Re (X), 2013 FC 1275, Tribunal Federal de Canadá, 2013. Para leer más sobre el caso véase "Vigilancia y democracia. Historias en diez países", INCLO, pp. 44–51, disponible en: https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf

[20] Cinco Ojos es el nombre de una alianza de inteligencia que comprende a EE.UU., el Reino Unido, Australia, Canadá y Nueva Zelanda.

[21] Liberty, "Secret policy reveals GCHQ can get warrantless access to bulk NSA data" (29 de octubre de 2014) disponible en: https://www.libertyhumanrights.org.uk/news/press-releases/secret-policy-reveals-gchq-can-get-warrantless-access-bulk-nsa-data. Un litigio iniciado por Liberty, miembro de INCLO, ha cuestionado esta situación.

[22] Privacy International, "Snowden Vindicated: The Truth About Raw Intelligence Sharing" (29 de noviembre de 2014), disponible en: https://privacyinternational.org/feature/1675/snowden-vindicated-truth-about-raw-intelligence-sharing

[23] Human Rights Watch, "Joint letter to European Commission on EU-US Privacy Shield" (26 de julio de 2017), disponible en: https://www.hrw.org/news/2017/07/26/joint-letter-european-commission-eu-us-privacy-shield

surgen una serie de problemas jurisdiccionales y de responsabilidad legal. Estos acuerdos no son claros respecto de si deben satisfacerse los marcos legales de ambos países, o de uno solo, o de ninguno. El ejemplo extremo de tal preocupación sería un país que permitiera a una agencia de inteligencia extranjera coleccionar SIGINT desde una base en su territorio, recolectar información que al país sede no se le permitiría recolectar y, luego, obtener esa información mediante una cooperación de inteligencia[24].

Punto de transferencia o posesión

El punto de transferencia o posesión se ha convertido en un asunto polémico en torno al cual se habilita el intercambio de inteligencia. Las agencias de inteligencia pueden declarar que, técnicamente, no tienen posesión del material de inteligencia hasta que no *miran* la información. Históricamente, cuando la información se entregaba *físicamente* a una agencia de inteligencia extranjera en un sobre manila, quedaba claro en qué momento la nueva agencia tomaba posesión de dicha información. Sin embargo, ahora que los servicios de inteligencia tienen redes electrónicas seguras y plataformas compartidas con socios cercanos que permiten el intercambio inmediato de información estratégica y SIGINT en bloque sin procesar, el punto en el que una agencia toma posesión de la información puede ocultarse tras distinciones lingüísticas algo arbitrarias que pueden eludir los derechos a la privacidad[25]. Por ejemplo, según las disposiciones actuales de la CSE canadiense, "la información adquirida a través de medios automatizados y mantenida en un búfer de datos no se considera interceptada sino hasta que un analista la haya consultado mediante una herramienta de búsqueda"[26]. Véase también el Reino Unido, donde los funcionarios del GCHQ han declarado que recolectar comunicaciones de cables de fibra óptica no es en sí una invasión a la privacidad hasta que no se examine por medios no automatizados, es decir, por un ser humano[27].

Efectos monopólicos

En los acuerdos de cooperación de inteligencia existe también el riesgo de un efecto monopólico que pueda aumentar la capacidad de agencias específicas de eludir normativas nacionales. Debido a la naturaleza a menudo bilateral de los acuerdos, nos preocupa que las agencias de inteligencia más poderosas puedan contar con un gran número de socios y usar los accesos provistos para construir una gran red de puntos de recolección de inteligencia[28]. Por ejemplo, si una agencia busca acceso a

[24] La NSA es un ejemplo clásico de agencia de inteligencia que tiene bases de inteligencia en otros países. Menwith Hill de el Reino Unido es supuestamente una base operada por la NSA. Los gobiernos se niegan a responder preguntas sobre las prácticas que se desarrollan allí. Véase, por ejemplo, Ryan Gallagher, "UK Government pressured over secret base's role in Trump's drone strikes" (*The Intercept*, 30 de noviembre de 2017), disponible en: https://theintercept.com/2017/11/30/drone-strikes-gchq-trump-menwith-hill-uk/

[25] Testimonio del Director General de la DGSE, Érard Corbin De Mangoux, ante el Comité de Defensa de la Asamblea Nacional (20 de febrero de 2013).

[26] Para un resumen general sobre estas distinciones, véase la Biblioteca del Parlamento, "Legislative Summary of Bill C-59: An Act respecting national security measures" (pre-release) (Biblioteca del Parlamento, 2017) pp.14-15.

[27] Véase más en Biblioteca del Parlamento, "Legislative Summary of Bill C-59: An Act respecting national security measures" (pre-release) (Biblioteca del Parlamento, 2017) pp.14-15.

[28] Estas preocupaciones también fueron expresadas por Edward Snowden en su presentación ante el Parlamento Europeo. Disponible en:

un cable submarino en particular, podría establecer dos acuerdos de cooperación por separado con dos países diferentes, que tengan acceso al cable. Si bien ambos países pueden estipular que el acceso no se puede utilizar para conseguir comunicaciones de sus ciudadanos, la agencia de inteligencia extranjera podría usar el acceso del primer país para adquirir comunicaciones sobre los ciudadanos del segundo país, y viceversa, sin violar los términos de ninguno de los dos acuerdos[29].

Falta de autorregulación

Las reglas que regulan el proceder de los socios de recolección de inteligencia no suelen ser rigurosas. Entre socios muy cercanos, las disposiciones del acuerdo a veces permiten que el socio extranjero recolecte SIGINT solo si su uso se sujeta a las obligaciones legales de los países recolectores. Sin embargo, estas protecciones tienden a no ser estrictamente exigidas. Véanse por ejemplo los sistemas de control que monitorean el acceso a las bases de datos SIGINT de Nueva Zelanda por otros miembros de los Cinco Ojos[30]. Para obtener acceso, los analistas de los Cinco Ojos deben ingresar a un sistema llamado "iLearn" y completar una sesión informativa sobre la NZSID7 (Directiva de Inteligencia de Señales de Nueva Zelanda)[31]. Ésta parece consistir en un ejercicio de selección de casilla de verificación, a libro abierto, que un agente puede completar de manera remota desde su escritorio a través de un análisis de "selección múltiple a libro abierto". No hay revisiones externas, requisitos adicionales o imposiciones técnicas[32] que impidan a los analistas omitir por completo este paso[33].

Además, no existe evidencia de que las agencias tengan control sobre el uso de su inteligencia por parte de otros socios. Si bien pueden existir controles normativos en los acuerdos de cooperación, esos controles se pierden tan pronto como la inteligencia se transfiere al organismo extranjero. Ninguna agencia de inteligencia u organismo de control tiene jurisdicción para ingresar a otro territorio y examinar su uso posterior. Los organismos de control han advertido que los acuerdos de cooperación de inteligencia no toman adecuadamente en cuenta esta situación, y que las agencias

---

http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

[29] Ese escenario fue descrito por Edward Snowden en su presentación ante el Parlamento Europeo. Disponible en: http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

[30] Los analistas pueden acceder tanto a datos rigurosamente seleccionados como a contenido "full-take". Véase Ryan Gallagher y Nicky Hager, "New Zealand Spies on Neighbors in Secret 'Five Eyes' Global Surveillance" (*The Intercept,* 4 de marzo de 2015) disponible en: https://theintercept.com/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore/

[31] De acuerdo con filtraciones del GCSB, existen sesiones informativas similares para el Reino Unido y los EE.UU. en la forma de capacitación "HRA" y "USSID-SP0018". Véase "GCSB access" disponible en: https://search.edwardsnowden.com/docs/GCSBaccess2015-03-06_nsadocs_snowden_doc

[32] Se solicita a los agentes que "copien y peguen los resultados en un documento de Word" para acceder a la base de datos compartida que deseen, lo que sugiere que no existe una aplicación técnica en vigor. Véase "GCSB access" (2011), disponible en: https://search.edwardsnowden.com/docs/GCSBaccess2015-03-06_nsadocs_snowden_doc

[33] "GCSB access" (2011), disponible en: https://search.edwardsnowden.com/docs/GCSBaccess2015-03-06_nsadocs_snowden_doc

de inteligencia deben ser más conscientes de que los intereses que están protegiendo no siempre coinciden con los intereses de esos servicios extranjeros y viceversa[34].

Eludiendo órdenes en Canadá. El caso Re (X)

> La Corte debe estar preocupada de que la autoridad que le otorga el Parlamento para autorizar actividades de investigación intrusiva del Servicio puedan ser percibidas en el ámbito público como una aprobación para vigilar e interceptar comunicaciones de la población canadiense por parte de agencias extranjeras.
>
> - Juez Mosley

En este caso, la Corte Federal de Canadá determinó que el Servicio de Inteligencia y Seguridad Canadiense (CSIS) había cometido "un incumplimiento del deber de sinceridad debido por el Servicio y sus asesores legales a la corte"[35]. En 2009, el juez Mosley otorgó permiso a la Agencia de Seguridad en las Comunicaciones (CSE) para ayudar al CSIS a vigilar a dos ciudadanos canadienses mientras estaban en el extranjero. Tal permiso era raro, ya que normalmente la CSE no tiene permitido interceptar las comunicaciones de los canadienses. El juez Mosley otorgó el permiso porque estaba convencido de que, al garantizarse que la vigilancia iba a ser recolectada y controlada desde dentro de Canadá, el CSIS y la CSE podían garantizar que las comunicaciones privadas que interceptaran de los canadienses solo se usarían en el caso de que fuesen esenciales para propósitos de seguridad nacional. Fue un precedente importante para el CSIS: durante los siguientes cuatro años, la Corte Federal emitió 35 órdenes judiciales similares basados en la decisión del juez Mosley.

Cuatro años después, el juez Mosley detectó en un informe de supervisión la recomendación de 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 al CSIS." El juez tomó la inusual decisión de llamar a los abogados del CSIS y la CSE para que se presentaran ante él y le explicaran qué estaba sucediendo exactamente. Se supo que la CSE había pedido a contrapartes de otras agencias –sus aliados de los Cinco Ojos–, que ayudaran a llevar a cabo la vigilancia electrónica. Esto violó claramente la letra y el espíritu de las garantías originales de la CSE. La orden judicial se había otorgado bajo el entendimiento específico de que el CSIS y la CSE controlarían la información de los objetivos canadienses, y que la información que reuniesen acerca de ellos permanecería en Canadá. Se reveló que la omisión del CSIS y la CSE de informar sobre su intención de pedir ayuda a otros aliados fue deliberada. El empleado de la CSE que compareció ante el juez admitió explícitamente que su presentación inicial fue cuidadosamente "elaborada" con asesoría legal para no mencionar a terceros a los que se podría pedir ayuda para llevar a cabo la vigilancia.

[34] Comité de Revisión de los Servicios de Inteligencia y Seguridad de los Países Bajos (CTIVD), "Review Report on the processing of telecommunications data by GISS and DISS" (5 de febrero de 2014), disponible en: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss/report-38-processing-telecommunications-data.pdf

[35] Véase Re (X), 2013 FC 1275, Tribunal Federal de Canadá, 2013. Para leer más sobre el caso véase "Vigilancia y democracia. Historias en diez países", INCLO, pp. 44–51, disponible en: https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf

II. De conformidad con la ley

La mayoría de las agencias de inteligencia son hoy en día órganos creados y regidos por disposiciones de orden legal. Hay autoridades legales que conducen la recolección de inteligencia, y salvaguardas y protecciones a la privacidad que actúan como un baluarte contra abusos y actos excesivamente intrusivos. Esto ha sido parte de una lenta transformación de las agencias de inteligencia para garantizar que los poderes de vigilancia se basen en la legislación nacional y cumplan con las leyes que protegen los derechos humanos. Sin embargo, todavía existen déficits o lagunas en las legislaciones domésticas que dirijan la aplicación de marcos legales a la cooperación o a los acuerdos de inteligencia internacional. A continuación, enumeramos la legislación nacional de los países miembros de INCLO, describimos el espectro de déficits emergentes y recomendamos normas y procedimientos claros que funcionen como estándar internacional.

A. Legislación nacional en los países miembros de INCLO

Argentina

En Argentina, la Ley de Inteligencia Nacional No. 25.520 es muy general y ambigua en sus facultades y normativas[36]. Aún mantiene un esquema regulatorio antiguo y deficiente en la atribución de facultades, mecanismos de control y acceso a la información. No autoriza expresamente a la Agencia Federal de Inteligencia (AFI) a firmar acuerdos internacionales de intercambio de inteligencia, ni ofrece ninguna protección respecto del intercambio de inteligencia sin procesar. Sin embargo, es altamente probable que haya regulaciones adicionales en la propia normativa de la AFI, que se mantienen en secreto. La Ley solo hace una referencia inespecífica a los cuerpos de inteligencia de otros países: en el artículo 13.4, establece que la AFI tiene entre sus funciones la de “dirigir y articular las actividades y el funcionamiento del Sistema de Inteligencia Nacional, así como también las relaciones con los organismos de inteligencia de otros Estados.”.

Canadá

El Servicio de Inteligencia y Seguridad Canadiense (CSIS) es el organismo que tiene la función central de recopilar, analizar y retener información e inteligencia humana respecto de las amenazas a la seguridad de Canadá. Tiene autoridad estatutaria para trabajar internacionalmente con agencias extranjeras. Cuando intercambia inteligencia con socios extranjeros, depende de la Ley del Servicio Canadiense de Inteligencia y Seguridad (Ley CSIS), que establece que el CSIS tiene permitido trabajar a nivel internacional. Su sección 17(1)(b) establece que puede, con la aprobación del Ministro, celebrar un acuerdo o cooperar con el gobierno de un Estado o institución extranjera con el propósito de llevar adelante sus deberes y funciones[37].

Como parte de su cooperación con socios extranjeros, el Ministro ha declarado que el CSIS no comparte datos sin procesar con socios extranjeros o nacionales; más bien, los productos de

[36] Ley de Inteligencia Nacional No. 25.520, art. 8.
[37] Ley del Servicio de Inteligencia de Seguridad de Canadá, RSC 1985, cC-23, s.17 (1)(b).

evaluación son compartidos "solo cuando se determina que están relacionados con una amenaza[38]." No queda claro qué se entiende por "productos de evaluación" en esta formulación.

La Agencia de Seguridad en las Comunicaciones (CSE), agencia de inteligencia de señales de Canadá, es actualmente administrada por el Departamento de Defensa Nacional y su mandato está consagrado en la Ley de Defensa Nacional [39]. La Ley actual no contiene ninguna autoridad explícita, ni ninguna limitación, con respecto al intercambio de información con entidades extranjeras. Sin embargo, existe una directiva ministerial para abordar los riesgos de compartir información con entidades extranjeras (recientemente actualizada en 2017) que, entre otras cuestiones, refiere al uso de la información obtenida mediante la práctica de la tortura[40]. Este déficit de autoridad y limitaciones sobre el intercambio de inteligencia ha sido abordado por el proyecto de ley C-59 sobre cuestiones de seguridad nacional, presentado en junio de 2017. El proyecto plantea un nuevo estatuto, la Ley de Establecimiento de Seguridad en las Comunicaciones, que dispone que la CSE puede concertar acuerdos con entidades que tengan poderes y deberes similares a los de la Ley, incluyendo instituciones de Estados extranjeros u organizaciones estatales internacionales, o instituciones de esas organizaciones. Estos arreglos tienen como fin promover las facultades de la CSE, incluyendo el intercambio de información o cooperación con dichas entidades, sujeto a la aprobación del Ministro de Defensa Nacional, que primero debe consultar con el Ministro de Relaciones Exteriores[41].

Colombia

En Colombia, la cooperación internacional entre agencias de inteligencia[42] está permitida explícitamente. El artículo 11 de la Ley 1621 de 2013 dice: "Los organismos de inteligencia y contrainteligencia podrán cooperar con organismos de inteligencia homólogos en otros países, para lo cual se establecerán los protocolos de seguridad necesarios para garantizar la protección y reserva de la información, de conformidad con las disposiciones contempladas en la presente Ley".

El artículo 6 del Decreto 4179 de 2011[43] también alienta la cooperación de la Dirección Nacional de Inteligencia en cuestiones de inteligencia y contrainteligencia, pero en el marco de tratados

[38] Ibíd.
[39] Ley de Defensa Nacional (R.S.C. 1985, c. N-5)
[40] Algunas legislaciones comportan una práctica positiva limitada. En Canadá, la Ley CSIS 1984, sección 17(2) requiere que el Comité de Revisión (actualmente el Comité de Revisión de Inteligencia de Seguridad, SIRC) reciba copias de todos los acuerdos del CSIS con gobiernos extranjeros y organizaciones internacionales. Este requisito seguirá vigente en la legislación de seguridad nacional propuesta actualmente ante el Parlamento canadiense aunque, de aprobarse el proyecto de Ley C-59, la revisión será realizada por una nueva e integrada Agencia de Seguridad Nacional y de Revisión de Inteligencia.
[41] Propuesta de Ley de Establecimiento de Seguridad en las Comunicaciones, s. 55 (1-2).
[42] En Colombia, la comunidad de inteligencia está compuesta por más de 24 agencias de inteligencia diferentes. Esta incluye la Dirección Nacional de Inteligencia (DNI), la Unidad de Análisis Financiero y la Dirección de Inteligencia Policial. Para todas las agencias identificadas, ver Dejusticia, "Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo" pp. 120-121, disponible en: https://www.dejusticia.org/publication/acceso-a-los-archivos-de-inteligencia-y-contrainteligencia-en-el-marco-del-posacuerdo/
[43] Como se establece en el artículo 6 del Decreto 4179 de 2011, una de la funciones de la Dirección Nacional de Inteligencia (DNI) es "adelantar acuerdos de cooperación internacional en temas relacionados con inteligencia y contrainteligencia, teniendo en cuenta las políticas de Gobierno y la normativa vigente, dentro del marco de

internacionales vinculantes para Colombia y respetando la facultad del presidente de la república para dirigir las relaciones internacionales.

Hungría

En Hungría, la Ley 125 de 1995 permite que la Oficina de Información y los Servicios de Seguridad Nacional compartan información internacionalmente para fines de seguridad nacional y decisiones gubernamentales[44]. Fomenta la cooperación con agencias de inteligencia extranjeras y el envío de datos personales, pero solo dentro de los límites prescritos por las normas legales que protegen los datos personales.

En concreto, la Ley 125 de 1995 permite que la Oficina de Información y los Servicios de Seguridad Nacional obtengan, analicen, evalúen y reenvíen información extranjera de relevancia o de origen extranjero que pueda utilizarse para promover la seguridad de la nación, necesaria para la toma de decisiones a nivel gubernamental [Art. 4 (a)]; para cooperar con agencias de inteligencia extranjeras sobre la base de acuerdos y compromisos internacionales [Art. 28 (4)]; y reenviar datos personales a administradores extranjeros de datos dentro de los límites de las normas legales que se aplican a la protección de datos personales (Art. 45).

Irlanda

La sección 28 de la Ley de la Garda Síochána 2005-2015 permite que el Comisionado de la Garda, con el consentimiento del Gobierno, celebre acuerdos con fuerzas policiales u organismos de seguridad fuera del Estado para una variedad de propósitos. De manera similar, el objetivo explícito de la Ley de 2008 de Justicia Penal (Asistencia Mutua) es efectivizar ciertos acuerdos internacionales entre el Estado y otros Estados relacionados con la asistencia mutua en asuntos penales. El artículo 75 de esta última Ley brinda una vía de acceso a datos retenidos con el fin de cumplir con solicitudes de un cuerpo policial o agencia de seguridad extranjera.

Asimismo, se ha confirmado en varias ocasiones que existe un intercambio entre Irlanda y agencias de inteligencia extranjeras[45]. En 2013, el entonces ministro de Justicia e Igualdad, Alan Shatter, dijo que existen enlaces de inteligencia entre la división de Inteligencia de las Fuerzas de Defensa (G2) y otros países en asuntos de seguridad del Estado[46]. La G2 no tiene una base jurídica y es considerada

---

los tratados internacionales vinculantes para Colombia y del respeto de la facultad del Presidente de la República de dirigir las relaciones internacionales".

[44] La Ley 125 de 1995 permite a la Oficina de Información y Servicios de Seguridad Nacional obtener, analizar, evaluar y remitir información de relevancia extranjera o de origen extranjero que pueda utilizarse para promover la seguridad de la nación, necesaria para la toma de decisiones a nivel gubernamental [Art. 4 (a)]; cooperar con agencias de inteligencia extranjeras sobre la base de acuerdos y compromisos internacionales [Art. 28 (4)]; y reenviar datos personales a los administradores de datos extranjeros dentro de los límites de las normas legales que se aplican a la protección de datos personales (Art. 45).

[45] Véase por ejemplo Alan Shatter, ministro de Justicia e Igualdad: "La Subdivisión de Inteligencia de las Fuerzas de Defensa proporciona evaluaciones periódicas, informes e informes al Jefe del Estado Mayor, al ministro de Defensa y al Secretario General del Departamento de Defensa, en relación con amenazas internas o externas a la seguridad del Estado e intereses nacionales. El enlace de inteligencia se lleva a cabo entre la Rama de Inteligencia y las autoridades nacionales de otros países para contrarrestar cualquier amenaza a la seguridad del Estado", Dáil Debates, respuestas por escrito, 18 de June de 2013.

[46] Disponible en: https://www.kildarestreet.com/wrans/?id=2013-06-18a.42

prácticamente como una rama de las Fuerzas de Defensa, que están legisladas por la Ley enmendada de Defensa de 1954[47].

India

Si bien en la India las agencias de inteligencia[48] parecen estar sujetas a regulaciones legales, la opacidad es la norma en lo que respecta a las acciones de vigilancia y al intercambio de inteligencia. Esto se ve reflejado en normas como la Ley de Tecnología de la Información de 2008. Esta Ley permite interceptar, controlar y descifrar información digital en virtud de las "relaciones amistosas con naciones extranjeras", así como de la defensa y seguridad del Estado, del orden público, de la investigación de un delito y de la soberanía e integridad de la India, previniendo la incitación a la comisión de cualquier delito reconocible.

Israel

En Israel no existe una legislación específica que autorice explícitamente a las agencias de inteligencia del Estado a intercambiar información o inteligencia sin procesar con organizaciones similares en el extranjero. Sin embargo, la Ley 5762-2002 del Servicio General de Seguridad permite que la agencia nacional de inteligencia de Israel, el Servicio General de Seguridad (SSG), comparta información con otros órganos en s8(a): "Para el cumplimiento de sus funciones, el Servicio tendrá competencia, a través de sus empleados... para transmitir información a otros organismos de acuerdo con las reglas que se prescribirán y estarán sujetas a las disposiciones de cualquier ley".

Además, no existe una legislación que regule el comportamiento de la agencia nacional de inteligencia militar, la Unidad de Inteligencia Militar 8200.

Kenia

Kenia carece de disposiciones legales explícitas que dirijan los acuerdos de intercambio de inteligencia con otros Estados. Si bien el intercambio de inteligencia no se menciona explícitamente, la sección 36(5) de la Ley de Prevención del Terrorismo de 2012 trata sobre las comunicaciones interceptadas y la posibilidad de que sirvan como evidencia. La sección 36(5)(b) establece específicamente la admisibilidad de las comunicaciones "interceptadas y retenidas en un Estado extranjero de acuerdo con la ley de ese Estado extranjero y certificadas por un tribunal de ese Estado extranjero como interceptadas y retenidas". Con el fin de ampliar el alcance de las agencias

[47] En Irlanda, las Fuerzas de Defensa tienen sus orígenes en el Ejército Republicano Irlandés (IRA), una organización guerrillera que combatió a las fuerzas del gobierno británico durante la Guerra de Independencia de Irlanda. El 16 de enero de 1922, la administración británica entregó el castillo de Dublín y el Gobierno Provisional asumió el poder. El 31 de enero de 1922, una antigua unidad del IRA (la Guardia de Dublín) asumió su nuevo papel como la primera unidad del nuevo Ejército Nacional. El 3 de agosto de 1923, el nuevo Estado aprobó la Ley de Fuerzas de Defensa (Disposiciones Temporales), que brindó una base legal a las fuerzas armadas existentes. Esa Ley permitía que "una fuerza armada se llamara Óglaigh na hÉireann (en lo sucesivo, las Fuerzas) y consistiera en la cantidad de oficiales, suboficiales y hombres que eventualmente proporcionaría el Oireachtas". Las Fuerzas de Defensa se establecieron el 1 de octubre de 1924, y el término Ejército Nacional cayó en desuso.

[48] En la India, la comunidad de inteligencia está conformada por numerosas agencias que incluyen (pero no se limitan a) el Ala de Investigación y Análisis, la Oficina de Inteligencia, la Organización Nacional de Investigación Técnica, la Agencia de Inteligencia de Defensa, las Oficinas Conjuntas de Cifrado y las direcciones de inteligencia del Ejército, Fuerza Aérea y Marina.

de seguridad que podrían iniciar acciones de vigilancia bajo esta Ley, la sección 36A se introdujo mediante enmienda para otorgar a las agencias de seguridad nacionales el poder de interceptar comunicaciones con el propósito de detectar, disuadir e interrumpir el terrorismo de acuerdo con los procedimientos que se prescribirán por el Secretario del Gabinete"

Intercambio de inteligencia en Kenia

Hay ejemplos destacados del intercambio de inteligencia de Kenia con Estados extranjeros.

- Durante una visita oficial de estado en 2016, el primer ministro israelí, Benjamin Netanyahu, dijo que Israel cooperaría con Kenia en cuestiones de inteligencia relacionadas con el terrorismo[49].
- En mayo de 2017 el embajador estadounidense Bob Godec reconoció que Estados Unidos brinda asistencia técnica a los servicios de seguridad kenianos en relación con varios procedimientos policiales que incluyen investigación del terrorismo y recolección de inteligencia[50].
- En junio de 2017, el ministro de Tecnología de la Información y la Comunicación de Kenia afirmó que Kenia y EE.UU. habían acordado colaborar en cuestiones de ciberseguridad y economía digital[51].

Rusia

En Rusia, el Artículo 13 de la Ley Federal "Sobre el Servicio Federal de Seguridad"[52], le otorga al Servicio Federal de Seguridad (FSB) el derecho de relacionarse con servicios de inteligencia y agencias de aplicación de la ley de Estados extranjeros. Específicamente, les permite intercambiar información operacional, técnica y de otro tipo con agencias extranjeras sobre una base recíproca. Toda la información y las cláusulas específicas sobre dicha cooperación están clasificadas.

Sudáfrica

En Sudáfrica, el ejecutivo nacional tiene el poder constitucional de entablar acuerdos vinculantes con otros Estados, incluyendo acuerdos de intercambio de inteligencia[53]. Cuando estos sean de naturaleza "técnica, administrativa o ejecutiva" y no requieran "ratificación o adhesión", como es el caso de los acuerdos de intercambio de inteligencia, todo lo que se requiere para comprometer a Sudáfrica es que el acuerdo se presente en el Parlamento[54]. El Comité pertinente es el Comité

[49] Véase el breve video disponible en: https://youtu.be/CW_B4jGSvbM; Nancy Agutu, "Israel will share intelligence in anti-terror war, Netanyahu tells Kenya" (*The Star*, 5 de julio de 2016), disponible en: https://www.the-star.co.ke/news/2016/07/05/video-israel-will-share-intelligence-in-anti-terror-war-netanyahu_c1380975)

[50] Declaración contenida en comentarios disponible en: https://ke.usembassy.gov/ambassador-godecs-remarks-outstanding-police-service-awards/

[51] Declaración del Ministerio de Información, Comunicaciones y Tecnología disponible en: http://www.ict.go.ke/kenya-to-collaborate-with-us-in-cyber-security/

[52] Véase Acuerdo No. 40-FZ of April 3, 1995.

[53] Constitución de la República de Sudáfrica, s. 231.

[54] Constitución de la República de Sudáfrica s. 231(2).

Permanente Conjunto sobre Inteligencia, que opera en secreto por defecto. Por lo tanto, cuando se concluyen los acuerdos de intercambio de inteligencia existe cierta supervisión, pero no un escrutinio público.

El intercambio de inteligencia lo lleva a cabo la Agencia de Seguridad del Estado (SSA), facultada por la Ley de Inteligencia Estratégica Nacional 39 de 1994 s2(2)(c) "para actuar de enlace con servicios de inteligencia o de seguridad u otras autoridades, de otros países o foros intergubernamentales de inteligencia o servicios de seguridad". Según s2(2)(f), la SSA puede "cooperar con cualquier organización en la República o en cualquier otro lugar para lograr sus objetivos[55]". El ministro de Seguridad del Estado tiene el poder de regular la manera en que se comparte la inteligencia y cualquier asunto accesorio bajo la sección 6 de la Ley Nacional de Inteligencia Estratégica. Todas estas disposiciones leídas conjuntamente ofrecen los medios para instancias individuales de intercambio de productos de inteligencia.

Estados Unidos

En los Estados Unidos, la comunidad de inteligencia depende principalmente del artículo II de la Constitución y Orden Ejecutiva 12333[56] (EO 12333) –que se basa a su vez en el artículo II– para coordinar el intercambio de información y celebrar acuerdos de inteligencia compartida con gobiernos extranjeros. Además, la Sección 104A(f) de la Ley de Seguridad Nacional de 1947 autoriza al Director de la Agencia Central de Inteligencia (CIA) a "coordinar las relaciones entre los elementos de la comunidad de inteligencia y los servicios de inteligencia o seguridad de los gobiernos extranjeros... en todos los asuntos que involucren inteligencia relacionada con la seguridad nacional o que impliquen inteligencia adquirida a través de medios clandestinos". La EO 12333 otorga al Director de la Inteligencia Nacional la responsabilidad de "celebrar acuerdos de inteligencia y contrainteligencia con gobiernos extranjeros y organizaciones internacionales."

La Sección 1.7 de la EO 12333 dispone que "los jefes de departamentos y agencias con organizaciones en la comunidad de inteligencia o los jefes de dichas organizaciones, según corresponda, deberán: (f) Difundir información de inteligencia a gobiernos extranjeros que cooperen en virtud de acuerdos establecidos o acordados por el Director de la Central de Inteligencia."

Reino Unido

La Ley de Poderes de Investigación (Investigatory Powers Act) de 2016 ahora incluye una referencia expresa, aunque limitada, al intercambio y divulgación de material en el extranjero[57]. Las protecciones[58] se aplican a la divulgación de material recolectado mediante intercepciones en bloque u órdenes de "interferencia de equipo" en el exterior. Estas protecciones incluyen la disposición de que solo el número mínimo de personas de una agencia extranjera tenga acceso al material, y que se hagan las copias mínimas necesarias de cualquier producto de inteligencia.

[55] Vale la pena señalar que una lectura liberal de s2(2)(f) podría abrir las puertas a la Agencia de Seguridad del Estado (SSA) para compartir o recibir inteligencia de actores no estatales.
[56] Orden Ejecutiva No. 12333, 3 C.F.R. 200 (1981), disponible en: https://www.archives.gov/federal-register/codification/executive-order/12333.html
[57] Ley de Poderes de Investigación (Investigatory Powers Act) 2016, disponible en: http://www.legislation.gov.uk/ukpga/2016/25/section/151/enacted
[58] Ibíd., en la Parte 6, capítulos 1 y 3.

Además, "el Secretario de Estado debe estar convencido de que la autoridad de ultramar cuenta con protecciones que se corresponden a las de la Ley en relación a la selección de datos a examinar". Tales protecciones contemplan que la selección del material a examinar se lleve a cabo con fines específicos y sea necesaria y proporcionada.

Revisión de la Corte Constitucional de Colombia C-540 de 2012

En Colombia, la cooperación internacional entre agencias de inteligencia está explícitamente permitida. El artículo 11 de la Ley 1621 de 2013[59] permite a las agencias de inteligencia cooperar con sus contrapartes en otros países por razones de seguridad. Este estatuto demanda protocolos para proteger la confidencialidad de la información de los ciudadanos intercambiada por las agencias de seguridad.

La constitucionalidad de esta Ley estuvo sujeta a una revisión obligatoria por parte de la Corte Constitucional colombiana (C-540 de 2012)[60]. El Tribunal declaró que el Artículo 11 era válido. Sin embargo, hizo una serie de observaciones importantes.

Primero, la disposición estatuaria que permite la cooperación internacional de agencias de inteligencia debe estar precedida por la intervención del Presidente de la República. "Al envolver relaciones internacionales debe acompañarse de los instrumentos internacionales de cooperación, máxime cuando se están comprometiendo asuntos de suma relevancia constitucional como la defensa y seguridad de la Nación y, como consecuencia, los derechos fundamentales de las personas residentes en Colombia" [61].

En segundo lugar, la transferencia de datos solo es legítima si el país receptor ofrece garantías de protección de datos comparables a las del país emisor. Esto refleja las pautas establecidas en la decisión reciente –pero no relacionada– de la Corte con respecto a la Ley de Protección de Datos (Ley 1581 de 2012).

En tercer lugar, las garantías de protección de datos deben incluir un marco de derechos para los titulares de los datos, obligaciones para quienes procesan la información personal, y un regulador o mecanismo de protección de datos para hacer cumplir las leyes de protección de datos basándose en los principios de protección de datos de Europa[62].

En cuarto lugar, cualquier protocolo de seguridad establecido debe tener en cuenta los mecanismos de derechos humanos de las Naciones Unidas. El tribunal se refirió específicamente al Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo[63].

[59] El artículo 11 de la Ley 1621 de 2013 establece: "Los organismos de inteligencia y contrainteligencia podrán cooperar con las agencias de inteligencia homólogas de otros países, para lo cual se establecerán los protocolos de seguridad necesarios para garantizar la protección y clasificación de la información, de conformidad con las disposiciones contempladas en esta Ley".
[60] Disponible en: http://www.corteconstitucional.gov.co/relatoria/2012/C-540-12.htm
[61] Ibíd.
[62] Tales principios articulados incluyen "La limitación del propósito; calidad de datos y proporcionalidad; transparencia; seguridad; acceso, rectificación y oposición; restricciones en transferencias sucesivas a otros países y disposiciones sectoriales o adicionales para el tratamiento de datos de tipo especial, incluidos los datos confidenciales, el marketing directo y la decisión individual automatizada".
[63] Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46_sp.pdf

B. Un abanico de déficits

La investigación de los miembros de INCLO sobre las leyes nacionales que regulan el intercambio internacional de inteligencia en sus países revela un espectro de déficits legales que van desde una falta total de compromiso para reglamentar las prácticas hasta la ausencia de controles rigurosos, control y revisión.

En países como Argentina, no existe un límite legislativo sobre lo que se puede compartir, con quién o con qué fin. En otros países, las agencias de inteligencia cuentan con disposiciones legales, pero se sabe poco acerca de cómo interpretan y aplican la normativa. En Israel, la ley pertinente exige que la actividad de intercambio de inteligencia se lleve a cabo "de acuerdo con las normas que se prescriban", pero no divulga cuáles son dichas normas[64]. En Hungría, debido a un ambiente político difícil que llevó a la reciente reelección de Viktor Orban, existen pocos mecanismos disponibles para arrojar luz sobre cómo funcionan realmente las disposiciones legales. Los mismos problemas surgen en Rusia, donde todas las normativas que legislan la cooperación están clasificadas. En Irlanda, la legislación pertinente no cumple de forma demostrable con la Carta de la Unión Europea y el Convenio Europeo de Derechos Humanos (CEDH). La falta de una regulación legislativa explícita que rija la cooperación entre servicios de inteligencia así como la ausencia de información pública respecto de cualquier documento interno, reglamentación o directriz detrás de dicha cooperación en estos países es profundamente preocupante.

Los países que tienen normas más explícitas legislando los acuerdos internacionales de intercambio de inteligencia también pueden padecer problemas importantes. En el Reino Unido, por ejemplo, las protecciones que se aplican a la interceptación y divulgación de información deben aplicarse solo "en la medida [si cabe] en que el Secretario de Estado considere apropiado". Tampoco existen requisitos de transparencia con respecto a qué autoridades extranjeras aplicarán qué garantías o cómo. No hay nada en el esquema del Reino Unido que cubra la recepción de material SIGINT sin procesar, un problema que el Comité de Inteligencia y Seguridad había criticado sobre la base de

---

Véanse prácticas 31 a 35, que requieren que los acuerdos de inteligencia internacional (i) Se basen en la legislación nacional que prevé normas bien definidas para esta operación, incluidas las condiciones que deben reunirse, las entidades con las que puede intercambiarse información y las salvaguardias aplicables a esos intercambios; (ii) provean una declaración de las partes en las que se comprometen a respetar los derechos humanos y proteger los datos, y una disposición según la cual el servicio que envíe la información puede pedir explicaciones sobre el uso de la información enviada; (iii) establezcan cauces de responsabilidad para el uso compartido de información; (iv) aseguren que toda la información enviada sea pertinente para el mandato del receptor, y que se utilizará de conformidad con las condiciones prescritas y no se destinará a fines contarios a los derechos humanos y (v) dejar un registro por escrito de todas las actividades de intercambio de información".

[64] Véase la Ley del Servicio General de Seguridad, 5762-2002, s22(a): "Las reglas, las directivas del Servicio y los procedimientos del Servicio en virtud de esta Ley no necesitan publicarse en *Reshumot* ni en ninguna otra publicación de carácter público". Reshumot es el boletín oficial del gobierno, y contiene, entre otras cosas, publicaciones de legislativas, proyectos de ley gubernamentales y legislación subsidiaria. Disponible en: http://www.justice.gov.il/En/Units/OfficialPublications/Pages/default.aspx

que "la proporción de material interceptado obtenido de socios internacionales es tal que no es apropiado excluirlo de legislación que pretende cubrir la interceptación[65]".

En los Estados Unidos, si bien el poder ejecutivo ha establecido ciertos límites a sus intercambios de inteligencia sin procesar, estos son en gran medida inaplicables. Las limitaciones incluyen la "minimización" de los registros relacionados con personas de los EE.UU.[66],y disponen garantías de seguridad para la protección de información clasificada e información sensible. Sin embargo, esas limitaciones han sido desarrollados por el ejecutivo mismo y no son exigibles en los tribunales estadounidenses. Además, la Directiva de Política Presidencial 28 sobre Actividades de Inteligencia de Señales permite compartir "SIGINT no evaluada" bajo la única muy permisiva y aparente condición de que el gobierno "informe al destinatario que la divulgación puede contener información personal, de modo que el destinatario pueda tomar medidas adecuadas para proteger dicha información" [67].

Del mismo modo, en Colombia, las protecciones que se aplican a la información que se comparte son establecidas por autoridades administrativas y no por el Parlamento. Al ordenar a las agencias de inteligencia a establecer protocolos de seguridad para el intercambio de información, el Artículo 11 de la Ley 1621 de 2013 otorga a las agencias de inteligencia el poder de regular los aspectos básicos del derecho fundamental a la protección de datos. Esto plantea claras cuestiones constitucionales acerca de la capacidad de las agencias para establecer reglas que competen a los derechos fundamentales sin control parlamentario.

Por su parte, la nueva legislación de seguridad nacional del gobierno de Canadá no requerirá control judicial o cuasijudicial independiente para los acuerdos de intercambio de inteligencia, aunque habrá, posiblemente, una revisión posterior al hecho de parte de la nueva Agencia de Seguridad Nacional y de Revisión de Inteligencia. El recién creado Comité de Parlamentarios de Seguridad e Inteligencia Nacional también podría tener algún rol, aunque hay una disposición dentro de su legislación por la cual los ministros del gobierno pueden rechazar el acceso del Comité a información "perjudicial para la seguridad nacional[68]", con lo que no queda clara su actual efectividad en el área del intercambio de información. La agencia cuasijudicial creada para supervisar algunas autorizaciones ministeriales –el Comisionado de Inteligencia–, no está específicamente destinada a supervisar el intercambio de inteligencia de señales por parte de la CSE. Tales acuerdos necesitarán

[65] Comité de Inteligencia y Seguridad del Parlamento, "Report on the draft Investigatory Powers Bill" (9 de febrero de 2016), disponible en: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20160209_ISC_Rpt_IPBill%28web%29.pdf?attachauth=ANoY7crUSED1hym_S-nCb3jS0n4Z84G3IUl2XrHmskxULqPOu5Ri0cybEIjtVmFQwqol0Sh-HYVp4i4I0pyHB3BU0D4IkvGUo7hAfG-NsBf8tgC89I69FZw8lmm9Tw_qigw_MNgkYsgMRaB7yznL7gTTuGFGrYLpJe0wCuzMoGxdB-x6RWzIiTo9EiZhg9rbtjOVvidOSHCqgxTfgKFX69xRYpJobeeCjaNfOOZDKE2BMOygvPbmrdpPnbW0tFk5mwKnh0cG0MeD&attredirects=0

[66] Directiva de Inteligencia de Señales de EE.UU. SP0018, Cumplimiento legal y procedimientos de minimización, s.7, 25 de enero de 2011.

[67] PPD-28 Sección 4 Procedimientos s. 7.2, 12 de enero de 2015. Disponible en: https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf

[68] Una Ley para establecer el Comité de Parlamentarios de Seguridad e Inteligencia Nacional y para establecer enmiendas consiguientes a ciertas Leyes, S.C. 2017, c. 15, s. 16 (1) (b).

solamente la aprobación del ministro de Defensa Nacional, después de que el ministro haya consultado con el ministro de Asuntos Exteriores[69].

Recomendación I de INCLO: normas y procedimientos claros

A pesar del creciente cuerpo de normas que regulan a las agencias de inteligencia, hay serios déficits en las leyes de los países miembro de INCLO. La falta de leyes y políticas internas sólidas que guíen los acuerdos de intercambio de inteligencia socava el núcleo mismo de los procesos democráticos.

Para proteger adecuadamente nuestros derechos humanos consagrados, INCLO respalda la recomendación del Panel de Juristas Eminentes de la Comisión Internacional de Juristas acerca de que los Estados deben establecer estatutos, políticas, reglamentos y procedimientos claros y aplicables respecto del intercambio de información con agencias de inteligencia extranjeras[70]. Asimismo, las políticas deben necesariamente reflejar los estándares y mecanismos de derechos humanos pertinentes y, en particular, el derecho a la privacidad, la libertad de expresión y la libertad de asociación[71]. Deben incluir principios de proporcionalidad y necesidad[72] y eliminar las prácticas de recolección en bloque de conformidad con la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas[73]. Deben exigir procesos efectivos de notificación así como procesos de reparación, con capacidad de cruzar fronteras hacia las personas afectadas[74].

[69] Propuesta de Ley de Establecimiento de Seguridad en las Comunicaciones, s. 55 (1-2)
[70] Panel de juristas eminentes de la Comisión Internacional de Juristas, “Evaluación de daños, acciones urgentes”, Ginebra, 2009, 90.
[71] Véanse los artículos 17, 19 y 22 de la Asamblea General de las Naciones Unidas, "Pacto Internacional de Derechos Civiles y Políticos" (16 de diciembre de 1966); Artículos 12, 19 y 20 de la Asamblea General de la ONU, 'Declaración Universal de los Derechos Humanos' (10 de diciembre de 1948); Artículos 9, 10 y 11 del Consejo de Europa, 'Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, modificado por los Protocolos nos. 11 y 14' (1 de junio de 2010); Artículo 9 de la Carta Africana de Derechos Humanos y de los Pueblos.
[72] Véase, por ejemplo, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, “Libertad de expresión e Internet” (31 de diciembre de 2013) para. 165, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf
[73] Véase el caso de *Tele2 Sverige*, Tribunal de Justicia de las Comunidades Europeas, C-203/15, ECLI: EU: C: 2016: 970, mn. 103: “Además, si bien la eficacia de la lucha contra los delitos graves, en particular el crimen organizado y el terrorismo, puede depender en gran medida del uso de técnicas de investigación modernas, ese objetivo de interés general, por fundamental que sea, no puede en sí mismo justificar que la legislación nacional que prevé la retención general e indiscriminada de todos los datos de tráfico y ubicación se considere necesaria para los fines de esa lucha”. Disponible en: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd4fc86499d441497a8c79b137b006e4ef.e34KaxiLc3qMb40Rch0SaxyNbNv0?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1255745
[74] Véase el Primer Informe del Relator Especial de las Naciones Unidas sobre el derecho a la privacidad en el Consejo de Derechos Humanos, A/HRC/31/64 (8 de marzo de 2016), p. 4, disponible en: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

III. Sin control y sin rendir cuentas

Proteger los derechos humanos requiere de un fuerte control y revisión de las prácticas de intercambio de inteligencia entre Estados para garantizar que las agencias de inteligencia cumplan las leyes nacionales y las normas de derechos humanos a través de sus asociaciones internacionales de intercambio de inteligencia. Deben redactarse leyes fuertes para garantizar que las exenciones, incluida la información suministrada por terceros ("Third Party Rule") [75], no eludan las supervisiones. Esta regla establece que la información compartida con agencias de inteligencia extranjeras no se puede compartir con otros terceros sin el permiso de la agencia de inteligencia que originalmente brindó la información. Con frecuencia, se considera a los órganos de control como "terceros" y, en calidad de tales, no pueden sondear adecuadamente la información relacionada con la cooperación internacional.

A. Prácticas de control y revisión en países miembro de INCLO

Argentina

En Argentina, la Comisión Bicameral de Fiscalización de Organismos y Actividades de Inteligencia del Congreso, creada por la Ley de Inteligencia Nacional*,* tiene la función de supervisar los procedimientos de la Agencia Federal de Inteligencia para obtener y reunir inteligencia, incluida la cooperación en materia de inteligencia. Sin embargo, la Comisión no ha sido muy activa y nunca ha hecho declaración alguna sobre la cooperación de inteligencia en sus informes.

Canadá

Canadá cuenta con revisiones de inteligencia *después* del intercambio de inteligencia, y de forma selectiva. El Comité de Revisión de Inteligencia de Seguridad canadiense (SIRC), el organismo de revisión del CSIS, ha hecho referencias y recomendaciones sobre las prácticas de intercambio de información del CSIS en sus tres informes más recientes. De hecho, uno de los objetivos del SIRC es "comprender mejor la relación del CSIS con sus socios nacionales y extranjeros mediante la evaluación de las actividades conjuntas, así como la cooperación operativa y el intercambio de información llevado a cabo por 'entidades extranjeras'[76]." En sus últimos tres informes, el SIRC ha prestado atención a las prácticas de intercambio de inteligencia del CSIS, incluida su cooperación con entidades extranjeras.

La oficina del Comisionado de la Agencia de Seguridad de las Comunicaciones, CSE, dejó claro en el pasado que no es capaz de evaluar con precisión si los socios de los Cinco Ojos cumplen sus promesas de proteger la información de los canadienses. La Canadian Press informó sobre una copia

[75] En el contexto de las relaciones de inteligencia de EE.UU., se conoce a los EE.UU. como el "la primera parte" y el Reino Unido, Canadá, Australia y Nueva Zelanda como "segundas partes". Rodos los demás países con una relación se consideran "terceros".
considered 'third parties'.

[76] Comité de Revisión de Inteligencia de Seguridad, "Accelerating Accountability: Annual Report 2016-2017", (Public Works and Government Services Canada, 2017), p. 28.

redactada de un informe de 2013 del entonces comisionado Robert Decary, quien escribió que el tema le preocupaba, ya que "estas actividades pueden afectar directamente la seguridad de un ciudadano de Canadá". Lo que descubrió fue que más allá de "ciertas declaraciones y garantías generales" entre la CSE y sus socios, era "incapaz de evaluar en qué medida los socios de los Cinco Ojos se circunscriben a los acuerdos con la CSE y protegen las comunicaciones privadas y la información sobre canadienses que el organismo comparte con los socios".

En el informe anual del Comisionado de la CSE 2016-17, se consigna una revisión del intercambio de información de la CSE con entidades extranjeras de febrero de 2010 a marzo de 2015[77]. El Comisionado descubrió que las dos secciones encargadas de las evaluaciones de riesgos dentro de la CSE no eran igualmente efectivas siguiendo protocolos, manteniendo registros o emitiendo advertencias, y notó la ausencia de una política general en lo referido al intercambio de información con entidades extranjeras. Emitió en consecuencia recomendaciones para mejorar las medidas de privacidad en algunos acuerdos formales con una cantidad de entidades extranjeras no identificadas.

Colombia

En Colombia, el artículo 19 de la Ley 1621[78] entró en vigor en 2013 y ordenó la creación de una Comisión Legal Parlamentaria, encargada de monitorear las actividades de inteligencia y contrainteligencia. Su función apunta a garantizar la eficiencia de los recursos utilizados, el respeto a las garantías constitucionales, y el cumplimiento de los principios, límites y propósitos estatutarios que regulan las actividades de inteligencia y contrainteligencia.

Aunque esta Ley entró en vigencia hace casi 5 años, la Comisión aún no ha podido llevar a cabo todas sus actividades encomendadas debido a supuestos desafíos procesales. Por lo tanto y por lo que Dejusticia sabe, este órgano de control no ha hecho ningún llamamiento a mejorar la regulación en el intercambio de inteligencia.

Hungría

En Hungría no existe actualmente un control efectivo de los acuerdos de intercambio de inteligencia. El Comité de Seguridad Nacional en el Parlamento encargado de supervisar los Servicios de Seguridad Nacional ha quedado en el medio de intensas batallas políticas que han impedido el ejercicio de sus funciones. El jefe del partido de la oposición es parte del Comité, y su presencia ha llevado a los partidos gobernantes a negarse a participar en los trabajos del Comité. Según el discurso de los partidos gobernantes, los propios partidos de oposición representan una amenaza para la seguridad nacional, aunque todos los miembros del Comité han sido ya examinados por los servicios secretos.

---

[77] La revisión del Comisionado incluyó el proceso mediante el cual se comparte inteligencia de señales extranjeras con entidades extranjeras; el marco legislativo y normativo relacionado con el intercambio de información con entidades extranjeras; si la CSE adquirió de entidades extranjeras y/o divulgó a entidades extranjeras comunicaciones privadas o información sobre canadienses; una muestra de intercambios de información, que incluye 161 evaluaciones de riesgo de maltrato realizados para compartir información, y acuerdos formales existentes con entidades extranjeras.

[78] Disponible en http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

Irlanda

En Irlanda no existe control parlamentario o independiente de las funciones de intercambio de inteligencia, por lo que en la práctica estas funciones solo están controladas por una supervisión ejecutiva[79]. El Comisionado de Protección de Datos tiene un poder limitado para revisar los procesos de vigilancia y de intercambio de inteligencia. Sin embargo, existe una exclusión general que establece que la ley de protección de datos "no se aplica a (...) los datos personales que, en opinión del ministro [de Justicia] o del ministro de Defensa, se retienen, o en cualquier momento se retuvieron, con el fin de salvaguardar la seguridad del Estado[80]".

India

Se supone que las cuestiones relativas a las agencias de inteligencia de la India están sujetas al control del Parlamento a través de sus comités de control. Sin embargo, este proceso difiere respecto de cada agencia y los ciudadanos no tienen acceso a los datos de los comités. Por ejemplo, el Comité Conjunto de Inteligencia (JIC) del gobierno de la India analiza los datos de inteligencia de la Oficina de Inteligencia y del Ala de Investigación y Análisis, de la Dirección de Inteligencia Militar, de la Dirección de Inteligencia Naval y de la Dirección de Inteligencia Aérea. El JIC tiene su propia secretaría, que depende del Primer Ministro a través de la Secretaría del Gabinete. Se trata de un comité independiente. Sin embargo, el nivel de control que ofrece, si es que ofrece alguno, no queda claro. El proceso es muy opaco y los comités parlamentarios varían periódicamente. Las agencias de inteligencia disfrutan de un nivel de secretismo que las mantiene lejos del alcance de la Ley de acceso a la información, las coberturas mediáticas o las consultas públicas.

Sudáfrica

El Inspector General de Inteligencia (IGI) es un cuerpo independiente y con funciones constitucionales encargado del control de los servicios de inteligencia sudafricanos. El IGI está obligado a supervisar todos los aspectos de cada servicio de inteligencia del país mediante disposiciones que se encuentran en s7(7) de la Ley 40 de Supervisión de Servicios de Inteligencia de 1994 con el objeto de supervisar el cumplimiento de la Ley, revisar acciones específicas de los servicios de inteligencia y manejar denuncias de la población o denunciantes dentro de los servicios de inteligencia. El IGI tiene el poder de acceder a toda la documentación, información o instalaciones de inteligencia conforme a la sección 7(8) de la misma Ley.

El presidente del IGI, Dr. Sethlomamaru Dintwe, declaró además que considera que el control del intercambio de información es una parte importante de las funciones de su oficina[81]. Sin embargo, reconoció que debido a limitaciones presupuestarias y de recursos humanos, su área se ve obligada a centrarse en las denuncias, y emprender el control y revisión de áreas críticas de recolección de inteligencia y, por lo tanto, del intercambio de inteligencia, no ha sido objeto de sus informes de supervisión recientes.

[79] Para un debate sobre las autoridades de inteligencia de Irlanda, véase Dr. TJ McIntyre, "National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update" 29 de junio de 2016.
[80] Sección 1(4) de las leyes de protección de datos de 1988 y 2003.
[81] Entrevista del Legal Resource Centre de Sudáfrica (LRC) con Setlhomamaru Dintwe, Inspector General de Inteligencia, y otro.

El Comité Permanente Conjunto de Inteligencia también tiene la tarea de supervisar los servicios de inteligencia. Se trata de un comité multipartidario, proporcionalmente representativo, conformado por miembros de ambas cámaras del Parlamento[82]. Como se señaló anteriormente, cuando se concluye un acuerdo internacional de intercambio de inteligencia, es este Comité el que recibe el texto del acuerdo según las Reglas de la Asamblea Nacional. Este Comité también recibe informes producidos por el IGI que pueden incluir temas relacionados con el intercambio de inteligencia. Como órgano de la legislatura, el Comité puede responsabilizar al ministro de Seguridad del Estado por las acciones de la Agencia de Seguridad Estatal (SSA) al compartir o recibir productos de inteligencia. Si bien a primera vista este proceso puede parecer relativamente transparente, las Reglas de la Asamblea Nacional estipulan que la presentación de tales acuerdos se realiza remitiéndolo al correspondiente Comité de Cartera[83].

Las preguntas sin respuesta de Naidoo[84]

Kumi Naidoo, ciudadano sudafricano, es un activista de trayectoria. Fue Director Ejecutivo Internacional de Greenpeace y hace poco fue nombrado Secretario General de Amnistía Internacional. En 2015, un periodista de Al Jazeera contactó a Naidoo y le comunicó que los cables de inteligencia filtrados revelaban que Corea del Sur lo había identificado como una posible amenaza a la seguridad durante la cumbre del G20 2010 en Seúl. Corea del Sur solicitó a Sudáfrica "evaluaciones específicas de seguridad" acerca de Naidoo, vinculándolo con otros dos sudafricanos que habían sido arrastrados en un raid antiterrorista en Pakistán y luego liberados. Sudáfrica nunca informó a Naidoo de la solicitud de Corea del Sur, y Naidoo cree que el servicio de inteligencia hizo la solicitud debido a su abierta oposición a la energía nuclear.

En julio de 2015, el Legal Resources Centre (LRC) de Sudáfrica emitió una solicitud de acceso a la información pública en nombre de Naidoo a la Agencia de Seguridad Estatal (SSA) pidiendo los registros relacionados con la operación de vigilancia solicitada. La SSA no ha emitido ninguna respuesta a esa solicitud. Tal inacción se considera un rechazo de la solicitud en virtud de la legislación sudafricana y, por lo tanto, el LRC interpuso un recurso interno, nuevamente sin respuesta. El LRC presentó una queja ante el Inspector General de Inteligencia el 15 de septiembre de 2017[85] y puede iniciar procedimientos judiciales en función del resultado de la denuncia para garantizar el acceso a cualquier producto de inteligencia compartido o a acuerdos bajo el cual se realizara el intercambio.

Mientras tanto, la respuesta pública dada por el gobierno sudafricano respecto de la información filtrada, y que sugiere que pudo haber puesto bajo vigilancia a un ciudadano –un activista pacífico de fama mundial–, es especialmente preocupante. En lugar de abrir un diálogo sobre posibles actividades de vigilancia, el Servicio de Seguridad de Sudáfrica condenó las filtraciones e indicó que se había iniciado una investigación completa sobre ellas; no sobre la posible vigilancia sobre Naidoo.

[82] Ley nacional de inteligencia estratégica, s. 2.
[83] Reglas de la Asamblea Nacional de Sudáfrica, novena edición, regla 343.
[84] Para saber más véase "Vigilancia y democracia. Historias en diez países", INCLO, disponible en: https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf. Véase también Apéndice VII para documentación relevante.
[85] Véase Apéndice VII para ver una copia de esa solicitud.

Reino Unido

En el Reino Unido no se había hecho referencia al intercambio de inteligencia en bloque sin procesar antes de las revelaciones de Snowden. Sin embargo, después de una campaña y un litigio sobre el tema, la oficina del Comisionado de Interceptación de Comunicaciones declaró que encargó una investigación sobre el intercambio internacional del material interceptado[86]. El informe explicaba que "en 2015 encargamos una investigación sobre los arreglos del Cuartel General de Comunicaciones del Gobierno (GCHQ) para compartir material interceptado y datos de comunicaciones con socios extranjeros con el fin de revisar el cumplimiento de las salvaguardas contempladas en la sección 15. Todavía estamos en proceso de llevar a cabo esta investigación. Una vez que se haya completado a fondo, necesitaremos una actualización anual sobre cualquier cambio o nuevos arreglos. Esta es un área que hemos estado discutiendo con nuestras contrapartes internacionales". La investigación sigue en curso.

Diez organizaciones de Derechos Humanos vs. el Reino Unido[87]

Este caso es el resultado consolidado de las objeciones lideradas por una serie de organizaciones de derechos humanos, incluidos siete miembros de INCLO[88] ante el Tribunal Investigador de Poderes (IPT). El caso comenzó en el IPT, un tribunal especial establecido para escuchar denuncias sobre casos de vigilancia ilegal. Las revelaciones de Edward Snowden plantearon la posibilidad de que las libertades civiles y las organizaciones no gubernamentales de todo el mundo no solo estuviesen en la mira de sus propios gobiernos sino de agencias de espionaje de otros países. El grupo de organizaciones se unió para saber si habían estado bajo la vigilancia del GCHQ[89].

Por primera vez en sus 11 años de historia, el IPT emitió una resolución desfavorable para con el gobierno en la demanda presentada por las diez organizaciones de derechos humanos. Sostuvo que el procedimiento que el gobierno del Reino Unido había utilizado para recibir información reunida por el gobierno de los EE. UU.[90]había sido ilegal durante años porque la población desconocía las salvaguardas que protegían cualquier material compartido.

Pero el tribunal también sostuvo que, gracias a las divulgaciones hechas durante el litigio, las salvaguardas ahora eran lo suficientemente públicas y el régimen cumplía con las normas de

[86] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/548075/IOCCO_Report_March_2015__Web_.pdf

[87] App No. 24960/15

[88] Los miembros de INCLO incluyen Liberty, ACLU, CCLA, EIPR, HCLU, ICCL y LRC. Poco después de las revelaciones de Edward Snowden en junio de 2013, Liberty presentó una queja ante el Tribunal de Poderes de Investigación del Reino Unido (IPT). Privacy International presentó una queja similar ante el IPT en julio de 2013. El IPT finalmente juntó estos reclamos con los de muchos otros grupos nacionales e internacionales.

[89] Para saber más véase "Vigilancia y democracia. Historias en diez países", INCLO, disponible en: https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf. pp. 105–108.

[90] En concreto, la NSA había utilizado los programas estado utilizando PRISM y Upstream, para recolectar comunicaciones de empresas de Internet.

derechos humanos.

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, declaró que la vigilancia masiva era en realidad una consecuencia "inevitable" de la tecnología moderna, y que los poderes otorgados en la Ley de Regulación de Poderes de Investigación del año 2000 permitieron al gobierno británico espiar a ciudadanos extranjeros sin una orden que identificara al sujeto de la vigilancia.

Sin embargo, en junio de 2015, el IPT emitió una nueva resolución en la que reveló que dos de las organizaciones demandantes habían sido objeto de vigilancia ilegal por parte del GCHQ. El LRC fue una de esas dos organizaciones. En relación con el LRC, el IPT encontró que:

> las comunicaciones de una dirección de correo electrónico asociada al LRC fueron interceptadas y seleccionadas para su análisis de conformidad con la s8(4) de la Ley de Regulación de los Poderes de Investigación. El [IPT] está convencido de que la interceptación fue legal y proporcionada y que la selección para el análisis fue proporcionada, pero que el procedimiento establecido por las políticas internas del GCHQ para seleccionar comunicaciones para analizar fue por un error no seguido en este caso.

El IPT concluyó que se trataba de una violación del artículo 8 del Tribunal Europeo de Derechos Humanos, pero que estaba convencido de que "la agencia de interceptación no hizo uso alguno de ninguno de los materiales interceptados, ni retuvo ningún registro". En consecuencia, dictaminó que el LRC no había sufrido ningún perjuicio o daño importante, y no se otorgaron compensaciones.

Las diez organizaciones han llevado este asunto al Tribunal Europeo de Derechos Humanos. El caso se escuchó a fines de 2017 y estamos a la espera de un juicio. La decisión del Tribunal constituirá una de las primeras ocasiones en que un tribunal regional de derechos humanos decidirá sobre la legalidad de los regímenes de vigilancia masiva y especulativa en la era post-Snowden. En vista de la intransigencia del gobierno y de sistemas legales estancados, se trata de una oportunidad clave para que el Tribunal afirme y dé contenido al derecho a la privacidad e insista en la responsabilidad de los Estados.

Estados Unidos

En los Estados Unidos no ha habido declaraciones o audiencias formales recientes sobre el intercambio de inteligencia con gobiernos extranjeros en las dos comisiones del Congreso que supervisan a la comunidad de inteligencia del país: la Comisión Permanente Selecta sobre Inteligencia de la Cámara de Representantes, y la Comisión Selecta del Senado sobre Inteligencia. La Junta de Supervisión de Privacidad y Libertades Civiles tampoco emitió ningún informe que analice el tema de la cooperación internacional de inteligencia.

Recomendación II de INCLO: prácticas estrictas de control

Incluso en los casos en los que existen políticas y normas de protección, hasta tanto se establezcan prácticas explícitas de control y revisión, la posibilidad de que las agencias de inteligencia eludan leyes nacionales y normas concernientes a los derechos humanos a través de sus asociaciones internacionales de intercambio de inteligencia permanecerá abierta. INCLO recomienda las observaciones de la Comisión de Venecia del Consejo de Europa respecto de que los órganos de supervisión y control deberían "decidir las reglas generales con respecto a quién, y en qué circunstancias, la inteligencia de señales puede intercambiarse con otras organizaciones de inteligencia de señales[91]".

Además, compartimos las preocupaciones expresadas por el Tribunal Europeo de Derechos Humanos en el sentido de que "la práctica cada vez más extendida de los gobiernos de transferir y compartir entre ellos la inteligencia obtenida en virtud de la vigilancia secreta (...) es otro factor que requiere especial atención cuando se trata de control externo[92]".

IV. A salvo del escrutinio público

> Cuando en la sociedad civil hablamos sobre seguridad nacional, se nos acusa de ser poco realistas, ingenuos o poco conscientes de las amenazas y las realidades operativas. Sin embargo, si hubiese más información pública, sabríamos más. En una democracia, nunca debería ser poco realista pedir una mayor protección a los derechos y libertades fundamentales. Puede ser difícil; los derechos compiten y el equilibrio es complicado. Pero pedir transparencia a las agencias con poderes y responsabilidades extraordinarios no es ingenuo, es profundamente sensato. También es necesario para establecer la confianza, la legitimidad y la aprobación social de nuestras agencias de inteligencia.
>
> *- Brenda McPhail, Directora, Proyecto de Privacidad, Tecnología y Vigilancia, Canadian Civil Liberties Association*

[91] Comisión de Venecia, "Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies" (marzo de 2015), disponible en: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

[92] Ver Szabó y Vissy v. Hungary, App. No. 37138/14, Tribunal Europeo de Derechos Humanos, Fallo, párr. 78, 12 de enero de 2016.

A. Estado de las solicitudes de acceso a la información pública

En nuestro intento de asegurar la publicación de información relacionada con la cooperación de inteligencia, diez miembros de INCLO presentaron solicitudes coordinadas de acceso a la información pública a los organismos nacionales pertinentes de los países miembros participantes. Pedimos[93]:

- Todos los acuerdos, memorandos de entendimiento y/u otros arreglos con países extranjeros concernientes al intercambio de datos de vigilancia de inteligencia extranjera entre el país miembro de INCLO y cualquier otro país, o institución internacional;

- Todas las políticas, directrices, opiniones, informes y memorandos relativos a:
  - Las circunstancias en las que la agencia de un país miembro de INCLO puede compartir datos de vigilancia extranjera con otro país.
  - Cualquier limitación en el intercambio internacional de datos de vigilancia con otros países.
  - Las circunstancias en las que el país miembro puede solicitar o adquirir de otro país datos de vigilancia electrónica.
  - Cualquier limitación a la adquisición (ya sea por solicitud o de otro tipo) de datos de vigilancia electrónica de otro país.
  - Cualquier limitación a la retención, uso o difusión de datos de vigilancia electrónica solicitados o adquiridos de otro país miembro de INCLO, incluido el uso de tales datos o de datos derivados de estos en procedimientos civiles, penales, administrativos o de otro tipo.
  - Las circunstancias –si las hay– bajo las que el país miembro de INCLO puede solicitar o adquirir datos de vigilancia electrónica de otro país.

A pesar de que INCLO inició estas solicitudes hace ya más de un año[94], muchas han sido rechazadas de plano sobre la base de exenciones legales, mientras que, en otros casos, se piden largos plazos para responder. Luego de este ejercicio de solicitudes de acceso a la información pública, INCLO concluye que, en general, todavía sabemos muy poco sobre la cooperación de inteligencia internacional en nuestros países miembros.

[93] Para una lista completa de las solicitudes FOI enviadas por las organizaciones miembros de INCLO véase el Apéndice. Véanse también nuestras solicitudes y respuestas publicadas en https://www.inclo.net/international-intelligence-sharing-project.html. No pudimos publicar todos los esfuerzos de acceso a la información debido a los riesgos que podrían suponer para las organizaciones.
[94] Las primeras solicitudes se enviaron en junio de 2017. Véase Apéndice.

Argentina

El CELS y otros miembros locales de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI) presentaron una solicitud de acceso a la información pública[95] a la Agencia Federal de Inteligencia. La respuesta de la Agencia[96] simplemente indicó que la información solicitada estaba clasificada y que esa respuesta era clasificada también. La ICCSI llevó esa decisión a la corte. El juez primero respondió que ICCSI debía presentar la solicitud de nuevo, esta vez bajo la nueva Ley de Acceso a la Información, que había entrado en vigor inmediatamente después de que se presentara la primera solicitud. Por lo tanto el CELS, junto con sus socios de ICCSI, presentó nuevamente la solicitud de acceso a la información. Pero la respuesta de la Agencia fue exactamente la misma que la primera vez. ICCSI volvió a llevar el caso a la Justicia. Sin embargo, más de siete meses después, debido a procesos judiciales deficientes, complejos e ineficaces, la Agencia Federal de Inteligencia aún no ha sido notificada de la existencia de ese litigio. Casos como este demuestran procesos problemáticos tanto en el Poder Ejecutivo (Agencia Federal de Inteligencia) como en el Poder Judicial, que se vuelven aún más complicados cuando se trata de asuntos de seguridad del Estado.

Canadá

En Canadá, existen excepciones obligatorias para la información recibida confidencialmente de parte de un gobierno extranjero[97]. En respuesta a la solicitud de acceso a la información pública presentada por la CCLA[98], el CSIS entregó algunos documentos[99] en un breve plazo, mientras que la CSE indicó que requeriría una extensión de 210 días para considerar la solicitud. Se ha brindado alguna información limitada en respuesta a la solicitud, incluyendo alguna divulgación sobre salvedades y garantías que debe incluirse a la información compartida con socios extranjeros. Sin embargo, debido a las exenciones obligatorias, todo el material relacionado con acuerdos específicos con otros países ha sido rechazado.

Colombia

Dejusticia envió una solicitud de acceso a la información a la Junta de Inteligencia Conjunta de Colombia (JIC)[100]. La JIC transfirió el tema a la Jefatura de Inteligencia y Contrainteligencia Militar Conjunta [101]. El Jefe Conjunto respondió[102] que, de acuerdo con los protocolos, la seguridad y la legislación vigente, la información solo se puede divulgar a destinatarios autorizados. Dejusticia repuso esta decisión sobre la base de que la negativa viola su derecho de petición de acceso a la

[95] Presentada por primera vez el 13 de junio de 2017 ante el Director General de la Agencia Federal de Inteligencia de Argentina (AFI), y presentada de nuevo el 4 de diciembre de 2017 debido a cambios en la legislación que requerían una nueva presentación. Véase Apéndice I.
[96] Enviado por el Director General de la Agencia Federal de Inteligencia el 23 de agosto de 2017, véase Apéndice I.
[97] Ley de Acceso a la Información s.13
[98] Presentada el 13 de junio de 2017 a CSE y CSIS, véase Apéndice II.
[99] Enviada por el CSIS el 13 de junio de 2017, véase Apéndice II.
[100] Presentada el 18 de octubre de 2017, véase Apéndice III.
[101] Presentada por la Oficina de Asuntos Jurídicos del Ministerio de Defensa Nacional de Colombia el 27 de octubre de 2017, véase Apéndice III.
[102] Presentada por el Despacho de Inteligencia y Contrainteligencia Militar Conjunta el 16 de noviembre de 2017, véase Apéndice III.

información pública[103]. Argumentaron que se debería realizar una evaluación de proporcionalidad y que al menos la existencia (en oposición al contenido) de cualquier acuerdo debería hacerse pública. Dejusticia se encuentra a la espera de la revisión del caso por parte de un juez administrativo.

Egipto

Problemas de las solicitudes de información en Egipto

Egipto no presentó una solicitud de acceso a la información pública en este proyecto. Es más probable que cualquier solicitud de información que emprendamos para ayudar a nuestro trabajo en Egipto se realice fuera de Egipto y, por lo tanto, es necesario trabajar estrechamente con otras partes. Una ley de acceso a la información podría cambiar esta situación y hay un proyecto en desarrollo. Esto supone una oportunidad para reflexionar seriamente acerca de cómo diseñar solicitudes legales para acceder a información gubernamental. El gobierno egipcio es una caja negra en lo que respecta a los procesos de intercambio de inteligencia, por lo que no tenemos idea de cómo se desarrollarían las solicitudes de información en la práctica. ¿Cuáles serán los costos? ¿Cómo será la fase de transición y con qué habrá que tener cuidado? Soy el mayor experto de solicitudes de acceso a la información pública en mi país y no sabría por dónde comenzar a presentar una solicitud si tuviera que hacerlo. Seguramente alguien estuvo en mi misma situación en los EE.UU. de fines de la década de 1960 o en Suecia antes de 1776.

- Amr Gharbeia, Egyptian Initiative for Personal Rights.

Hungría

En Hungría, la solicitud de acceso a la información pública presentada por el HCLU fue rechazada por los ministros responsables y también por el Comité de Seguridad Nacional del Parlamento. A pesar de que la legislación hace referencia al intercambio de inteligencia, solicitudes de información adicional y de documentos específicos que describieran las políticas detrás de los acuerdos fueron rechazadas debido a que nadie tenía la información solicitada.

[103] Presentada el 21 de noviembre de 2017, véase Apéndice III.

Irlanda

> Por razones de seguridad, los funcionarios no comentan públicamente los detalles de los acuerdos detrás de la lucha contra el terrorismo. Cabe señalar que, debido a nuestra historia específica, lamentablemente hemos estado involucrados en la lucha contra el terrorismo durante décadas y los acuerdos actualmente en vigor han servido al pueblo irlandés para contrarrestar las amenazas a la seguridad del Estado. Las Fuerzas de Defensa y la Garda tienen un largo y orgulloso historial protegiendo y defendiendo al Estado de una sostenida amenaza terrorista durante muchos años.
>
> - Charlie Flanagan, secretario privado del ministro de Justicia e Igualdad[104]

En Irlanda, el ICCL solicitó información a la Garda Síochána (la policía de Irlanda), el Departamento de Defensa y el Departamento de Justicia e Igualdad[105]. La Garda Síochána rechazó la solicitud argumentando que están sujetos a la Ley de acceso a la información solo en relación con "registros administrativos relacionados con recursos humanos, finanzas o asuntos de adquisiciones[106]". El Departamento de Defensa también se negó diciendo que "la información solicitada no puede ser divulgada por razones de seguridad" [107]. El Departamento de Justicia e Igualdad respondió que hicieron una búsqueda exhaustiva de la solicitud y que la búsqueda resultó en "un registro identificado en el alcance de su solicitud", pero su publicación fue rechazada porque "refiere a asuntos que puedan perjudicar o menoscabar la prevención, detección o investigación de delitos" y también porque ese documento "es un instrumento confidencial e internacional para la aplicación de la ley y su divulgación afectaría negativamente la seguridad del Estado y las relaciones internacionales del Estado[108]."

India

En la India, en virtud de la Ley de Derecho a la Información de 2005 no existe la obligación de dar información a los ciudadanos que se considere perjudicial para la soberanía e integridad del país, los intereses de seguridad, estratégicos, científicos o económicos del Estado, incluyendo sus relaciones con un Estado extranjero, o que puedan conducir a la incitación de un delito.

[104] Respuesta del Departamento de Justica e Igualdad al Dr Hosein, Dr McIntyre, y Liam Herrick de parte de Privacy International fechada el 4 de abril de 2018. Véase Apéndice V.
[105] Enviada el 13 de junio de 2017 a la *Garda Síochána,* Departamento de Defensa y Departamento de Justicia e Igualdad. Véase Apéndice V.
[106] Enviada por la *Garda Síochána* el 23 de junio de 2017, véase Apéndice V.
[107] Enviada por el Departamento de Defensa el 20 de junio de 2017, véase Apéndice V.
[108] Enviada por el Departamento de Justicia e Igualdad el 14 de junio de 2017, véase Apéndice V.

Israel

> Cuando las reglas que rigen el intercambio de información entre agencias de inteligencia tienen lugar entre muros secretos que están protegidos por una excepción legal, se restringe gravemente la transparencia de la democracia".
>
> - Avner Pinchuk, Association for Civil Rights in Israel (ACRI)

En Israel, la ACRI no presentó solicitudes de acceso a la información pública porque el Servicio de Seguridad General (GSS) y la Unidad de Inteligencia Militar 8200 están exentos de responder a las solicitudes de información bajo la Ley de Libertad de Información israelí. Mientras que el Primer Ministro está sujeto a las Solicitudes de Libertad de Información, la exención de la que goza el GSS significa que incluso una información tan general como el número de permisos de escuchas telefónicas que el Primer Ministro aprueba cada año permanece clasificado. Cuando el Primer Ministro fue presionado directamente sobre la cuestión de las escuchas telefónicas, insistió en que la información no estaba en su posesión "física", ya que remite todas las solicitudes y aprobaciones de escuchas telefónicas al GSS. Este argumento fue aceptado por la Corte Suprema después de que la ACRI presentara una petición para acceder a esa información[109].

Kenia

En Kenia, el KHRC no presentó solicitudes de acceso a la información pública debido a las limitaciones del estatuto. La Ley de Acceso a la Información de 2016 y sus Restricciones en Relación con la Seguridad Nacional se promulgaron para que, entre otras cosas, "proveyeran un marco para que las entidades públicas y privadas divulguen proactivamente la información que posean y brinden información previa solicitud de acuerdo con la principios constitucionales".

Si bien sus límites aún no se han puesto a prueba judicialmente, la sección 6(1)(a) de esta Ley limita el derecho a la información si se considera que su divulgación socava la seguridad nacional de Kenia. Según s6(2), la información relacionada con la seguridad nacional incluye, entre otras cosas, información de gobiernos extranjeros con implicaciones para la seguridad nacional, actividades de inteligencia, fuentes, capacidades, métodos o códigos y relaciones exteriores.

Rusia

En Rusia, Agora presentó una solicitud de acceso a la información pública al Ministerio de Asuntos Exteriores, al FSB y al Ministerio del Interior[110]. El Ministerio de Asuntos Exteriores denegó la solicitud sobre la base de acuerdos multilaterales y bilaterales sobre el intercambio de información y

[109] En 2014, la ACRI presentó una FOI al tribunal de distrito en busca de una orden que obligaría a la Oficina del Primer Ministro (PMO) a proporcionar el número de órdenes emitidas por el primer ministro para ejecutar escuchas telefónicas de seguridad en los últimos cinco años, incluido el número de personas, y el número de ciudadanos y residentes israelíes, cubiertos por dichas órdenes. El tribunal de distrito desestimó la petición. La ACRI apeló a la Corte Suprema pero perdió. Véase ACRI vs. La Oficina del Primer Ministro, resolución APA 4349/14 (3 de noviembre de 2015) disponible (en hebreo) en: https://supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts\14\490\043\g08&fileName=14043490_g08.txt&type=2; véase también ACRI, "Court Denies ACRI's FoI Petition on Secret Security Wiretaps" (20 de mayo de 2014), disponible en: https://www.acri.org.il/en/2014/05/20/foi-wiretaps-2/

[110] Véase Apéndice VI.

la "lucha contra la delincuencia en el ámbito de la informática" [111]. El Ministro recomendó la remisión de la solicitud a los órganos estatales competentes, incluido el FSB, al que Agora ya había recurrido.

La respuesta del FSB fue muy similar, y también recomendó dirigir la solicitud de acceso a la información pública a otros cuerpos estatales, ¡incluyendo el FSB!

El Ministerio del Interior justificó la colaboración secreta entre la Federación Rusa y otros Estados a fin de revelar actividades ilegales de personas sospechosas y permitir que los organismos encargados de hacer cumplir la ley "tomen decisiones de procedimiento". Afirmó que compartir información transfronteriza sobre proveedores de servicios o usuarios está justificado cuando los perpetradores usan Internet para cometer delitos. Esa respuesta indicó que, en Rusia, las direcciones IP no entran dentro de la categoría de "datos personales" protegidos.

Sudáfrica

En Sudáfrica, el LRC envió una solicitud de acceso a la información al Departamento de Justicia y Desarrollo Constitucional y a la Agencia de Seguridad Estatal (SSA) [112]. El Departamento de Justicia y Desarrollo Constitucional respondió[113] que la solicitud había sido transferida al Departamento de Relaciones Internacionales y Cooperación ya que "el tema de la consulta está más estrechamente relacionado con las funciones del Departamento de Relaciones Internacionales y Cooperación". Más tarde el Departamento de Relaciones Internacionales y Cooperación[114] notificó al LRC que la solicitud había sido debidamente considerada y se había decidido transferirla a la SSA ya que el tema de la solicitud estaba más estrechamente relacionado con las funciones de ese Departamento. La SSA solo acusó recibo de la solicitud inicial de acceso a la información y no respondió a la transferencia del Departamento de Relaciones Internacionales y Cooperación ni a la correspondencia adicional del LRC. La legislación sudafricana respecto de las solicitudes de información establece que existe una presunta denegación cuando no se recibe respuesta dentro de los 30 días posteriores a la presentación de la solicitud. El período de 30 días expiró en términos tanto de la solicitud inicial como de la solicitud transferida, lo que llevó al LRC a presentar una apelación interna contra la presunta denegación[115]. Esta apelación también fue ignorada por la SSA.

Dado que existe una clara exención de seguridad nacional a las solicitudes de acceso a la información pública en la Ley de Promoción del Acceso a la Información de Sudáfrica, las perspectivas de éxito en el litigio son mínimas. El LRC decidió entonces buscar apoyo de órganos de

[111] La respuesta cita como fuente el sitio web del ministerio: www.mid.ru. Existen acuerdos multilaterales entre Rusia y los países pertenecientes a la Organización de Cooperación de Shanghai y la Comunidad de Estados Independientes. Los acuerdos bilaterales destacados mencionan a Brasil, Bielorrusia, Cuba, China e India. Para el segundo punto de la solicitud FOI, el ministerio recomienda recurrir a "los organismos estatales competentes", principalmente al "Ministerio del Interior, la Fiscalía General y el Servicio Federal de Seguridad de Rusia".

[112] Enviada el 13 de junio de 2017, véase Apéndice VII.

[113] Enviada por el Departamento de Justicia y Desarrollo Constitucional el 15 de junio de 2017, véase Apéndice VII.

[114] Enviada por el Departamento de Relaciones Internacionales y Cooperación el 3 de agosto de 2017, véase Apéndice VII.

[115] Enviada el 4 de diciembre de 2017, véase Apéndice VII.

control que tienen algún tipo de mandato sobre los servicios de inteligencia o el acceso a la información. Así, se establecieron reuniones con el Comité Permanente Conjunto sobre Inteligencia[120], IGI[121] y el Regulador de Información de Sudáfrica[122].

El inspector general de Inteligencia vs. la Agencia de Seguridad del Estado

En Sudáfrica, cuando el Centro de Recursos Legales (LRC) no tuvo éxito con las primeras solicitudes de acceso a la información pública, envió una serie de mensajes al IGI, al Regulador de Información de Sudáfrica y al Comité Permanente Conjunto sobre Inteligencia pidiendo reuniones para discutir su rol en el control del intercambio de inteligencia.

Posteriormente, el LRC se reunió con el Presidente del IGI, Dr. Setlhomamaru Dintwe[116], para expresar su preocupación respecto del intercambio internacional de inteligencia y discutir las insuficiencias en el control estatal, y para expresar su preocupación por la falta de control efectivo de la vigilancia secreta[117].

Durante la reunión del 28 de febrero de 2018, el Dr. Dintwe confirmó que el IGI era el órgano de control encargado de investigar las denuncias de presuntos abusos o ilícitos dentro de la SSA. Después de la reunión, el Dr. Dintwe expresó su frustración por la falta de independencia institucional de su oficina y pidió al LRC que considerara cuestionar la Ley de supervisión de Inteligencia. El Dr. Dintwe citó preocupaciones tales como el hecho de que el presupuesto del IGI surge de una partida presupuestaria de la SSA, lo que significaba que tenía que solicitar fondos del Director General de la SSA y rendirle los gastos.

El 11 de abril de 2018, el IGI presentó una solicitud urgente para evitar que el Director General de la SSA revocara sus autorizaciones o frustrara de alguna otra manera una investigación sobre presunto abuso de poder por parte del Director General de la SSA, Arthur Fraser[118]. La Parte B de esa solicitud buscaba impugnar varias disposiciones de la Ley de Supervisión de Inteligencia que ponían en peligro la independencia institucional del IGI, como se indicó anteriormente. Sin embargo, el 17 de abril Arthur Fraser fue trasladado al Departamento de Servicios Correccionales, ya que su Director General y el ministro de Seguridad del Estado revocaron la decisión de Fraser de retirar las autorizaciones del Dr. Dintwe[119]. Esto socavó la urgencia de la solicitud, si bien permanece en los tribunales. El LRC ha expresado su intención de intervenir como amicus curiae para apoyar al IGI en su argumento a favor de una mayor independencia institucional, poniendo énfasis en la necesidad de independencia presupuestaria, la libertad de nombrar su propio personal (el personal de IGI se encuentra actualmente en el organigrama de SSA) y la necesidad de rendir cuentas ante el Parlamento y no ante el Poder Ejecutivo.

[116] El LRC también se aseguró una reunión con el Presidente del Comité Permanente Conjunto sobre Inteligencia, pero se pospuso el día debido a la renuncia del presidente Zuma. Los esfuerzos para reprogramar el encuentro continúan.
[117] Carta del LRC al IGI fechada 13 de diciembre de 2017, véase Apéndice VII.
[118] Solicitud de medidas provisionales ante el Tribunal Superior de Sudáfrica, División de Gauteng, Pretoria, del Inspector General de Inteligencia contra el ministro de Seguridad del Estado, el Director General de Seguridad del Estado, el ministro de Finanzas, el Comité Permanente Conjunto de Inteligencia y el presidente de la República de Sudáfrica, caso nro. 25/21/18.
[119] Disponible en: https://www.enca.com/south-africa/inspector-general-of-intelligences-security-clearance-reinstated
[120] Carta enviada el 13 de diciembre de 2017, véase Apéndice VII.
[121] Ibíd.
[122] Ibíd.

Reino Unido

En el Reino Unido, la solicitud de acceso a la información pública de Liberty al GCHQ[123] fue rechazado ya que el GCHQ goza de una excepción absoluta en la legislación de Libertad de Información. En una carta explicando la negativa[124], el GCHQ afirmó que "los estados extranjeros pueden elegir tener relaciones de intercambio de inteligencia con el Reino Unido bajo la estricta comprensión de que esas relaciones se mantendrán confidenciales" y, sobre esa base, es "obviamente imposible, y nunca podría ser posible" brindar la información solicitada. Sin embargo, la respuesta también indicó que el GCHQ "está trabajando actualmente con varios de nuestros socios internacionales para establecer si se puede poner más información sobre la cooperación de inteligencia en dominio público, incluido el intercambio de datos sin procesar y otra información, de una manera que no dañe el interés público" [125].

Estados Unidos

En los Estados Unidos, la ACLU presentó solicitudes de acceso a la información pública a la NSA, la CIA, la Oficina del Director de Inteligencia Nacional (ODNI), la Oficina Federal de Investigaciones (FBI) y el Departamento de Defensa[126]. El Departamento de Defensa respondió que realizaron una búsqueda en la Oficina del Subsecretario de Defensa–Inteligencia y que "no encontraron registros que respondieran" a la solicitud. La Oficina informó que debido a que la solicitud parecía referirse específicamente a Inteligencia Nacional y no tiene relación con la inteligencia militar, la solicitud debía ser dirigida a la ODNI.

La ODNI[127] y la CIA[128] rechazaron la solicitud de procesamiento expedito, argumentando que manejan todas las solicitudes en el orden en que las reciben[129]. La NSA también denegó la solicitud de tramitación expedita declarando "si bien puede haber cierto interés público con respecto al tema ('acuerdos con otros países sobre el intercambio de datos de vigilancia de inteligencia extranjera entre los Estados Unidos y cualquier otro país'), el valor de la información no se perderá si no se difunde rápidamente[130]." También declararon que "debido a los aumentos significativos en el número de solicitudes recibidas por esta Agencia, estamos experimentando retrasos en el procesamiento. Le proporcionaremos una respuesta más sustantiva tan pronto como podamos". El FBI denegó una solicitud de procesamiento expedito indicando que la ACLU no había brindado "suficiente información sobre los requisitos legales para dicha expedición[131]."

---

[123] Enviada el 19 de mayo de 2017, véase Apéndice VIII.
[124] Enviada por el GCHQ el 13 de noviembre de 2017, véase Apéndice VIII.
[125] Privacy International ha cuestionado esta excepción absoluta de divulgación ante el Tribunal Europeo de Derechos Humanos. Ver "Privacy International v. United Kingdom (UK Five Eyes FOIA)", disponible en: https://www.privacyinternational.org/node/1764
[126] Presentadas el 13 de junio de 2017 a la NSA, la CIA, la ODNI, el FBI y el Departamento de Defensa. Véase Apéndice IX.
[127] Respuesta de la ODNI, 23 de junio de 2017, véase Apéndice IX.
[128] Respuesta de la CIA, 21 de junio de 2017, véase Apéndice IX.
[129] Las excepciones a esta regla solo tienen lugar cuando un solicitante alega una necesidad imperiosa según los estándares de las reglamentaciones. Existe una "necesidad apremiante" cuando 1) el asunto comporta una amenaza inminente a la vida o la seguridad física de un individuo, o 2) una persona que se dedica principalmente a difundir información realiza la solicitud, y dicha información es relevante para un asunto de urgencia pública sobre una actividad real o presunta del gobierno federal.
[130] Enviada por la NSA el 27 de junio de 2017, véase Apéndice IX.
[131] Respuesta del FBI, 29 de junio de 2017, véase Apéndice IX.

Recomendación III de INCLO: transparencia

Cinco años después de la publicación de documentos por parte de Edward Snowden, no deberíamos depender de filtraciones de información para determinar el estado de los acuerdos de inteligencia. A INCLO le preocupa profundamente que esos acuerdos continúen fuera del alcance de las normas y de la supervisión del gobierno y el escrutinio público. Al mantener esos acuerdos en secreto, los gobiernos han eliminado la capacidad de los ciudadanos de cuestionar acciones de las que son responsables y que amenazan nuestros derechos humanos, nuestras democracias y el Estado de derecho.

Por lo tanto, INCLO sostiene que se necesitan acuerdos públicos fuertes y transparentes para promover la rendición de cuentas y evitar que las agencias de inteligencia utilicen sus alianzas internacionales para eludir el Estado de derecho. Apoyamos las conclusiones de los Principios Globales sobre Seguridad Nacional y el Derecho a la Información respecto de que los acuerdos bilaterales y multilaterales y otros compromisos internacionales importantes del Estado en materia de inteligencia son una categoría de información con una fuerte presunción o un interés preponderante en favor de su divulgación[132]. Otros requisitos mínimos son la publicación de informes periódicos sobre las actividades de las agencias involucradas en acuerdos de intercambio de inteligencia en relación con las normas y políticas generales que rigen su comportamiento; la divulgación de la existencia y los términos de los acuerdos bilaterales y multilaterales y otros compromisos internacionales importantes por parte del Estado en materia de inteligencia; y el mantenimiento de registros de toda la información divulgada y recibida por una agencia de inteligencia extranjera.

Conclusión

A pesar del escándalo que ocasionaron las revelaciones de Snowden sobre vastas y secretas redes de vigilancia en todo el planeta, todavía no hay acuerdos públicos que rijan el intercambio de inteligencia en ninguna parte del mundo. Hoy, los únicos acuerdos públicos son artefactos históricos[133] o aquellos que han sido filtrados por informantes. INCLO se ha embarcado en la ambiciosa tarea de acceder a esa información en un intento por aprender más y exigir una mejor protección de nuestros derechos y libertades fundamentales.

Se trata de una tarea de importancia constante. El alcance y la escala del intercambio y la cooperación de inteligencia está en pleno crecimiento, sin incrementos correspondientes en las reglamentaciones, supervisiones o transparencia. Sin embargo, estos controles y equilibrios deben aplicarse a un área sumamente opaca. Los gobiernos deben regular mejor el intercambio internacional de inteligencia a fin de garantizar un adecuado control, revisión y acceso a la información para que las agencias de inteligencia rindan cuentas.

[132] Véase el principio 10 de los Principios Globales sobre Seguridad Nacional y el Derecho a la Información (12 de junio de 2013), disponible en: https://www.opensocietyfoundations.org/sites/default/files/tshwane-espanol-10302014%20%281%29.pdf

[133] Disponible en: https://www.nationalarchives.gov.uk/ukusa/

Con este fin, INCLO insta a todos los Estados a actuar y someter el intercambio de inteligencia al Estado de derecho, de modo que los ciudadanos de todas las naciones estén protegidos contra la vigilancia injustificada. Hasta tanto no se sigan estrictamente las recomendaciones generales de INCLO, la capacidad de las agencias de inteligencia de utilizar sus alianzas internacionales será una amenaza constante para la democracia y el Estado de derecho.

Acrónimos y terminología

ACLU - American Civil Liberties Union (Unión Americana de Libertades Civiles)
ACRI - Association for Civil Rights in Israel (Asociación para los Derechos Civiles de Israel)
AFI - Agencia Federal de Inteligencia de la Argentina
AGORA - Agora International Human Rights Group (Grupo Internacional de Derechos Humanos Agora)
CCLA - Canadian Civil liberties Association (Asociación Canadiense de Libertades Civiles)
CEDH – Convenio Europeo de Derechos Humanos
CELS - Centro de Estudios Legales y Sociales
CIA - US Central Intelligence Agency (Agencia Central de Inteligencia de los Estados Unidos)
CSE - Canadian Communications Security Establishment (Agencia de Seguridad en las Comunicaciones de Canadá)
CSIS - Canadian Security Intelligence Service (Servicio de Inteligencia y Seguridad de Canadá)
CSS - US Central Security Service (Servicio Central de Seguridad de los Estados Unidos)
CTIVD - Dutch Review Committee on the Intelligence and Security Services
DGSE - French General Directorate for External Security
DISS - Dutch Defence Intelligence and Security Service (Comité de Revisión de los Servicios de Inteligencia y Seguridad de los Países Bajos)
DNI – Dirección Nacional de Inteligencia de Colombia
ECHR - European Convention on Human Rights (Convenio Europeo de Derechos Humanos)
ECtHR - European Court of Human Rights (Tribunal Europeo de Derechos Humanos)
EIPR - Egyptian Initiative for Personal Rights (Iniciativa Egipcia por los Derechos Personales)
EO 12333 - Orden Ejecutiva 12333 de los Estados Unidos
FBI - US Federal Bureau Investigation (Buró Federal de Investigaciones de los Estados Unidos)
Five Eyes - Cinco Ojos, una asociación de inteligencia entre los EE.UU., el Reino Unido, Australia, Canadá y Nueva Zelanda
FSB – Servicio Federal de Seguridad de Rusia
G2 - Fuerzas de Defensa de Irlanda
GCHQ - UK Government Communications Headquarters (Cuartel General de Comunicaciones del Gobierno de Reino Unido)
GCSB - New Zealand Government Communications Security Bureau (Buró de Seguridad de Comunicaciones del Gobierno de Nueva Zelanda)
GISS – General Intelligence and Security Service (Servicio General de Seguridad e Inteligencia de Holanda)
GSS - Israeli General Security Service (Servicio de Seguridad General de Israel)
HCLU - Hungarian Civil Liberties Union (Unión Húngara de Libertades Civiles)
HRLN - Human Rights Law Network (Red de Derechos Humanos, India)

ICCL - Irish Council for Civil liberties (Consejo irlandés para las Libertades Civiles)
ICCSI- Iniciativa Ciudadana para el Control del Sistema de Inteligencia, Argentina
IGI - South African Inspector General of Intelligence (Inspector General de Inteligencia)
INCLO - International Network of Civil Liberties Organizations (Red Internacional de Organizaciones por los Derechos Civiles)
IPT - Investigatory Powers Tribunal (Tribunal Investigador de Poderes)
ISNU - Israeli SIGINT National Unit (Unidad Nacional SIGINT de Israel)
JIC - Junta de Inteligencia Conjunta de Colombia
JIC - Indian Joint Intelligence Committee (Comité Conjunto de Inteligencia de la India)
KHRC - Kenya Human Rights Commission (Comisión Keniana de Derechos Humanos)
LRC - Legal Resource Centre (Centro de Recursos Legales, Sudáfrica)
MOU – Memorando de entendimiento
NSA - US National Security Agency (Agencia de Seguridad Nacional de los Estados Unidos)
ODNI - US Office of the Director of National Intelligence (Oficina del Director de Inteligencia Nacional de los Estados Unidos)
PRISM - Programa utilizado por la NSA para interceptar el tráfico de comunicaciones en Internet.
SIGINT - Inteligencia de señales derivada de señales electrónicas y sistemas utilizados por objetivos extranjeros
SIRC - Canadian Security Intelligence Review Committee (Comité de Revisión de Inteligencia de Seguridad de Canadá)
SSA - South African State Security Service (Agencia de Seguridad del Estado de Sudáfrica)
Third Party Rule – Regla de la información suministrada por terceros. Un requisito común en los acuerdos de intercambio de inteligencia es que el material compartido en virtud del acuerdo no se pueda compartir con ningún tercero.
Upstream - Programa utilizado por la NSA para interceptar el tráfico de comunicaciones de Internet.

APÉNDICE: solicitudes, respuestas y materiales relacionados

I. Argentina

- Solicitud del CELS al Director General de la AFI, fechada el 13 de junio, 2017.
- Respuesta del director de la AFI al CELS, fechada el 28 de agosto, 2017.
- Solicitud del CELS al Director General de la Agencia Federal de Inteligencia recibida el 4 de diciembre, 2017.
- Respuesta del Director General de la AFI al CELS fechada el 27 de diciembre, 2017.

II. Canadá

- Solicitud de la Asociación Canadiense de Libertades Civiles (CCLA) al CSIS, fechada el 13 de junio, 2017.
- Solicitud de la Asociación Canadiense de Libertades Civiles (CCLA) al CSIS, fechada el 13 de junio, 2017.
- Respuesta del CSIS a la CCLA, fechada el 25 de octubre, 2017 con información acompañante.

III. Colombia

- Solicitud de Dejusticia al Presidente, Junta de Inteligencia Conjunta, fechada el 18 de octubre, 2017.
- Respuesta del Despacho de la Junta de Inteligencia Conjunta al Jefe de la Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, fechada el 15 de octubre, 2017.
- Respuesta del Jefe de la Jefatura de Inteligencia y Contrainteligencia Militar Conjunta a Dejusticia, fechada el 16 de noviembre, 2017.
- Apelación de Dejusticia al Presidente, Junta de Inteligencia Conjunta, fechada el 21 de noviembre, 2017.

IV. Hungría

- Solicitid de HCLU a presidente, Comité de Seguridad Nacional, fechada el 8 de junio de 2017.
- Solicitud de HCLU a la Oficina del Primer Ministro, fechada el 8 de junio de 2017.
- Solicitud de HCLU al ministro del Interior, fechada el 8 de junio de 2017.
- Respuesta del ministro del Interior a HCLU, fechada el 11 de junio de 2017.
- Respuesta del presidente, Comité de Seguridad Nacional a HCLU, fechada el 20 de junio de 2017.
- Respuesta de la Oficina del Primer Ministro a HCLU, fechada el 27 de junio de 2017.

V. Irlanda

- Solicitud del ICCL a An Garda Siochána, Departamento de Defensa y Departamento de Justicia e Igualdad, fechada el 13 de junio de 2017.
- Respuesta del Departamento de Justicia e Igualdad al ICCL fechada el 14 de junio de 2017.
- Respuesta del Departamento de Defensa al ICCL fechada el 19 de junio de 2017.
- Respuesta de la Garda Síochána al ICCL fechada el 20 de junio de 2017.
- Respuesta del Departamento de Justicia e Igualdad al Dr Hosein, Dr McIntyre y Liam Herrick de parte de Privacy International fechada el 4 de abril de 2018.

VI. Rusia

- Solicitud traducida del AGORA al Ministerio de Asuntos Exteriores de la Federación Rusa, Servicio Federal de Seguridad de la Federación Rusa, al Ministerio del Interior de la Federación de Rusia.
- Respuesta del Ministerio del Interior de la Federación Rusa a AGORA fechada el 20 de junio de 2017.
- Respuesta del Servicio Federal de Seguridad de la Federación Rusa a AGORA fechada el 28 de junio de 2017.
- Respuesta del Ministerio de Asuntos Exteriores a AGORA fechada el 11 de agosto de 2017.

VII. Sudáfrica

- Solicitud de LRC al Departamento de Justicia y Desarrollo Constitucional fechado el 13 de junio de 2017.
- Respuesta del Departamento de Relaciones Internacionales y Cooperación al LRC fechada el 3 de agosto de 2017.
- Acuse de recibo de la solicitud DE ACCESO A LA INFORMACIÓN de LRC de parte del Departamento de Justicia y Desarrollo Constitucional a LRC fechado el 15 de junio de 2017.
- Solicitud de LRC al presidente de IGI por una investigación sobre las acciones de vigilancia a Naidoo fechada el 15 de septiembre de 2017.
- Solicitud de LRC a presidente, Comité Permanente Conjunto de Inteligencia, fechada el 13 de diciembre de 2017.
- Solicitud de LRC a presidente, Regulador de Información de Sudáfrica, fechada el 13 de diciembre de 2017.
- Solicitud de LCR a IGI fechada el 13 de diciembre de 2017.
- Acuse de recibo del SSA a LRC fechado el 13 de junio de 2017.
- Correo electrónico de seguimiento de LCR a SSA fechado el 13 de octubre de 2017.
- Respuesta de LCR a SSA con respecto a la denegación presunta de la solicitud DE ACCESO A LA INFORMACIÓN fechada el 4 de diciembre de 2017.

VIII. Reino Unido

- Solicitud de Liberty al director de GCHQ, fechada el 19 de mayo de 2017.
- Respuesta del Jefe del equipo de legislación de información de GCHQ a Liberty, fechada el 13 de noviembre de 2017.

Estados Unidos

- Solicitud de la Unión Americana de Libertades Civiles (ACLU) al NSA, CIA, ODNI, FBI, Departamento de Defensa, fechada el 13 de junio, 2017.
- Respuesta del Departamento de Defensa a ACLU, fechada el 19 de junio, 2017.
- Respuesta de la CIA a ACLU, fechada el 21 de junio, 2017
- Respuesta de la Oficina del Director Nacional de Inteligencia a ACLU, fechada el 23 de junio, 2017.
- Respuesta de la NSA a ACLU, fechada el 27 de junio, 2017.
- Respuesta del FBI a ACLU, fechada el 28 de junio, 2017.
- Respuesta del FBI a ACLU, fechada el 29 de junio, 2017.
- Respuesta del Departamento de Defensa a ACLU, fechada el 16 de agosto, 2017.