pensar
Revista de Ciências Jurídicas
e-ISSN:2317-2150
DOI: 10.5020/2317-2150.2019.9528

"Big Brother Watch and Others v. The United Kingdom": el régimen de vigilancia social y el derecho al respecto a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos*

"Big Brother Watch and Others v. the United Kingdom": o regime de vigilância social e o direito ao respeito à vida privada e familiar e à liberdade de expressão frente à Corte Europeia de Direitos Humanos

"Big Brother Watch and Others v. The United Kingdom": the social surveillance regime and the right to respect for private and family life and to the freedom of expression under the European Court of Human Rights

João Pedro Seefeldt Pessoa**
Rafael Santos de Oliveira***

Resumen

A partir de las revelaciones de Edward Snowden en 2013, se hicieron públicos diversos detalles sobre programas de vigilancia global y de interceptación de comunicaciones personales, dirigidos por agencias estatales, principalmente de Estados Unidos y del Reino Unido. Los programas de espionaje plantearon problemas relacionados con la seguridad y la defensa nacional en contra de los derechos humanos, como la privacidad y la libertad de expresión. De esta manera, la investigación tiene por objetivo estudiar de qué modo la Corte Europea de Derechos Humanos firma posicionamiento sobre violaciones al derecho al respeto a la vida privada y familiar y a la libertad de expresión frente a la vigilancia social global, considerando el caso "Big Brother Watch and Others v. "The United Kingdom". Para ello, se utiliza el método de abordaje deductivo, aplicándose, como método de procedimiento, el monográfico, a partir de una investigación bibliográfica y documental. Al final, se constató que el TEDH, en esa decisión, entendió que la falta de supervisión en partes del procedimiento de interceptación y la ausencia de garantías reales y públicas al régimen de vigilancia viola el derecho a la privacidad y, tratándose de periodistas, vulnera también el derecho a la libertad de expresión.

Palabras-clave: Vigilancia social. Derecho al respecto a la vida privada y familiar. Derecho a la libertad de expresión. Corte Europea de Derechos Humanos.

Resumo

A partir das revelações de Edward Snowden em 2013, tornaram-se públicos diversos detalhes sobre programas de vigilância global e de interceptação de comunicações pessoais, dirigidos por agências estatais, principalmente dos Estados Unidos

* Pesquisa financiada pela Fundación Carolina, agência de fomento, mobilidade acadêmica e bolsas de estudos do governo da Espanha.

** Mestre em Direito pela Universidad de León, Espanha, pelo qual é bolsista da Fundação Carolina. Mestre em Direito pela Universidade Federal de Santa Maria (UFSM), pelo qual foi bolsista CAPES. Pesquisador do Centro de Estudos e Pesquisas em Direito e Internet da Universidade Federal de Santa Maria (CEPEDI), cadastrado na plataforma de pesquisas do CNPq. Atuação na linha de pesquisa "Riscos e (des)controles do ciberespaço". Integrante do projeto de pesquisa "Ativismo digital e as novas mídias: desafios e oportunidades da cidadania global". León - Espanha. E-mail: jpseefeldt@gmail.com. Orcid: https://orcid.org/0000-0003-1974-0247.

*** Doutor em Direito pela Universidade Federal de Santa Catarina (UFSC). Mestre em Integração Latino-Americana (Direito da Integração) pela Universidade Federal de Santa Maria (UFSM). Bacharel em Direito pela Universidade Federal de Santa Maria (UFSM). Professor Adjunto III no Departamento de Direito da Universidade Federal de Santa Maria (UFSM) e no Programa de Pós-graduação em Direito da UFSM (Mestrado). Atuação na linha de pesquisa "Riscos e (des)controles do ciberespaço". Integrante do projeto de pesquisa "Ativismo digital e as novas mídias: desafios e oportunidades da cidadania global". E-mail: advrso@gmail.com.em Direito pela Universidad de León, Espanha, pelo qual é bolsista da Fundação Carolina. Mestre em Direito pela Universidade Federal de Santa Maria (UFSM), pelo qual foi bolsista CAPES. Pesquisador do Centro de Estudos e Pesquisas em Direito e Internet da Universidade Federal de Santa Maria (CEPEDI), cadastrado na plataforma de pesquisas do CNPq. Atuação na linha de pesquisa "Riscos e (des)controles do ciberespaço". Integrante do projeto de pesquisa "Ativismo digital e as novas mídias: desafios e oportunidades da cidadania global". Santa Maria - RS - Brasil. E-mail: jpseefeldt@gmail.com. Orcid: https://orcid.org/0000-0003-1974-0247.

e do Reino Unido. Os programas de espionagem levantaram problemáticas relacionadas à segurança e defesa nacional em desfavor de direitos humanos, como à privacidade e à liberdade de expressão. Dessa maneira, a pesquisa tem por objetivo estudar de que modo a Corte Europeia de Direitos Humanos firma posicionamento sobre violações ao direito ao respeito à vida privada e familiar e à liberdade de expressão frente à vigilância social global, considerando o caso "Big Brother Watch and Others v. The United Kingdom". Para isso, utiliza-se o método de abordagem dedutivo, aplicando-se, como método de procedimento, o monográfico, a partir de uma pesquisa bibliográfica e documental. Ao fim, verificou-se que o TEDH, nessa decisão, entendeu que a falta de supervisão em partes do processo de interceptação e a ausência de garantias reais e públicas ao regime de vigilância viola o direito à privacidade e, tratando-se de jornalistas, vulnera também o direito à liberdade de expressão.

Palavras-chave: *Vigilância social. Direito ao respeito à vida privada e familiar. Direito à liberdade de expressão. Corte Europeia de Direitos Humanos.*

Abstract

From the Edward Snowden's revelation back in 2013, a number of details about global surveillance and interception of personal communications programs, run by state agencies, principally the United States and the United Kingdom, became public. Spy programs have raised issues related to national security and defense in the face of human rights, such as privacy and freedom of expression. The aim of the research is to study how the European Court of Human Rights has established a position on violations of the right to respect for private and family life and freedom of expression in the face of global social surveillance, taking into account the case "Big Brother Watch and Others v. The United Kingdom ". For this, the method of deductive approach is used, applying, as a method of procedure, the monographic, based on a bibliographical and documentary research. Finally, it was concluded that the ECHR, in that decision, found that the lack of supervision in parts of the interception process and the absence of real and public guarantees to the surveillance regime violate the right to privacy and, in the case of journalists, also violates the right to freedom of expression.

Keywords: *Social surveillance. Right to respect for private and family life. Right to freedom expression. European Court of Human Rights.*

1 Introducción

El desarrollo de las tecnologías de información y comunicación y la democratización del acceso a tales dispositivos por diferentes actores sociales revolucionó las posibilidades de ser en la sociedad de la información. Además, el flujo de personas internacionales, la delincuencia global y el avance de técnicas de criptografía hicieron surgir nuevos desafíos a la gubernamentalidad, especialmente en el combate a las amenazas extranjeras por parte de los Estados nacionales, lo que culminó en la creación de agencias secretas de seguridad y en el perfeccionamiento de regímenes de vigilancia social global para el control de la población.

En particular sobre el objeto del presente trabajo, se percibe en la actualidad que la excepcionalidad de un programa de vigilancia social global, mediante la interceptación de comunicaciones, la obtención de datos personales y el intercambio de información con otros países, exige una supervisión pública, ya que afecta derechos humanos comunitarios y constitucionalmente reconocidos en las democracias modernas. De esta manera, la presente investigación intenta examinar de qué modo la Corte Europea de Derechos Humanos firma posicionamiento sobre violaciones al derecho al respeto a la vida privada y familiar y a la libertad de expresión frente a la vigilancia social global, considerando el caso "Big Brother Watch and Others v. "The United Kingdom".

En términos de objetivos, la investigación se pretende revisar las revelaciones sobre el régimen de vigilancia social global dirigido por las agencias de seguridad estatales, especialmente denunciadas por Edward Snowden, y la relación existente con el derecho al respeto a la vida privada y familiar ya la libertad de expresión. Aún, se desea analizar el posicionamiento de la Corte Europea de Derechos Humanos en el caso "Big Brother Watch and Others v. "The United Kingdom", juzgado en 2018, y las implicaciones de esa sentencia sobre el derecho al respeto a la vida privada y familiar ya la libertad de expresión.

Para realizar la presente investigación, se utiliza el método de abordaje deductivo, una vez realizada una conexión descendente, estudiando por primero el régimen de vigilancia social y su implicación en los derechos humanos, para luego traer el caso "Big" Brother Watch and Others v. "The United Kingdom", juzgado en 2018. Como método de procedimiento o, aún, abordaje de segundo orden, se utiliza el monográfico para estudiar con profundidad la decisión referida, considerada como un caso clave por la propia Corte Europea. En relación a procedimientos y técnicas, se emplea el análisis bibliográfico y documental, a partir de fichas, resúmenes y manejo de decisión judicial.

2 "El Gran Hermano te vigila": la vigilancia social global y la interceptación de datos en el contexto de los derechos humanos

Durante la Segunda Guerra Mundial, gobiernos de diferentes países aliados, incluyendo el Reino Unido y Estados Unidos, han interceptado, leído y analizado varios mensajes intercambiados por los alemanes y japoneses militares, resultando en la creación, al final del conflicto, de una red planetaria de inteligencia de señales y escuchas, que se materializó en el Tratado de Seguridad de UK-USA, con la participación posterior de los Cinco Ojos, Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos, cuya existencia se reveló sólo a finales del siglo XX y se confirmó a principios del siglo XXI (GREENWALD, 2014; NORTON-TAYLOR, 2010, s.p.).

En ese sentido, durante el acuerdo de cooperación de inteligencia, comúnmente denominado UKUSA, y bajo la coordinación de la National Security Agency, con la sigla NSA, y de la General Communications Headquarters, con la sigla GCHQ, agencias de inteligencia estadounidense y británica, respectivamente, cuyas instituciones también se ha mantenido en secreto por varias décadas, se ha elaborado el sistema de vigilancia global "Echelon", con funciones de captar y analizar, virtualmente, informaciones provenientes de llamadas telefónicas y mensajes de fax, télex, correo electrónico y otros dispositivos, enviados de cualquier lugar del mundo (UNIÓN EUROPEA, 2001, s.p.). Se trata(ba) de una red de espionaje que, a través de estaciones de interceptación, es capaz de captar todo el tráfico de informaciones y comunicaciones ocurridas vía satélite, fibra óptica, frecuencia de radio, microondas, cables submarinos, internet y otras formas de procesamiento de datos, aunque cifradas.

Este programa de vigilancia, que luego adquirió escala de interceptación global, fue sido perfeccionado a lo largo del siglo XX, siendo que en la década de 40, el objetivo identificado era de espionaje militar y diplomático; en la década de los 60, tuvo como finalidad el espionaje comercial e industrial; y en la década de 1990 tuvo como objetivo el combate al crimen organizado, el lavado de dinero, el tráfico de drogas, armas y personas y, principalmente, al terrorismo (UNIÓN EUROPEA, 2001, s.p.). En el Informe del 11 de julio de 2001, el Parlamento Europeo, tras una investigación profunda, identificó que, a través del sistema Echelon, datos brutos de comunicación captados por las agencias de inteligencia, tanto de voz, télex, internet e internet, fueron y podían ser grabados, analizados, intercambiados, vendidos y clasificados por medio de filtros (UNIÓN EUROPEA, 2001, s.p.).

Posteriormente, en 2006, Julian Assange, periodista y ciberativista, fundó WikiLeaks, organización transnacional pro-transparencia, con el objetivo de publicar informaciones y datos confidenciales sensibles a la fuga o hackeados de gobiernos y otras instituciones para acceso abierto y difusión general, en especial para otras comunidades periodísticas, con la intención de viralizar el mensaje (WIKILEAKS, 2019, s.p.). En 2010, Chelsea Manning, en la época, Bradley Manning, entregó a WikiLeaks más de 700.000 (setecientos mil) archivos secretos, vídeos de enfrentamientos y comunicaciones diplomáticas del Departamento de Estado de Estados Unidos, revelando, entre otras cosas, la existencia de segmentos de inteligencia del gobierno (AYUSO; PEREDA, 2017, s.p.).

En el año 2013, Edward Snowden, analista de sistemas antes contratado por el gobierno estadounidense, desveló diversos detalles confidenciales sobre la existencia de la Agencia Nacional de Seguridad de Estados Unidos, así como sobre los programas integrantes del sistema de vigilancia global estadounidense (GREENWALD, 2014, s.p.). Para ello, Snowden viajó hasta Hong Kong en mayo de 2013, entregó los

documentos comprobatorios a los periodistas Glenn Greenwald y Laura Poitras, que más tarde se convirtieron en noticias por los portales The Guardian, The Washington Post y The Intercept, generando una incomodidad y vergüenza institucional global, ya que se ha revelado un gran régimen de interceptación de datos (GREENWALD, 2014, s.p.).

Con la revelación de documentos ultra secretos, se descubrieron otros programas de vigilancia global, en el marco del sistema Echelon o no. Por ejemplo, PRISM, de los Estados Unidos, Australia, Reino Unido y Países Bajos; XKeyscore, de los Estados Unidos, Alemania y Suecia; Proyecto 6, de Alemania y Estados Unidos; Stateroom, de los Cinco Ojos; Lustre, de los Estados Unidos y Francia; Optic Nerve, de los Estados Unidos y del Reino Unido; Turbina, de los Estados Unidos, Reino Unido y Japón; Operación Socialista del Reino Unido; Tempora, Muscular, Follow the Money, Marina, Dishfire, Mystic, estos todos de los Estados Unidos (PIRES, 2014, s.p.)

Se verificó que, además de agencias de seguridad e inteligencia de los países referidos, importantes universidades también estuvieron involucradas en el proyecto para el suministro de bases científicas, como por ejemplo, la Universidad de California, la Universidad de Stanford, el Instituto de Tecnología de Massachusetts (MIT), la Universidad de California Berkeley, Instituto de Tecnología de California *(Caltech)* y *Johns Hopkins University* (GREENWALD, 2014, s.p.). Por otro lado, documentos secretos revelan la participación y suministro de información por empresas y organizaciones de diferentes sectores económicos, como *Google, Facebook, Microsoft, Apple, Verizon, Vodafone, EDS, AT & T, Qwest, Motorola, Intel, IBM, Qualcomm, Cisco , HP, Oracle*, entre otras (GREENWALD, 2014, s.p.).

En cuanto a los Estados Unidos, la National Security Agency confirmó la existencia de dos programas, llamados PRISM y UPSTREAM. En síntesis, PRISM es un programa de inteligencia con el cual el gobierno americano obtiene material de inteligencia oriundo de los proveedores de servicios, de forma específica y direccionada, sin poseer amplia capacidad de *data mining* (UNION EUROPEA, 2018, s.p.). El gobierno, además, alega que el programa está regulado por la Foreign Intelligence Service Act (FISA) y que la solicitud del material depende de la aprobación por una corte compuesta por jueces (UNION EUROPEA, 2018, s.p.). Por otro lado, el UPSTREAM es un programa que permite la recolección de datos de comunicación a través de cables de fibra óptica e infraestructura de propiedad de los proveedores de servicio, con amplio acceso a los datos globales, incluso de ciudadanos no americanos (UNION EUROPEA, 2018, s.p.).

En cuanto al Reino Unido, se descubrió que el Gobierno Communications Headquarters operaba un programa llamado “Tempora”, que permitía acceder y almacenar grandes volúmenes de datos de portadores (UNION EUROPEA, 2018, s.p.). En esta línea, el procesamiento de datos, en apretado resumen, compara el tráfico de datos con una lista de selecciones y búsquedas predeterminadas respecto a un blanco en específico, pudiendo hacer una clasificación de la comunicación realizada con potencial valor investigativo para posterior análisis (UNION EUROPEA, 2018, s.p.). La agencia señala que el programa se basa en el *Investigatory Powers Act 2000* (RIPA), que permite que el Secretario de Estado emita órdenes de interceptación de comunicaciones externas (UNION EUROPEA, 2018, s.p.).

Conforme a documentos expuestos a partir de 2013, las agencias de seguridad pueden cruzar datos de teléfono, direcciones IP, mensajes intercambiados, redes sociales, cuentas bancarias e información del sistema de posicionamiento global (GPS), posibilitando la creación de innumerables tipos de perfiles un individuo y otros tantos tipos de relación, con el objetivo de identificar patrones comportamentales, relaciones sociales, políticas y religiosas y movimientos de los usuarios encuestados y de personas relacionadas a ellos (POITRAS; RISEN, 2013, s.p.).

La principal razón para la creación y/ o desarrollo y recrudecimiento de técnicas que permitan el monitoreo de informaciones y comunicaciones de la población ha sido la lucha contra el crimen, pero especialmente, al terrorismo, ya que, a partir de la interceptación de comunicaciones, es posible identificar sospechosos, prever ataques, bombardeos, disparos, explosiones, etc. Bajo el manto de una guerra al terror, los principales gobiernos del mundo unen esfuerzos para anticipar supuestas amenazas a la seguridad nacional y a la defensa nacional, aunque para tanto, comunicaciones entre millones de ciudadanos nacionales o extranjeros sean monitoreadas y calificadas (GREENWALD, 2014, s.p.). Principalmente, a partir de los

atentados terroristas sufridos por Estados Unidos en 2001, por España en 2004, por el Reino Unido en 2005, entre varias otras amenazas, el derecho a la intimidad, la intimidad y la libertad de expresión son, en parte, suplantados por cuestiones de seguridad nacional y de defensa nacional.

El derecho a la privacidad se reconoce expresamente en la Declaración Universal de Derechos Humanos, que en el artículo 12 define que "nadie sufrirá intromisiones arbitrarias en su vida privada, en su familia, en su domicilio o en su correspondencia, ni ataques a su honor y reputación", siendo que "contra tales intromisiones o ataques toda persona tiene derecho a protección de la ley" (ORGANIZACIÓN DE LAS NACIONES UNIDAS, 1948, s.p.). En el ordenamiento comunitario, el derecho a la intimidad, bajo el topónimo, de derecho al respeto a la vida privada y familiar, establecido en el Convenio Europeo de Derechos Humanos, declara, en el artículo 8, que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia", no pudiendo haber "injerencia de la autoridad pública en el ejercicio de este derecho sino cuando esta injerencia esté prevista en la ley y constituir una providencia que, en una sociedad democrática, sea necesaria", en las excepciones previstas en ley (UNIÓN EUROPEA, 1950, s.p.).

El derecho a la privacidad, "right to privacy", se remite al derecho de estar solo, o, aún, en otra dimensión, el derecho de ser dejado sólo o "right to be let alone", y el Estado no puede interferir indebidamente en la vida de cada individuo, siendo tal circunstancia, incluso, exigible del Estado para que él tutele ese derecho y no permita la injerencia también de terceros. Se trata del derecho de cada uno de asegurar una paz, una tranquilidad de parte de su vida, que no esté abarcada por una actividad pública, por ejemplo, o, incluso, de evitar con qué hechos de su vida que le son íntimos se divulguen (MENDES, 2015, p. 279-282).

Conviene mencionar, además, la diferenciación entre el derecho a la intimidad y el derecho a la privacidad. Esto, pues, el derecho a la intimidad puede ser considerado aquel que pretende garantizar a las personas de los sentidos de otros, pudiendo excluir del conocimiento de terceros todo aquello sobre sí; es, además, el derecho correspondiente al deber de los demás de no inmiscuirse en la intimidad ajena, rechazando cualquier incumplimiento (DONEDA, 2006). Así, la intimidad podría ser referente a informaciones del ámbito exclusivo, que alguien reserva para sí, ausente de cualquier repercusión social, incluso al alcance de la vida privada. Por otro lado, la privacidad, por más aislada que la persona intente vivir, se caracteriza por la convivencia con otros en una sociedad (por ejemplo, en lo que se refiere a la familia, al trabajo, a la recreación).

Por otro lado, el derecho a la libertad de expresión también se expresa en la Declaración Universal de los Derechos Humanos, que en el artículo 19 establece que "todo ser humano tiene derecho a la libertad de opinión y expresión; este derecho incluye la libertad de, sin interferencia, tener opiniones y de buscar, recibir y transmitir informaciones e ideas por cualquier medio e independientemente de fronteras" (ORGANIZACIÓN DE LAS NACIONES UNIDAS, 1948, s.p.). En el ámbito europeo, el derecho a la libertad de expresión, contemplado en el art. 10 del Convenio Europeo de Derechos Humanos, dice que "cualquier persona tiene derecho a la libertad de expresión" y que "este derecho comprende la libertad de opinión y la libertad de recibir o de transmitir informaciones o ideas sin que pueda haber injerencia de cualquier autoridad pública y sin consideraciones de fronteras (UNIÓN EUROPEA, 1950, s.p.).

Es importante señalar que ambos derechos a la privacidad y a la libertad de expresión tienen limitaciones ya definidas en el propio ordenamiento jurídico comunitario, lo que, por sí solo, constituye el fundamento de los programas de vigilancia social. Sobre el derecho al respeto a la vida privada y familiar, la Convención menciona que puede haber injerencia de autoridad pública en los casos de "seguridad nacional, para la seguridad pública, para el bienestar económico del país, la defensa del orden y la prevención infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y libertades de terceros"; y sobre el derecho a la libertad de expresión, el texto incluye las providencias necesarias para garantizar la "seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del crimen, [...] la protección de la salud o de la moral, la protección del honor o de los derechos de otro, para impedir la divulgación de informaciones confidenciales [...]" (UNIÓN EUROPEA, 1950, s.p.).

3 "Big Brother Watch and Others v. the United Kingdom": el derecho al respeto a la vida privada y familiar y a la libertad de expresión[1]

El caso "Big Brother Watch and Others v. The United Kingdom" fue el juzgado conjunto, por la Primera Sección del Tribunal Europeo de Derechos Humanos, de tres reclamaciones, nº 58170/2013, nº 62322/2014 y nº 24960/2015, interpuestas, respectivamente, en 04 de septiembre de 2013, 11 de septiembre de 2014 y 20 de mayo de 2015, propuestas por las entidades, en la primera aplicación, Big Brother Watch, English PEN, Open Rights Group y Dr Constanze Kurz; en la segunda aplicación, *Bureau of Investigative Journalism* y *Alice Ross,* y, en la tercera aplicacíón, *Amnesty International Limited, Bytes For All, The National Council for Civil Liberties ("Liberty"), Privacy International, The American Civil Liberties Union, The Canadian Civil Liberties Association, The Egyptian Initiative For Personal Rights, The Hungarian Civil Liberties Union, The Irish Council For Civil Liberties Limited* y *The Legal Resources Centre*; todas en contra del Reino Unido de Gran Bretaña e Irlanda del Norte.

Además, en la primera aplicación, intervinieron las entidades *Human Rights Watch, Access Now, Bureau Brandeis, Center For Democracy & Technology, European Network of National Human Rights Institutions and Equality and Human Rights Commission, Helsinki Foundation For Human Rights, International Commission of Jurists, Open Society Justice Initiative, The Law Society of England and Wales* y *Project Moore*; en la segunda aplicación, *Center For Democracy & Technology, Helsinki Foundation For Human Rights, International Commission of Jurists, National Union of Journalists* y *Media Lawyers' Association*; y, en la tercera aplicación, las entidades *Article 19, Electronic Privacy Information Center* y *Equality and Human Rights Commission*, demostrando la importancia metaindividual y mundial de la discusión llevada a cabo por la Corte.

El mérito de las reclamaciones se refería al alcance y la magnitud de los programas de vigilancia electrónica operados por el gobierno británico, teniendo como base introductoria las revelaciones realizadas por Edward Snowden en 2013 relativas a los acuerdos de cooperación entre las agencias de inteligencia de los Estados Unidos y del Reino Unido, como se ha indicado anteriormente. En una estrecha síntesis (que se desarrollará más adelante), los postulantes creían que, debido a la naturaleza de sus actividades periodísticas, sus comunicaciones electrónicas pudieron ser interceptadas por el servicio de inteligencia del Reino Unido; u obtenidas por los servicios de inteligencia del Reino Unido tras ser interceptadas por gobiernos extranjeros; o, incluso, adquiridas por las autoridades del Reino Unido a través de los Proveedores de Servicios de Comunicación (Communications Service Providers, en inglés, con la sigla CSP).

En cuanto a los procedimientos domésticos de cada caso, los primeros postulantes protocolaron una solicitud para que el gobierno británico declarara que las Secciones 1 y 3 del *Intelligence Services Act*, Sección 1 del *Security Services Act* y Sección 8 del RIPA eran incompatibles con el Convenio Europeo de Derechos humanos. En respuesta, el gobierno afirmó que la Sección 65 del RIPA excluía de la jurisdicción de la Corte Europea las reclamaciones sobre derechos humanos relativas a los servicios de inteligencia, pero que el desacuerdo podría ser llevado al *Investigatory Powers Tribunal* para su análisis. Los segundos postulantes no iniciaron ningún procedimiento doméstico, pues creían que no tendrían respuesta efectiva a sus quejas.

Los terceros postulantes protocolaron una reclamación ante el *Investigatory Powers Tribunal*, alegando que los servicios de inteligencia violaban los artículos 8, 10 y 14 de la Convención Europea, por el acceso, recepción y/o interceptación de comunicaciones por los programas de vigilancia, no habiendo, el gobierno británico, confirmado ni negado las acusaciones. Después del procedimiento legal, incluso recursal, el juez británico entendió que la cuestión de los programas de inteligencia afectaba a dicho artículo 8 y 10 de la Convención, y para que la interferencia fuera considerada de acuerdo con la ley, no podía haber discreción irrestricta sobre la en el argumento de la seguridad nacional, pero que, al menos, las reglas y el ámbito de

[1] El presente capítulo, salvo cuando expresamente escrito de otra forma, es enteramente hecho bajo la referencia: UNIÓN EUROPEA, 2018, s.p.

aplicación deberían ser de conocimiento público, lo que la Corte consideró que no eran suficientemente divulgadas; y, en lo que se refiere a la protección periodística, el Tribunal acordó que era imposible anticipar una autorización judicial en los casos de monitoreo no dirigido, pero que el código de práctica del gobierno tenía soluciones adecuadas para el caso de encontrar comunicación protegida.

Insatisfechos con las respuestas de las jurisdicciones internas, las entidades referidas demandaron ante la Corte Europea de Derechos Humanos un posicionamiento sobre la cuestión jurídica, siendo los casos admitidos ante el tribunal. El juicio abordó: a) supuesta infracción del artículo 8 del Convenio, por incompatibilidad del régimen de interceptación masiva bajo la Sección 8 (4) del RIPA, del régimen de intercambio de datos y del régimen de adquisición de datos de comunicaciones del Capítulo II del RIPA; b) la supuesta infracción del artículo 10 de la Convención, ya que el régimen de interceptación masiva bajo la Sección 8 (4) del RIPA y el régimen de adquisición y uso compartido de datos de comunicaciones bajo el Capítulo II del RIPA socavan la libertad de expresión, entre ellas la cobertura periodística y posturas o entidades similares de investigación; c) supuesta violación del art. 6 de la Convención; y d) supuesta violación del art. 14, de la Convención, en combinación con los artículos 8 y 10 del Convenio.

La Sección 8 (4) del RIPA señala que la necesidad de contener a una persona como objeto de interceptación o un conjunto de premisas respecto de las cuales la interceptación debe recaer es alejada en los casos en que a) la descripción de las comunicaciones es suficiente para limitar la comunicación conducta autorizada en el mandamiento, cuando éste se trate de la interceptación de comunicaciones externas en el curso de un sistema de telecomunicación; y b) cuando el Secretario de Estado emita un certificado en cuanto a las descripciones del material en el que considera necesario el examen (REINO UNIDO, 2000, s.p.). Y el Capítulo II del RIPA permite la interceptación de datos cuando una persona designada cree que es necesario, por interés de la seguridad nacional, para el propósito del crimen aplicable, en interés del bienestar económico del Reino Unido y en interés de la seguridad pública (REINO UNIDO, 2000, s.p.).

En cuanto al régimen de interceptación masiva de comunicaciones bajo la Sección 8 (4) del RIPA y su incompatibilidad con el artículo 8 de la Convención, los solicitantes recordaron seis parámetros ya juzgados por la Corte: a) el motivo de las interceptaciones ("interés de seguridad nacional" y "bienestar económico del Reino Unido") es muy vago para proveer un límite claro de las actividades; b) no hay una definición clara de la comunicación interna o externa, de modo que cualquier persona podría ser objeto de una búsqueda; c) la interceptación puede no tener límite de duración, ya que la orden puede renovarse indefinidamente; d) el procedimiento de filtro, almacenamiento y análisis del material interceptado no posee garantías adecuadas, pues los filtros no están dispuestos en los mandatos y requerimientos; e) en relación con la divulgación del material interceptado a otro Estado, las garantías son ineficaces, ya que los términos "mínimo necesario para el fin autorizado" y "informaciones que son o serán probables de ser necesarias" son muy amplias; y f) no hay garantía eficaz contra la retención desproporcionada de los datos interceptados.

El gobierno británico, en respuesta, afirmó que la información e inteligencia obtenida bajo la Sección 8 (4) del RIPA era crítica para la protección del Reino Unido de amenazas de seguridad nacional y de terrorismo. Por otra parte, el Gobierno negó que la Sección 8 (4) del RIPA permita la vigilancia masiva o el acceso generalizado de comunicaciones, pero que, por medio de una orden, puede interceptar determinadas comunicaciones, y la distinción entre comunicación interna y "externa" estaba bien clara. Asimismo, declaró que, en otras oportunidades, la Corte entendió que los motivos de interceptación eran suficientemente claros. Se ha señalado que el material interceptado no puede ser leído, visto o escuchado por cualquier persona, salvo con el certificado del Secretario de Estado, siendo que la duración del mandato guarda relación con la necesidad de interceptación y que la norma impone el almacenamiento y la destrucción segura de dicha información. En cuanto a la comunicación de estos datos a terceros, el gobierno argumentó que existen precauciones para una transmisión segura.

Después de analizar los argumentos, la Corte entendió que la decisión de operar un régimen de interceptación en masa pertenece al margen de apreciación del Estado y que, ante las revelaciones de Edward Snowden y de las investigaciones realizadas, los servicios de inteligencia del Reino Unido se toman en serio sus obligaciones y no abusan de sus poderes bajo la Sección 8 (4) del RIPA. Sin embargo,

analizando estos poderes, dos áreas son de mayor preocupación: primero, la falta de supervisión de todo el proceso de selección, incluyendo la selección de ceñidos para interceptación, los términos y criterios de búsqueda para filtrar comunicaciones interceptadas, y la selección de material para el examen por un analista; y, en segundo, la ausencia de garantías reales aplicables a la selección de datos de comunicaciones relacionadas para el examen. Así, ante estas deficiencias, consideró que la Sección 8 (4) no cumple el requisito de "calidad de la ley" y es incapaz de mantener la interferencia en lo que es necesario a una sociedad democrática, lo que, por lo tanto, viola el artículo 8º de la Convención.

En lo que se refiere al régimen de intercambio de datos, los solicitantes discuten que no hay base legal para ese intercambio de información entre los servicios de inteligencia y que el régimen no atiende a los requisitos de "calidad de ley". Además, los solicitantes explican que la recepción de información de interceptación por el Reino Unido de un Estado extranjero es tan grave como la propia vigilancia del Estado demandado en sí y que dicho régimen de intercambio de datos no respeta en la misma medida los seis parámetros identificados en el caso de la Sección 8 (4) del RIPA.

En contestación, el gobierno declaró que el régimen de compartir tiene base en ley interna y que la ley es claramente accesible por el pueblo. Se refutó que sería necesario cumplir los seis parámetros identificados anteriormente, pues era imposible saber cómo y por qué el Estado extranjero había obtenido tales datos y que, incluso si eran aplicables al caso, se garantizaban la comunicación alcanzada. Señaló que el régimen de intercambio de datos estaba sujeto a mecanismos de supervisión y que, hasta el momento, no hay noticia de abuso o ilegalidad.

Por su parte, la Corte concluyó que la legislación interna indica claramente el procedimiento para solicitar la interceptación o el envío de material de interceptación de agencias de inteligencia extranjeras, siendo recomendado que el material transferido sólo deba poder ser investigado si todas las exigencias materiales de una búsqueda nacional se cumpliesen y eso fuese debidamente autorizado de la misma forma que una búsqueda masiva obtenida por la agencia de inteligencia. El Tribunal observó, además, que no había pruebas de ninguna deficiencia significativa en la aplicación y funcionamiento del régimen y que, por consiguiente, el régimen no violaba el artículo 8 del Convenio.

En lo que se refiere al régimen de adquisición de datos de comunicaciones bajo el Capítulo II del RIPA, los solicitantes alegaron que dicho dispositivo legal permitía la obtención de datos de comunicación en una amplia gama de circunstancias mal definidas, sin garantías adecuadas, como, por ejemplo, en relación con el manejo y la explotación de datos de comunicaciones. Además, se quejaron que la autorización para la adquisición de datos de comunicaciones era proporcionada por una persona designada, que no era suficientemente independiente del ejecutivo o incluso del organismo que solicitó la divulgación.

Por su parte, el gobierno británico apuntó que, como el régimen del Capítulo II es un régimen direccionado, no hay nada "no intencional" en su operación, o sea, la adquisición de datos de comunicación bajo ella sería siempre intencional, siendo, por lo tanto, distinguible de los regímenes para la interceptación masiva o la adquisición masiva de datos. Asimismo, ha puntuado que las leyes internas proporcionan garantías relativas a la conservación de datos de comunicaciones adquiridos en virtud del régimen del Capítulo II y que el Comisario de Interceptación de Comunicaciones proporciona un grado importante de supervisión del funcionamiento del régimen.

La Corte, por otra parte, entendió que la legislación interna del Reino Unido entra en conflicto con la legislación comunitaria de la Unión Europea, en cuyo caso esta última tiene primacía. Esto quiere decir que, si el acceso a los datos retenidos no se limitaba al objetivo de combatir "crimen grave" y si el acceso a los datos retenidos no estaba sujeto a revisión previa por un tribunal o por un órgano administrativo independiente, entonces dicho régimen entra en conflicto con las determinaciones comunitarias. Es decir, cualquier régimen que permita a las autoridades el acceso a los datos retenidos por los proveedores para combatir "crimen grave" debe estar sujeto a la revisión previa por un tribunal u órgano administrativo independiente. Así, como el régimen del Capítulo II permite el acceso a datos retenidos con el objetivo de combatir crimen (y no "crimen grave") y, salvo cuando el acceso es buscado con la finalidad de determinar la fuente de un

periodista, no está sujeto la revisión previa por un tribunal u órgano administrativo independiente, viola evidentemente el artículo 8 de la Convención.

Las demandantes, en otro punto, alegaron que los programas de vigilancia en masa violan el artículo 10 del Convenio, ya que la interceptación de las comunicaciones puede crear un riesgo significativo de revelar fuentes periodísticas o material periodístico confidencial, de modo que ello sólo se justificaría en caso de "interés público superior" y la autorización sólo podría ser concedida por un juez u órgano independiente. Las entidades refirieron que, en calidad de periodistas involucrados en cuestiones de interés público, incluso en funciones de vigilancia pública, la protección conferida por el artículo 10 era de importancia crítica para ellos.

En concreto, en relación con el régimen de la Sección 8 (4) del RIPA, las entidades argumentaron que la interceptación del material recogido a través de la vigilancia masiva no contaba con la presencia de garantías adecuadas, porque, primero, la definición de "material periodístico confidencial" era muy restringido; y, en segundo, porque el régimen no cumplía con las garantías del artículo 10 de la Convención, en lo que se refiere al "interés público superior" y la necesidad de una autorización judicial, o al menos independiente. En relación al régimen del Capítulo II del RIPA, las entidades reclamaron que la interceptación de datos de comunicación era tan invasiva como la propia obtención del material periodístico confidencial, ya que los datos podrían revelar la identidad de la fuente y otra enorme cantidad de detalles.

En respuesta, el Gobierno británico alegó que, durante una interceptación en masa, no hay como haber una autorización previa para un seguimiento estratégico de la interceptación, pero que, si un material periodístico fuera interceptado durante el funcionamiento de dicho régimen, la norma interna prevé un marco protocolo de protección de tal material confidencial. Sobre el Capítulo II del RIPA, el gobierno indicó que ese régimen era siempre intencional y dirigido en el objetivo de adquisición de datos de comunicación y que, por lo tanto, en el caso de intento de descubrir una fuente periodística, una autorización judicial era siempre necesaria, no habiendo lo que se refiere a garantías adicionales.

La Corte, en primer lugar, reiteró que la libertad de expresión constituye uno de los fundamentos esenciales de una sociedad democrática y que las garantías a ser concedidas a la prensa son de particular importancia, especialmente la protección de fuentes periodísticas, de forma que una injerencia no puede ser compatible con el artículo 10 del Convenio, a menos que esté justificada por una exigencia imperiosa de interés general. En cuanto al régimen de la Sección 8 (4) del RIPA, el Tribunal consideró que las autoridades sólo saben que el material interceptado es confidencial cuando se ha examinado o utilizado filtros de selección para el análisis del contenido, lo que, por el entendimiento de los jueces, los analistas podrían hacer sin la utilización de garantías adicionales, según lo exigido por el artículo 10, de la Convención, como por ejemplo "interés público superior" o después de la autorización judicial.

Por otro lado, en cuanto al régimen del Capítulo II del RIPA, la Corte observó que, aunque es reconocido que permite una protección reforzada cuando los datos son solicitados con el objetivo de identificar la fuente de un periodista, estas disposiciones no se aplican en todos los casos en que existe una solicitud para obtener datos de comunicación de un periodista, lo que sugiere una injerencia desproporcionada y en desacuerdo con la ley. Por tales motivos, el Tribunal consideró que el régimen de la Sección 8 (4) y el régimen del Capítulo II del RIPA infringe el artículo 10 del Convenio.

A continuación, los solicitantes del tercer caso reclamaron que las limitaciones inherentes del Tribunal doméstico, especialmente una reunión secreta celebrada entre miembros del Tribunal y el Servicio de Seguridad británico (MI5) y audiencias sigilosas, eran desproporcionales en cuanto a la esencia de un tribunal justo, consubstanciado en el artículo 6 del Convenio, en el que cualquier persona tiene derecho a que su causa sea examinada, equitativa y públicamente, en un plazo razonable por un tribunal independiente e imparcial establecido por la ley (UNIÓN EUROPEA, 1950, s.p.). Además, la norma dice que el juicio debe ser público, salvo cuando la publicidad pueda ser perjudicial para los intereses de la justicia (UNIÓN EUROPEA, 1950, s.p.).

En la referida cuestión, el Tribunal recordó que ya se había manifestado en otros casos similares, en el sentido de que, para garantizar la eficacia del régimen de vigilancia secreta y teniendo en cuenta la

importancia de tales medidas para la lucha contra el terrorismo y la delincuencia las limitaciones procesales eran necesarias y proporcionadas. Además, sobre la reunión celebrada entre miembros del IPT y del MI5, la Corte ponderó que, debido a la especialidad de esa justicia, el encuentro con el servicio de inteligencia para discutir cuestiones de procedimiento y protocolos no pone en duda la imparcialidad o independencia de la jurisdicción, tanto que no hay noticia ni prueba sustancial de perjuicio a las partes. Así, el procedimiento llevado a cabo ante el *Investigatory Powers Tribunal* no perjudicó la esencia misma de los derechos al artículo 6 de la Convención.

Por último, las demandantes del tercer caso formularon una reclamación, en relación con los artículos 8 y 10 del Convenio, pues que el régimen de interceptación masiva bajo la Sección 8 (4) del RIPA y las garantías adicionales de la Sección 16 del RIPA, eran indirectamente discriminatorios por razón de la nacionalidad, en afrenta al artículo 14 del Convenio. Esto, pues, considerando que parte de los objetivos de interceptación es comunicación "externa", las personas extranjeras al Reino Unido tienen más probabilidades de ser monitoreadas, así como que las garantías de la Sección antes citada se dirigen sólo a personas conocidas en las Islas Británicas.

Sin embargo, la Corte respondió que, aunque el régimen busque "comunicaciones externas", es decir, "una comunicación enviada o recibida fuera de las Islas Británicas", la interceptación de comunicaciones implica una parte que se encuentra en territorio británico o, aún, en el carácter accesorio, se puede descubrir una comunicación "interna" entre personas dentro del territorio británico, no habiendo que hablar de discriminación o mayor probabilidad de interceptación de personas extranjeras. Además, en cuanto a las garantías de la Sección 16 del RIPA, el Tribunal mencionó que el examen de las interceptaciones tiene en cuenta la ubicación geográfica en las Islas Británicas y no la nacionalidad u otros aspectos personales, y no hay otra diferencia de trato relevante, que, por consiguiente, no afecta al artículo 14 del Convenio.

En este escenario y por tales razones, la Corte Europea de Derechos Humanos: a) declaró, unánimemente, inadmisibles las reclamaciones formuladas por los postulantes del tercer caso concernientes al artículo 6, artículo 10 y artículo 14; b) declaró, unánimemente, admisibles las demás reclamaciones formuladas por los postulantes del tercer caso; c) declaró, por mayoría, admisibles las reclamaciones formuladas por los postulantes del primer y segundo casos. Además, el Tribunal: d) resolvió, por cinco votos a dos, que hubo una violación del artículo 8 de la Convención, respecto a la Sección 8 (4) del RIPA; e) resolvió, por seis votos a uno, que hubo una violación del artículo 8 de la Convención sobre el Capítulo II del RIPA; f) resolvió, por cinco votos a dos, que no hubo violación del artículo 8 de la Convención, respecto al régimen de intercambio de datos de comunicación; g) resolvió, por seis votos a uno, que se produjo una infracción del artículo 10 del Convenio sobre la Sección 8 (4) y el Capítulo II del RIPA; y h) resolvió, unánimemente, que no hubo necesidad de examinar las otras reclamaciones postuladas por las entidades del tercer caso con respecto al artículo 10 del Convenio.

Y, en relación a la indemnización, la Corte resolvió, por seis votos a uno, que el Estado demandado debe pagar a los postulantes, en tres meses desde la fecha en que el juicio se convierta en definitivo: a) a los postulantes del primer caso, el valor de EUR 150.000,00 (ciento cincuenta mil euros), más cualquier tipo aplicado sobre gastos y gastos, debidamente corregido para la moneda correspondiente del país pagador; y b) a los postulantes del segundo caso, el valor de EUR 35.000 euros (treinta y cinco mil euros), más cualquier tipo aplicado a las costas y gastos, debidamente corregido para la moneda correspondiente del país que paga. Sin embargo, se solicitó la devolución del juzgado al Tribunal Pleno para confirmar o alterar la sentencia, lo que aún está pendiente, de conformidad con el artículo 43 y el artículo 44 de la Convención.

4 Conclusión

En el primer capítulo de esta investigación, además de las constataciones hechas acerca de un cambio de paradigma surgido con el desarrollo de la cibernética y de las tecnologías de información y comunicación, se abordó parte de las revelaciones traídas por el Informe del 11 de julio de 2001 del Parlamento Europeo y por Edward Snowden sobre la existencia de programas globales de vigilancia electrónica basados en la

interceptación de comunicaciones y datos de comunicaciones llevados a cabo por las agencias de seguridad de Estados Unidos y del Reino Unido. A partir de eso, se ha hecho una relación con el actual marco jurídico comunitario sobre los derechos a la privacidad y a la libertad de expresión, que son particularmente afectados por tales regímenes.

En el segundo capítulo, se analizó un caso concreto, titulado "Case of Big Brother Watch and Others v. Reino Unido", que es propuesto por diversas entidades, entre ellas Big Brother Watch, en contra del Reino Unido, cuya decisión fue pronunciada el 13 de septiembre de 2018, pendiente de revisión de recurso por el colegio de jueces. En este momento se señalaron los principales argumentos de las partes y la respuesta jurisdiccional concedida, especialmente en relación con las supuestas violaciones de los artículos 6º, 8º, 10º y 14º del Convenio Europeo de Derechos Humanos, por el régimen de interceptación de comunicaciones del RIPA, legislación británica sobre vigilancia electrónica.

En ese sentido, se vio que la Corte Europea de Derechos Humanos entendió, por mayoría de votos, que hubo una violación del artículo 8º de la Convención, respecto a la Sección 8 (4) del RIPA y del Capítulo II del RIPA; así como una violación del artículo 10º de la Convención por los mismos regímenes, ya que la falta de supervisión en partes del procedimiento de interceptación y la ausencia de garantías reales y públicas al régimen de vigilancia viola el derecho a la intimidad y, considerando se trataren de periodistas, cuyas garantías son aún más necesarias, viola también el derecho a la libertad de expresión. Además, se notó que, por otra parte, por mayoría, el Tribunal entendió que no hubo violación del artículo 8º de la Convención, respecto al régimen de intercambio de datos de comunicación entre Estados extranjeros, por tratarse de potestad del Estado.

La Corte Europea de Derechos Humanos, entonces, realiza un importante análisis de los regímenes de vigilancia masiva, al menos, sobre uno en el cual tiene jurisdicción, bajo la égida de los derechos al respeto a la vida privada y familiar y a la libertad de expresión. En este escenario, toma posición en el sentido de que, aunque los programas de vigilancia están dentro del margen de aplicación de los Estados y encuentran guarida en las excepciones presentes en el orden jurídico vigente, la forma con que fueron y vienen siendo desarrollados por las agencias de seguridad puede violar los derechos fundamentales de los administrados, debido a la falta de supervisión pública del proceso de interceptación, a la falta de garantías adicionales a sectores específicos que pueden ser objeto de investigación y a la falta de publicidad relacionada con los programas, en sus límites, ya que sus existencias han sido reveladas bajo polémicas internacionales.

Sin embargo, la Corte, por mayoría, aprobó el régimen de intercambio de datos entre agencias de seguridad nacionales, no entendiendo que había violación en esta hipótesis. Se observa que, si en los demás regímenes ha habido violación por no haber supervisión pública o garantías seguras y reales, es presumible que, en ese régimen de intercambio entre los gobiernos, podría haber violación de igual forma, ya que exigibles aún más garantías y procedimientos nacionales de autorización, por involucrar autoridad que puede no guardar relación alguna con el sujeto objeto de vigilancia. Además, el hecho de que el régimen cumpla exactamente la legislación interna que lo estructura no se refiere que la privacidad de los individuos es garantizada o que el programa no tiene fallas, lo que merecería más atención por parte del Tribunal, en particular teniendo en cuenta la nueva normativa europea de protección y transferencia de dados, que entró en vigor en mayo de 2018.

Referencias

AYUSO, Silvia; PEREDA, Cristina. Obama conmuta la pena de la soldado Chelsea Manning. **El País**, Whashington, 18 ene. 2017. Disponible en: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html. Acceso en: 10 abr. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

GREENWALD, Gleen. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10. ed. São Paulo: Saraiva, 2015.

NORTON-TAYLOR, Richard. Not so secret: deal at the heart of UK-US intelligence. **The Guardian**, 2010. Disponible en: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released. Acceso en: 15 fev. 2019.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. **Declaración Universal de Derechos Humanos de 1948**. Disponible en: https://www.un.org/es/universal-declaration-human-rights/. Acceso en: 10 abr. 2019.

PIRES, Hindenburgo Francisco. Geografia das indústrias globais de vigilância em massa: limites à liberdade de expressão e organização na internet. **Ar@cne Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales**, Universidad de Barcelona, n. 183, abr. 2014. Disponible en: http://www.ub.edu/geocrit/aracne/aracne-183.htm#_edn16. Acceso en: 02 abr. 2019.

POITRAS, Laura; RISEN, James. N.S.A. gathers data on social connections of U.S. citizens. **The New York Times**, 28 sept. 2013. Disponible en: http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html. Acceso en: 14 fev. 2019.

REINO UNIDO. **Regulation of Investigatory Powers Act 2000**. Disponible en: https://www.legislation.gov.uk/ukpga/2000/23/section/8. Acceso en: 10 abr. 2019.

UNIÓN EUROPEA. **Convenio Europeo de Derechos del Hombre, de 04 de noviembre de 1950**. Disponible en: https://www.echr.coe.int/Documents/Convention_ENG.pdf. Acceso en: 10 abr. 2019.

UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. **Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)**. Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048. Acceso en: 12 abr. 2019.

UNIÓN EUROPEA. Parlamento Europeo. **Informe de 11 de julio de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON)**. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//ES. Acceso en: 12 abr. 2019.

WIKILEAKS. **What is WikiLeaks**. 03 November 2015. Disponible en: https://wikileaks.org/What-is-Wikileaks.html. Acceso en: 16 fev. 2019.

Recebido em: 28/05/2019
Aprovado em: 09/08/2019