DERECHO PUCP
N° 75, 2015
pp. 207-228
REVISTA DE LA FACULTAD DE DERECHO

Vigilancia y privilegio periodístico en la era de las nuevas tecnologías de las telecomunicaciones bajo la Convención de Derechos Humanos y Libertades Fundamentales y la Constitución de la República de Polonia

Journalistic monitoring and privilege in the era of new telecommunications technologies under the Convention on Human Rights and Fundamental Freedoms and the Constitution of the Republic of Poland

JAN PODKOWIK*

Resumen: La era digital ha reconfigurado los servicios de seguridad, sobre todo las formas de vigilancia masiva que buscan prevenir distintas amenazas para la sociedad. No obstante, este escenario puede convertirse en problemático desde la perspectiva de la protección de la libertad de los medios de comunicación y del privilegio periodístico. El autor del presente artículo nos ofrece un panorama sobre los alcances de la tutela del privilegio periodístico en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como sobre su tratamiento en Polonia a partir de los desarrollos realizados por su Tribunal Constitucional.

Palabras clave: Privilegio periodístico – vigilancia masiva – secreto profesional – libertad de prensa – Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales –Tribunal Europeo de Derechos Humanos – Tribunal Constitucional de Polonia

Abstract: The digital age has reconfigured the security services, especially the forms of mass surveillance aimed at preventing various threats to society. However, this scenario may become problematic from the perspective of protecting the freedom of the media and journalistic privilege. The author of this article offers an overview of the scope of the protection of the journalistic privilege pursuant to the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as its management in Poland from the developments prepared by its Constitutional Court.

* Doctor en Derecho por la Universidad de Varsovia y Profesor Asistente en la Facultad de Derecho y Administración de la Universidad Jagellónica de Cracovia (investigador posdoctoral en el proyecto: «Implicación de la jurisdicción constitucional en las relaciones jurídicas de los privado-partidos»); empleado de la ley en la Oficina del Tribunal Constitucional de la República de Polonia. Anteriormente trabajó en la oficina del Defensor de los Derechos Humanos y en la Universidad Nacional de Defensa (Varsovia, Polonia). Correo electrónico: podkowik@trybunal.gov.pl

Key words: Journalistic privilege – mass surveillance – professional secret – press freedom – European Convention for the Protection of Human Rights and Fundamental Freedoms – European Court of Human Rights – Polish Constitutional Tribunal

I. LA NATURALEZA DEL PROBLEMA DE INVESTIGACIÓN

I.1. El propósito de este trabajo es exponer el problema de las violaciones del secreto periodístico, en particular, de la confidencialidad de las fuentes periodísticas, con respecto al uso de las medidas de vigilancia electrónica, en particular la llamada vigilancia masiva.

I.2. El desarrollo de nuevas tecnologías basadas en las redes de telecomunicaciones y comunicaciones por satélite ha contribuido a los cambios en los procesos de recolección, procesamiento y transferencia de datos entre los diferentes tipos de entidades. Aparte de la telefonía fija y móvil, han ido apareciendo el correo electrónico, la telefonía por Internet (VOIP) y otros servicios de mensajería por Internet, incluida la comunicación por satélite, que cada vez es más común (Zittrain, 2008). En la práctica, esas formas de comunicación han reemplazado fundamentalmente a las tradicionales, como la correspondencia.

Hoy en día, Internet no es solo una forma de comunicación, cada vez es más importante para la computación en nube, que permite el acceso universal, conveniente y concedido bajo demanda a un conjunto compartido de recursos, incluyendo espacios entre los discos y los servidores o aplicaciones para editar textos, imágenes y otros contenidos multimedia, comercio electrónico, e-learning, etcétera (Rittinghouse & Ransome, 2010; Pearson & Yee (eds.), 2013). Por lo tanto, Internet permite el acceso remoto a los recursos almacenados en la nube desde cualquier lugar del mundo y por cualquier dispositivo electrónico, sin almacenar los datos en los discos duros y sin ningún contacto físico con la unidad.

I.3. El desarrollo tecnológico es uno de los factores que ha contribuido a un cambio fundamental en el modelo operativo de las fuerzas de policía y los servicios de inteligencia. La transferencia masiva de datos, junto con su extraterritorialidad han exigido que los servicios de seguridad

se mantengan al día con una realidad social dinámica. La vigilancia con un objetivo específico, que consiste en las escuchas telefónicas o la incautación a documentos concretos con una orden judicial, ha sido sustituida por la denominada vigilancia preventiva. Esta última está basada en sistemas inteligentes utilizados para la recolección, almacenamiento y análisis del contenido de los mensajes transmitidos a través de redes de telecomunicaciones, la información almacenada en los discos virtuales o diferentes tipos de metadatos. Tal forma de vigilancia se lleva a cabo no solo para detectar delitos graves ya cometidos, como el espionaje o el terrorismo, sino para identificar las amenazas y prevenir su aparición. Esto es así pues actualmente el enfoque ha cambiado y ha pasado de la detección de amenazas a la prevención de amenazas.

La divulgación de los métodos de vigilancia causaría inevitablemente su ineficacia (Tribunal Constitucional de Polonia, 2005, parte III, 1.1.). En la práctica, el público tiene un conocimiento elemental sobre las acciones realizadas sobre la base de informes lacónicos entregados por las autoridades de supervisión. Sin embargo, también recibe información adicional a través de las actividades de los informantes[1]. Parece ser que cierto grado de desinformación —incluso sobre formas de vigilancia y sus estadísticas generales— ha sobrepasado el punto crítico. La sociedad —no solo en los países del antiguo bloque soviético, donde después de la II Guerra Mundial se instalaron sistemas de supervisión, sino también en los países con democracias bien establecidas— no está de acuerdo con sacrificar su propia libertad y la privacidad en aras de una promesa incierta de seguridad. La renuencia a nuevos métodos de protección de la seguridad nacional, que impliquen injerencia en la esfera privada, se hace más común sobre todo en la eficacia de la denominada vigilancia masiva, la cual es criticada incluso por antiguos miembros de alto rango de los servicios que están bien familiarizados con la eficacia de tales medidas[2] y los órganos parlamentarios o internacionales de protección de los derechos humanos (Organización de las Naciones Unidas (ONU), 2014; Asamblea Parlamentaria del Consejo de Europa, 2015a).

1 Un ejemplo de modelo del control parlamentario de los servicios de inteligencia es la reacción del Parlamento Europeo a la divulgación de información por Edward Snowden de la colección masiva de datos por la Agencia Nacional de Seguridad (NSA) de los Estados Unidos y la cooperación con las agencias de los Estados miembros. Como resultado de la alarma de Snowden, se examinó el problema. Por lo tanto, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo llevó a cabo su propia investigación, cuyos resultados fueron recogidos en el documento de trabajo sobre los Programas de vigilancia de los Estados Unidos y los Estados miembros de la UE y su repercusión sobre los derechos fundamentales de los ciudadanos europeos. Sobre la base de este documento, se aprobó la resolución correspondiente (Parlamento Europeo, 2014b).

2 Según un memorándum abierto presentado al presidente Obama por antiguos directivos de la NSA, la colección masiva de datos no aumenta la capacidad de prevenir futuros ataques terroristas; mientras que los autores subrayan que la vigilancia masiva llevada a cabo por la NSA no ha resultado en la prevención de ningún ataque y que miles de millones de dólares se han gastado en programas que son menos eficaces y mucho más intrusivos en las relaciones jurídicas de la privacidad de los ciudadanos que otros tipos de tecnología (NSA Insiders Reveal What Went Wrong, 2014).

I.4. Diversas formas de vigilancia son muy conocidas en todo el mundo. Las formas más comunes son, por ejemplo, escuchas telefónicas y otras medidas técnicas que permitan acceso al contenido de los mensajes de telecomunicaciones. Por lo general, están permitidas solo con el fin de prevenir o combatir delitos graves. Además, se requiere la aprobación de un tribunal u otro órgano imparcial para su uso. La admisibilidad de dichas medidas en un Estado democrático de derecho es incuestionable (Tribunal Europeo de Derechos Humanos, 1978; 1984; 1990; 2001; 2006; 2007a; 2007b; 2009a; 2010a; 2012a).

Durante varios años, la policía y los servicios de inteligencia de todo el mundo se han beneficiado de los metadatos de las telecomunicaciones —datos de tráfico y de localización, sin el contenido de la información transmitida— (Bignami, 2007; Stalla-Bourdillon, 2014, p. 59; para la retención de datos en Canadá, China, Reino Unido, Estados Unidos, Alemania, Israel, India, Australia y Japón, véase Cate & otros (eds.), 2012). La obligación de recopilar metadatos en la Unión Europea se impuso a los proveedores de telecomunicaciones por la Directiva 2006/24/CE (Parlamento Europeo & Consejo de la Unión Europea, 2006), la cual fue recientemente anulada por el Tribunal de Justicia de la Unión Europea (TJUE, 2014). En términos generales, la Directiva obliga a los proveedores de telecomunicaciones a retener ciertas categorías de datos por un período de entre seis meses y dos años y ponerlos a disposición, previa solicitud, de las autoridades policiales para la investigación, detección y enjuiciamiento de delitos graves y actos de terrorismo.

Sobre la base de estos datos, resulta posible determinar el flujo de información dentro de un grupo de entidades para reconstruir los procesos de toma de decisiones e incluso la jerarquía de grupos criminales, así como para identificar qué individuos se comunican entre sí en determinado lugar y tiempo (Xu & otros, 2004; Tribunal Constitucional Federal Alemán, 2010). Según el TJUE, teniendo en cuenta la creciente importancia de los medios de comunicación electrónica, los datos retenidos brindan a las mencionadas autoridades oportunidades adicionales para esclarecer los delitos graves, por ello, son una herramienta valiosa para las investigaciones criminales. En consecuencia, la retención de datos puede considerarse como apropiada para alcanzar el objetivo perseguido por dicha Directiva.

La lucha contra las formas graves de corrupción —en especial contra la delincuencia organizada y el terrorismo— es, de hecho, de suma importancia a fin de garantizar la seguridad pública y su efectividad puede depender, en gran medida, de la utilización de técnicas modernas de investigación. Sin embargo, como explicó el TJUE, la Directiva no establece ningún criterio objetivo mediante el cual se limite el número

de personas autorizadas a acceder y utilizar los datos retenidos a lo estrictamente necesario a la luz del objetivo perseguido.

Adicionalmente, el acceso de las autoridades nacionales competentes a los datos conservados no depende de un examen previo llevado a cabo por un tribunal o por un órgano administrativo independiente, cuya decisión trataría de limitar el acceso a los datos y su uso a lo estrictamente necesario para la finalidad de alcanzar el objetivo perseguido y cuya intervención sigue una solicitud motivada de dichas autoridades presentadas en el marco de los procedimientos de prevención, detección o enjuiciamiento penal. Por otra parte, el período de retención se ajusta a entre un mínimo de 6 meses y un máximo de 24 meses, pero no se establece que la determinación del período debe basarse en criterios objetivos a fin de garantizar que se limite a lo estrictamente necesario. La Directiva no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales.

Hoy en día existe *software* de inteligencia de vigilancia masiva que permite recoger diferentes tipos de datos de personas no identificadas y luego analizarlos en términos de criterios programados —por ejemplo, palabras clave, números—. Programas como PRISM, Xkeyscor, MUSCULAR, Tempora y otros prestan servicios de inteligencia de acceso a los recursos de los proveedores de telefonía o Internet (Parlamento Europeo, 2014a). En tales casos, los riesgos asociados a este tipo de vigilancia preventiva de los ciudadanos son reconocidos correctamente, ya que dicha vigilancia no se dirige contra personas sospechosas de actividades ilegales, sino contra cualquier persona que utiliza los nuevos medios de comunicación a distancia o herramientas de procesamiento y almacenamiento de datos. Por lo tanto, el riesgo de ser sometidos a la vigilancia no depende de que se incurra en un delito, sino que el simple hecho de utilizar determinados medios de comunicación es suficiente para estar en riesgo.

I.5. En mi opinión, el desarrollo tecnológico, por un lado, y el cambio de la metodología de operación de la policía y los servicios de inteligencia, por el otro, redefinen la clasificación legal de la privacidad y el privilegio periodístico. El problema central en la era digital no es la cuestión de si se puede exigir la divulgación de la identidad de los informantes a través de una orden judicial (lo que era un tema fundamental en la era de la comunicación analógica), sino, más bien, cómo los efectos de la interferencia con el privilegio periodístico, en lo que respecta a las herramientas automáticas para la recolección y análisis de datos, podrían ser minimizados.

Las preguntas fundamentales son: ¿cuándo podemos hablar de una violación del privilegio periodístico? ¿Descargar los datos personales

almacenados en la nube, la cual contiene información sujeta al secreto periodístico, constituye una violación? ¿Solo se considera interferencia el análisis directo de datos conducente a la identificación de la periodista y su fuente? Preocupaciones similares se relacionan con las circunstancias en las que se obtiene información por los servicios de inteligencia. Por ejemplo, se plantea la cuestión de si existe una violación al privilegio periodístico solo después de la negativa del periodista a proporcionar la información, citando privilegio periodístico, o tal vez una violación del privilegio periodístico tiene lugar siempre que los servicios entraran en posesión de información que se genera y se asocia con la actividad periodística de una persona determinada. Por último, otro problema se refiere al derecho a la protección, en particular, si ese derecho incluye entidades involucradas en el periodismo ciudadano —que no trabajan como periodistas profesionales—.

Hasta cierto punto, tales dilemas resultan de las deficiencias de las soluciones legislativas aplicadas en un período de comunicaciones analógicas, las cuales no son adecuadas para procesos masivos de intercambio de información en la era de la comunicación digital.

I.6. El problema de la protección de la libertad de los medios y el privilegio periodístico son aún de vital importancia (Asamblea Parlamentaria del Consejo de Europa, 2015b; Dobbie (ed.), 2013). Dar respuestas a todas las cuestiones antes mencionadas, no es posible en este momento. Por lo tanto, me centraré en solo tres preguntas principales. En primer lugar, si las jurisprudencias del Tribunal Europeo de Derechos Humanos sobre el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales —más conocido como la Convención Europea de sobre los Derechos Humanos (CEDH)— y del Tribunal Constitucional de Polonia en relación con el privilegio periodístico siguen siendo adecuadas para la evaluación de la legislación y la práctica del uso en vigilancia masiva y las nuevas tecnologías. En segundo lugar, ¿qué criterios deben tenerse en cuenta para evaluar la proporcionalidad de la interferencia en el privilegio periodístico ocasionada por la vigilancia? En tercer lugar, me gustaría hacer referencia al caso relativo a la constitucionalidad de las disposiciones polacas sobre el control operativo y la retención de datos. El 30 de julio de 2014, el Tribunal Constitucional de Polonia dictaminó que algunas disposiciones de la ley de vigilancia —el llamado control operacional y la retención de datos— son inconstitucionales (Tribunal Constitucional de Polonia, 2014.). Estas disposiciones fueron controvertidas ya que, entre otras cosas, no protegían suficientemente el secreto profesional, sobre todo de abogados y periodistas, ni los privilegios médicos. Por esta razón, fueron declaradas incompatibles con el derecho a la defensa (artículo 42, apartado 2), el derecho a la intimidad (artículo 47) y la libertad de expresión (artículo 54, párrafo 1 de la Constitución polaca).

II. EL SIGNIFICADO DEL SECRETO PERIODÍSTICO Y SU PROTECCIÓN DESDE EL PUNTO DE VISTA DE LA CEDH Y LA CONSTITUCIÓN DE POLONIA DE 1997

II.1. El uso de la información obtenida de informantes confidenciales es una de las herramientas más valiosas para los periodistas. A través de los materiales enviados por los informantes, se hace posible alertar a la opinión pública sobre las irregularidades, fraudes o delitos, que han permanecido ocultos cuidadosamente, de aquellos en el poder. Como explicó el TEDH, sin esa información proporcionada por las fuentes, el papel vital de vigilancia pública de la prensa podría verse socavado y la capacidad de la prensa para proporcionar información precisa y confiable puede verse afectada (TEDH, 1996, párrafo 39; 1999, párrafo 59; 2003, párrafo 57; 2009c, párrafo 59; 2007c, párrafo 53). Por lo tanto, la protección del privilegio periodístico frente a la presión derivada del Estado, al que, por diversas razones, le gustaría conocer la identidad de los informantes, es de particular importancia. Por ello, la protección del privilegio periodístico es ampliamente considerada como uno de los pilares de la libertad de prensa (TEDH, 2010b, párrafo 50). Por otra parte, el privilegio de los periodistas debe ser visto como una obligación legal y ética del periodista a no revelar la identidad de sus fuentes.

El fundamento jurídico del privilegio periodístico y su ámbito de protección en la CEDH y en la Constitución de la República de Polonia se detallan a continuación[3].

A) El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales

II.2. La CEDH no se refiere directamente al privilegio periodístico. En la jurisprudencia del TEDH se señaló que su protección se deriva del artículo 10, párrafo 1 de la CEDH (TEDH, 2007c, párrafo 60; 2013b, párrafo 95). Por lo tanto, es parte de la libertad de comunicación y difusión de información, así como la libertad de prensa (libertad de los medios), estrechamente integrada allí. El planteamiento del TEDH a este problema parece haberse estabilizado. Como explicó la corte, el derecho de los periodistas a no revelar sus fuentes no puede ser considerado un mero privilegio que se concede o quita dependiendo de la legalidad o ilegalidad de sus fuentes, sino que es parte integral del derecho a la información, y debe ser tratado con la máxima cautela (TEDH, 2007c, párrafo 65; 2013b, párrafo 97).

3 Vale la pena mencionar que ni la Convención ni la Constitución polaca estipulan *expressis verbis* el derecho del periodista a mantener en secreto la identidad de sus fuentes. Sin embargo, tal derecho —como un elemento integral de la libertad de prensa— está claramente prescrito en el artículo 38 (2) (b) de la Constitución de Portugal.

II.2.1. El tratamiento del privilegio periodístico como parte de la libertad de expresión se justifica sobre todo en la parte del artículo 10, párrafo 1 de la CEDH que se refiere al concepto de «la libertad de recibir o de comunicar informaciones». Parece que el concepto de esta libertad se ve no solo en la dimensión positiva, como una posibilidad de compartir la información disponible con los demás, sino también en la dimensión negativa, como «la libertad de la transmisión de información a otras partes», o de otra manera como «la libertad de silencio» (TEDH, 1992). La esencia del privilegio periodístico es la «libertad negativa» de un periodista —la libertad de divulgar información a otras personas, especialmente a las autoridades estatales—, y un derecho correlativo para garantizar que ninguna persona obtiene información en contra de la voluntad o sin el conocimiento de la persona interesada. Este punto de vista implica que el privilegio periodístico es un valor protegido por la CEDH como parte de la libertad de recibir o comunicar informaciones. Teniendo esto en cuenta, la obligación de revelar información, conforme a lo dispuesto por la ley, implica cada vez la violación del artículo 10, párrafo 1 de la CEDH, a menos que cumpla con los criterios de proporcionalidad del artículo 10, párrafo 2 de la CEDH (Kamiński, 2010, p. 510).

Independientemente del hecho de que el artículo 10 de la CEDH comprende la libertad de divulgación de información por parte de los periodistas y el derecho a proteger el secreto profesional, la protección de la información debe ser revisada también en el contexto de otras disposiciones de la Convención, en particular su artículo 8, que garantiza «el respeto de la vida privada» y «el respeto a la correspondencia». Por lo tanto, dos de estas disposiciones de la CEDH deben considerarse como garantías complementarias del privilegio periodístico (TEDH, 2012b, párrafo 102).

II.2.2. El artículo 10 de la CEDH no solo protege las fuentes anónimas que colaboran con la prensa para informar al público sobre asuntos de interés público (TEDH, 2005). También garantiza el derecho a no revelar su identidad en material de prensa —por ejemplo, mediante un artículo anónimo o un artículo firmado con un seudónimo—, enviando en una carta al editor.

Un tema complejo que no se ha resuelto de manera adecuada en la jurisprudencia del Tribunal de Estrasburgo es si el secreto periodístico se aplica también a las personas que participan en el periodismo ciudadano, en particular, los *bloggers* y otros involucrados con la edición, sin fines de lucro, de sitios web (como Facebook, Twitter, blogs, etcétera), donde el contenido se publica para el interés público. Parece que no hay obstáculos legales para los no profesionales —quienes pueden acogerse a la libertad de expresión e invocar el privilegio periodístico—. Después

de todo, a la luz de la redacción del artículo 10, párrafo 1 de la CEDH, la libertad de la divulgación de información no se limita subjetivamente y es ejercida por todos, no solo los periodistas.

Sin embargo, la otra cuestión se refiere a la medida del margen de apreciación que un Estado tiene en la creación de limitaciones a este privilegio, que consiste en el establecimiento de la obligación legal de proporcionar información o en un permiso para adquirir información sin el consentimiento de la persona interesada. En otras palabras, ¿en qué medida pueden los Estados construir el marco legal del privilegio periodístico? Parece que reducir el alcance de la protección únicamente a las personas que proporcionan información de manera permanente o profesional, y como tal, el ejercicio de control social, debe ser considerada como justificada. Con este supuesto, los que informan a la opinión pública por los medios de comunicación social solo incidentalmente no pueden exigir la misma protección que los periodistas. La razón de esta suposición es, en particular, la necesidad de garantizar la protección efectiva de los valores mencionados en el artículo 10, párrafo 2 de la CEDH. Si cualquier persona, incluso al informar a la opinión pública por accidente, pudiese invocar «la libertad de silencio» y exigir protección jurídica, la protección de los valores mencionados en el artículo 10, párrafo 2 de la CEDH sería en realidad ilusoria.

Vale la pena mencionar que el TEDH no dudó en tomar en cuenta las garantías derivadas del artículo 10, párrafo 1 de la CEDH en lo que respecta a recibir información sobre asuntos públicos de organizaciones sociales. Las organizaciones no gubernamentales desempeñan un papel similar al de los medios de comunicación como organismos de control público y, por lo tanto, pueden confiar en la protección resultante del artículo 10, párrafo 1. 1, de la CEDH, por lo menos cuando se trata de acceder a la información pública (TEDH, 2009, párrafo 27; 2013a, párrafo 20).

II.2.3. El ámbito subjetivo de protección de los periodistas parece amplio. Comprende no solo la protección de identidad de las fuentes (en sentido estricto), sino también la protección de los datos que permitan la identificación de la identidad de las fuentes. Por lo tanto, además del nombre, la protección también abarca dirección, voz y/o imagen. En la jurisprudencia del TEDH —siguiendo la Recomendación del Comité de Ministros del Consejo de Europa (2000)— se supone que, al identificar la información proporcionada por una fuente, debe tenerse consideración para con las circunstancias de hecho de adquirir información de una fuente por parte de un periodista, para con el contenido no publicado de la información proporcionada por una fuente a un periodista, y para con los datos personales de los periodistas y sus empleadores en relación con su labor profesional.

El marco sustantivo de la protección del secreto periodístico, expresado en la Recomendación y posteriormente adoptado en la jurisprudencia de Estrasburgo, si se determinase como un catálogo cerrado, sería insuficiente. En la era digital, la identificación de una fuente es posible en buena parte a través de varios análisis de los metadatos del proceso de comunicación. El uso del teléfono, Internet u otro medio de comunicación o difusión de información siempre deja una señal en la realidad virtual, como una huella digital, lo que permite identificar a la persona inmediatamente. En términos generales, el análisis de los metadatos puede conducir a la identificación de la persona que ha creado un archivo o de personas que se comunican entre sí.

Teniendo esto en cuenta, parece que, en la era digital, es necesario redefinir el alcance de la protección del privilegio periodístico para que incluya en él todos los datos utilizados en el proceso de comunicación, preparación, elaboración o recopilación de información que permita la identificación de un informante o un autor de un comunicado de prensa, incluso si dicha identificación requiere mucho tiempo y esfuerzo. Estos datos serían considerados como metadatos de telecomunicaciones (por ejemplo, de medición, datos de localización, números de IP) o contenidos en el código fuente de archivos (por ejemplo, la dirección o la ubicación geográfica del lugar donde se creó el archivo, los datos de los equipos que se utilizaron para crear el archivo).

B) La Constitución de la República de Polonia

II.3. En la Constitución polaca de 1997 —así como en la CEDH— la protección del secreto periodístico no se expresa directamente. Sin embargo, no crea un obstáculo para el Tribunal Constitucional, el cual puede interpretar las disposiciones ampliamente y de conformidad con las normas europeas. Se trata de una jurisprudencia constitucional bien establecida que el contenido normativo de la CEDH y la jurisprudencia del TEDH no pueden ser omitidos en el proceso de aplicación de la Constitución (Tribunal Constitucional de Polonia, 2012). De hecho, el nivel de protección de las libertades y derechos fundamentales es al menos el mismo. El punto de partida para el Tribunal Constitucional es la suposición de que la CEDH establece las normas mínimas y la Constitución polaca —como la ley suprema normativa de la República de Polonia (artículo 8 de la Constitución)— solo puede establecer estándares más altos, y no menores.

II.3.1. En el sistema jurídico de Polonia, la protección de la identidad de las fuentes se deriva de la libertad de prensa (artículo 14) y de la libertad —estrechamente relacionado con la primera— de adquirir y difundir información (artículo 54, párrafo 1 de la Constitución; Tribunal Constitucional de Polonia, 2001; 2006). Más aun, debe considerarse

vinculada a la protección de la vida privada (artículo 47) y a la autonomía informacional (artículo 51, párrafo 1 de la Constitución). Este enfoque también se confirmó en la sentencia del 30 de julio de 2014 del Tribunal Constitucional de Polonia.

El artículo 14 de la Constitución, es una de las principales reglas fundantes del sistema indicadas en el primer capítulo de la Constitución; expone los fundamentos del orden jurídico y del sistema jurídico de la República de Polonia. Su contenido es el siguiente: «La República de Polonia velará por la libertad de prensa y otros medios de comunicación social». La libertad para adquirir y difundir información, a su vez, se expresa directamente en el artículo 54, párrafo 1 de la Constitución. Esta disposición se establece en el capítulo sobre las libertades, los derechos y las obligaciones de las personas y los ciudadanos: «La libertad de expresar opiniones, adquirir y difundir la información estará garantizado a todas las personas». El enfoque del Tribunal en torno a las raíces de secreto periodístico está —más o menos— en consonancia con la presentada por el TEDH.

II.3.2. Se da un énfasis especial a la protección de la información adquirida por las personas que realizan las llamadas profesiones de fe pública en el ejercicio de sus actividades (Tribunal Constitucional de Polonia 2004, párrafo III.3; 2007, párrafo III.7; 2011, párrafo III. 6.4.). Aparte de las profesiones de médico o abogado, la profesión de periodista también es considerada como una de confianza pública. Los contactos entre dicha persona y otros individuos se basan en la confianza, no solo en las cualificaciones profesionales, sino también en la confidencialidad. Por lo tanto, la protección de la confidencialidad de la «información adquirida» —aunque no la protección de la «persona que adquiere la información»— es un requisito inmanente de un complejo de protección de la confianza, tanto en la dimensión individual como privada.

II.3.3. En mi opinión, la Constitución de la República de Polonia garantiza la libertad de silencio y la libertad de la divulgación de información como parte de la libertad de expresión (artículo 54, párrafo 1 de la Constitución). El Tribunal, sin embargo no trata el secreto profesional desde el punto de vista personal, como un privilegio del periodista, como lo hace el TEDH. El privilegio del periodista no es una «libertad negativa de un periodista». Se señaló claramente que todos los secretos profesionales son obligaciones legales y éticas de los sus depositarios (custodios), no un privilegio o derecho.

Desde el punto de vista constitucional, es admisible derogar el privilegio periodístico, si se hace al servicio de objetivos legítimos de un Estado democrático y de acuerdo con la regla de la proporcionalidad. La protección de la seguridad nacional y el orden público, del entorno natural, la salud o la moral públicas o los derechos y libertades de otras

personas (artículo 31, párrafo 3 de la Constitución) son considerados objetivos legítimos de un Estado democrático. Aunque el artículo 31, párrafo 3 de la Constitución parece estar redactado de una manera más general que el artículo 10, párrafo 2 de la CEDH, una norma para la injerencia en el secreto periodístico parece ser concurrente.

III. LA VIGILANCIA Y EL ALCANCE DE LA PROTECCIÓN PERIODÍSTICA

III.1. De acuerdo con la jurisprudencia establecida, solicitar a los periodistas renunciar a su derecho a guardar silencio y proporcionar información sobre sus fuentes o para obtener acceso a la información periodística interfiere con la libertad de expresión periodística (TEDH, 1996, párrafo 39; 2010b, párrafo 59; 2009c, párrafo 56).

III.2. El TEDH ha reconocido que llevar a cabo una búsqueda para poder identificar las fuentes periodísticas es más oneroso —desde el punto de vista de la protección del privilegio periodístico y la libertad de la prensa— que una orden oficial para entregar documentos o proporcionar información sobre la identidad de las fuentes (TEDH, 2003, párrafo 47; 2007c, párrafo 56; 2013b, párrafo 95). En consecuencia, en una situación así, un periodista es solo un observador pasivo de una búsqueda llevada a cabo por las autoridades públicas en su hogar o lugar de trabajo, mientras que en el caso de la orden judicial, él o ella podrían negarse a cooperar y decidir no revelar la identidad de sus fuentes.

En mi opinión, la interferencia con el privilegio periodístico por medio de la vigilancia es al menos tan onerosa —o incluso más onerosa para la privacidad y la libertad de prensa— como la inspección de una vivienda o un lugar de trabajo. Durante la vigilancia, los periodistas no solo son observadores pasivos, sino que ni siquiera saben de los controles, la adquisición o el análisis de los datos que son objeto de protección por el privilegio periodístico.

Tomando en cuenta lo anterior, las solicitudes de revelar ciertos documentos o identidades de las fuentes, así como la adquisición de este tipo de piezas de información por medio de la vigilancia sin el consentimiento del periodista, deben ser consideradas como interferencia con la protección que otorga el artículo 10 de la CEDH (la libertad de prensa y el privilegio periodístico). La posibilidad de utilizar estos métodos desencadena un efecto negativo no solo respecto del derecho al respeto de la vida y la correspondencia privada, concedida en virtud del artículo 8, sino también respecto de la libertad de expresión y la libertad de prensa (CEDH, artículo 10)[4].

4 En el caso Weber y Saravia contra Alemania, el TEDH consideró que el problema de la vigilancia de los periodistas y de las violaciones de su secreto profesional debía ser examinado desde el punto de

III.3. Teniendo en cuenta la importancia de las nuevas tecnologías en el reconocimiento efectivo, la prevención y la lucha contra los delitos, se debe asumir que una exclusión incondicional de la admisibilidad de la información clasificada adquirida por los periodistas conduce a dificultades en la obtención de pruebas en el caso de, por ejemplo, ciberdelitos, en los que los periodistas también pueden estar involucrados. Por lo tanto, hoy en día, el foco se ha puesto en favor del establecimiento de garantías procesales adecuadas que evadan el riesgo de revelar información protegida por la ley cuando no es necesario.

III.4. Como ya se mencionó, solo aquellos que proveen profesionalmente o regularmente a la opinión pública de información podrían considerarse como controladores sociales y pueden invocar el privilegio periodístico. El problema surge cuando quien es vigilado no es un periodista, sino un tercero (propietario de un servidor o un equipo en el que los datos de los periodistas están siendo almacenados, etcétera). Dificultades análogas se producen en el caso de la vigilancia masiva, la cual no se centra directamente en revelar las identidades de las fuentes, como se mencionó antes.

III.4.1. La sentencia del caso Weber y Saravia contra Alemania contiene alguna orientación sobre los requisitos que deberán cumplir las legislaciones nacionales en este sentido (TEDH, 2006). El Tribunal de Estrasburgo examinó, entre otras cosas, la violación del artículo 10 de la CEDH en lo que se refiere al uso del llamado seguimiento estratégico de las telecomunicaciones[5]. Uno de los demandantes en dicho asunto (un periodista) sostuvo que la posibilidad del seguimiento estratégico es, por sí misma, una injerencia en la libertad garantizada por el artículo 10 de la CEDH. El TEDH sostuvo que efectivamente se violó el artículo 10 de la CEDH, ya que la legislación alemana relativa a dicha forma de vigilancia no tenía el objetivo de revelar la identidad de las fuentes, sino luchar contra delitos graves. En otras palabras, el objetivo de la vigilancia en este caso no era superar el privilegio periodístico. Tal interferencia no puede describirse como «particularmente grave». Además, se han adoptado numerosas garantías procesales que garantizan la proporcionalidad de

vista del artículo 8 —garantizando el derecho a la protección de la vida y correspondencia privadas—, antes que desde la libertad de expresión contenida en el artículo 10 de la CEDH (TEDH, 2006). Mientras que en el caso de Telegraaf Media, el TEDH explicó que, a pesar de que las preguntas planteadas por las medidas de vigilancia suelen ser consideradas en virtud del artículo 8, en ese caso la cuestión como debía ser revisada en los artículos 8 y 10 al mismo tiempo (TEDH, 2012b).

5 Bajo las restricciones del secreto de correspondencia, correos y la Ley de Telecomunicaciones (llamada Ley G10), el seguimiento estratégico está dirigido a la recopilación de información mediante la interceptación de las telecomunicaciones con el fin de identificar y evitar peligros graves que enfrenta la República Federal de Alemania, como un ataque armado contra su territorio, la comisión de atentados terroristas internacionales y otros delitos graves. Por el contrario, la llamada vigilancia individual, es decir, la intervención de las telecomunicaciones de determinadas personas, sirve para prevenir o investigar ciertos delitos graves que las personas supervisadas son sospechosas de haber planificado o cometido.

los medios utilizados y la reducción de la divulgación de la identidad de las fuentes «a un mínimo inevitable».

Con el fin de evaluar si se ha producido una injerencia en la libertad de prensa incompatible con la CEDH, es necesario evaluar si la obtención de información tenía como objetivo divulgar las fuentes. Este razonamiento se confirma en el caso de Telegraaf Media y otros contra los Países Bajos (TEDH, 2012b). La denuncia fue presentada por un editor de periódicos holandeses y sus dos periodistas. Durante el procedimiento, los denunciantes dieron cuenta de que sus teléfonos estaban intervenidos y de que estaban siendo investigados por los servicios de inteligencia. El TEDH consideró que había habido una violación simultánea del artículo 8 y del artículo 10 de la CEDH. En primer lugar, la vigilancia específica de los periodistas se llevó a cabo con el fin de determinar de dónde habían obtenido su información. En segundo lugar, la vigilancia contra los solicitantes no había sido ordenada ni supervisada por un tribunal o una autoridad de la independencia e imparcialidad comparable. Los solicitantes solo podían presentar una queja *post factum*. Esto no es suficiente porque, en el caso de la revelación de las identidades de fuentes, la confianza en un periodista, una vez arruinada, no puede ser reconstruida.

III.4.2. Las garantías procesales que resultan en la protección del privilegio periodístico —según se indicaba en la jurisprudencia de Estrasburgo— deberán incluir disposiciones sobre la participación de la corte o un órgano independiente. . En su sentencia del caso Sanoma Uitgevers B.V. contra los Países Bajos, el Tribunal de Estrasburgo declaró lo siguiente:

> La primera y más importante de estas garantías es la garantía de revisión por parte de un juez o un órgano de decisión independiente e imparcial. […] La revisión requerida debe ser realizada por un órgano independiente del ejecutivo y otras partes interesadas, investido de la facultad para determinar si existe un requerimiento de primer orden en el interés público que anule el principio de protección de las fuentes periodísticas antes de que se haga entrega de dicho material, y para impedir el acceso innecesario a la información capaz de revelar la identidad de las fuentes si no existe tal requerimiento» (TEDH, 2010b, párrafo 90).[6]

6 Ver: Las sentencia del TEDH en Sanoma Uitgevers BV v las Netherland, párrafo 90.

IV. LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL DE 30 DE JULIO DE 2014

IV.1. El problema constitucional en el caso se debe a los niveles diferenciados de injerencia en el secreto profesional en el sistema jurídico polaco. Mientras que en un proceso penal, el legislador ha garantizado el secreto periodístico por las prohibiciones de pruebas (medios de prueba específicos), no ha establecido aún garantías cercanas para los procedimientos de obtención de información de una manera no revelada para fines de inteligencia operativa (por lo tanto, las actividades previas al juicio).

IV.2. El alcance legal de la protección del secreto periodístico en Polonia es el siguiente. De acuerdo con el artículo 180 del Código de Procedimiento Penal (CPC por sus siglas en inglés), los que están obligados a mantener el secreto profesional pueden negarse a declarar como testigos en el procedimiento sobre las circunstancias que se extienden a esta obligación. La decisión de utilizar el derecho pertenece al testigo, que está sujeto a la confidencialidad en virtud de las disposiciones aplicables al secreto profesional específico. En el caso de los periodistas, esta obligación se deriva del artículo 15 de la Ley del Derecho de Prensa. Esta protección se aplica plenamente a los documentos en poder de los periodistas, lo cual está, a su vez, determinado por el artículo 226 del CPC.

La protección legal del secreto profesional no es absoluta. Un fiscal o un tribunal pueden eximir de la obligación de secreto (artículo 180 *in fine* CPC). Dicha exención implica que no hay posibilidad de que el testigo evada dar testimonio debido a la obligación de reserva. Sobre la base del artículo 226 del CPC, esa regla también será aplicable a determinados documentos que contienen información protegida por el secreto. La exención de la obligación de secreto profesional es permisible solo cuando es necesario para el interés de la justicia, y cuando un hecho no puede determinarse sobre la base de otras pruebas (artículo 180, §2 del CPC). Sin embargo, en el caso de los periodistas, el legislador también ha introducido una restricción adicional. Un periodista no puede ser eximido de mantener la confidencialidad de los datos que permitan la identificación de un autor de material de prensa, una carta al director u otro material de esta naturaleza, así como la identificación de las personas que facilitan la información publicada o presentada para su publicación, si se reservan el derecho de no divulgación de sus datos (artículo 180, §3 del CPC). Los periodistas no tienen derecho a declararse bajo el privilegio periodístico si esta información se aplica a delitos graves que incluyen, entre otros, los delitos contra la República de Polonia (es decir, la traición o espionaje), contra las fuerzas de la vida y las fuerzas armadas, entre ellos los delitos de terrorismo.

En tales casos, no existe un derecho efectivo a permanecer en silencio e invocar privilegio periodístico.

IV.3. A su vez, el sistema jurídico polaco no ofrece garantías procesales con alcance similar en cuanto al procedimiento para la exención del secreto profesional, en el marco del proceso penal, que impida las infracciones sobre el secreto profesional. En particular, no hay supervisión imparcial judicial o fiscal u otro consecuente sobre el contenido de los materiales recogidos de una manera no revelada. El legislador no excluye ni minimiza el riesgo de que los agentes de policía o inteligencia dispongan —usando las medidas de vigilancia— de contenido al que normalmente no tendrían acceso o recibirían solo por orden de la corte o fiscal, emitida en un procedimiento distinto.

A la luz de la situación legal actual en Polonia, la protección de la confidencialidad de privilegio periodístico en realidad sigue dependiendo de los medios de comunicación con los informantes. En el caso en que un periodista utilice un teléfono o Internet, el alcance de la protección será drásticamente más estrecho que si el informante es contactado directamente, o por medio de las modernas tecnologías de procesamiento de datos.

Esto demuestra que el legislador polaco resulta ser inconsistente en mantenerse al ritmo de los cambios tecnológicos, como resultado de la difusión de la tecnología de comunicación a la distancia y de Internet. A pesar de la introducción de soluciones legislativas que permiten prestar servicios de seguridad para utilizar las nuevas tecnologías para combatir las amenazas a la seguridad y el orden público, no se establecieron las adecuadas garantías de los derechos fundamentales, incluida la libertad de expresión.

IV.4. En la sentencia del 30 de julio de 2014, el Tribunal dictaminó disposiciones sobre el control operativo en la medida en que no prevén una garantía de que los materiales que contengan información que fue prohibida como evidencia deben ser objeto de inmediata destrucción testificada, en el caso en que el tribunal no había levantado requisito de confidencialidad profesional —como incompatible con el artículo 42 (2), el artículo 47, el artículo 49, el artículo 51 (2) y el artículo 54 (1) en relación con el artículo 31 (3) de la Constitución—.

En opinión del Tribunal, el objetivo de la ley era asegurar que hubiese garantías procesales, en lugar de eliminar el acceso no autorizado a la información por las fuerzas policiales y los servicios de seguridad del Estado; dicha información debe ser protegida por la ley, debido a su contenido y las circunstancias en que fue transferida. Existe un determinado modelo de solución en el procedimiento criminal, según lo establecido en el artículo 180 (2) del Código de Procedimiento

Penal polaco. Dicha disposición autoriza a un tribunal a suprimir la obligación de secreto profesional, si esto es necesario para el beneficio de la administración de justicia, mientras que una determinada circunstancia no puede indicarse de una manera diferente, es decir, sin comprometer el secreto profesional. Un mecanismo similar podría estar en su lugar en lo que respecta a la vigilancia operacional. En la actualidad, no existe tal mecanismo. El legislador no ha previsto la obligación de verificar —bajo la supervisión de un tribunal determinado— los datos recogidos en el curso de la vigilancia operacional que podría contener información incluida en el ámbito del secreto profesional.

En resumen, el enfoque del Tribunal es más riguroso que el de la CEDH. Mientras que la CEDH requiere un control eficaz independiente sobre el ordenamiento de vigilancia, el Tribunal Constitucional requiere revisión independiente no solo antes, sino que exige la introducción de un control judicial después de la recolección de materiales, si solo tales materiales contienen potencialmente información de secreto profesional. Por lo tanto la corte debería poseer la facultar de evaluar toda la información y suprimir el secreto periodístico si es necesario.

V. DESAFÍOS PARA EL LEGISLADOR Y LA PRÁCTICA

La naturaleza de la participación de un tribunal o de un órgano independiente en el procedimiento relativo a la renuncia al derecho de los periodistas al secreto profesional no es tan obvia como parece a primera vista. A saber, la pregunta es si el consentimiento de un tribunal o una autoridad independiente es o no necesaria para la vigilancia y si, por separado —después de recoger el material—, un tribunal o una autoridad independiente debe verificar el material y emitir una decisión derogando el privilegio periodístico si el material contiene información que esté sujeta al secreto periodístico, o si el consentimiento antes de la vigilancia es suficiente, ya que cuenta con el consentimiento de la abrogación del privilegio.

Sin embargo, a pesar del hecho de que la sola existencia de una supervisión independiente del material recogido en el curso de la vigilancia secreta tiene muchas ventajas y permite una amplia protección del privilegio periodístico, en la práctica podría ser poco realista. En primer lugar, no siempre es posible evaluar, en el curso de la vigilancia, si el material recogido está sujeto a privilegio periodístico. En segundo lugar, no se puede perder de vista las limitaciones técnicas que puedan afectar a la posibilidad real de ejercer un control efectivo sobre el material recogido en el curso de la vigilancia.

Esto se aplica principalmente a los datos de telecomunicaciones, archivos de metadatos, así como las llamadas y otras formas de comunicación de la información recolectados durante la vigilancia indirecta. Los números de teléfono en sí, listas de llamadas o de metadatos de archivos —sin las herramientas informáticas adecuadas y los conocimientos operativos— no son suficientes para establecer, por ejemplo, las identidades de las fuentes o hechos relevantes de la vida del periodista. Por lo tanto, no está claro cómo y en qué medida un tribunal u órgano independiente evaluaría si el material adquirido está sujeto a privilegio periodístico o si la revocación del privilegio estaría justificada. Por otra parte, estos registros son generalmente grandes conjuntos de datos. Su cuidadoso análisis y la concesión de la autorización a la derogación del privilegio parecen casi imposibles de cumplir.

Por lo tanto, en mi opinión, en la era digital, el único camino para la protección del secreto periodístico necesario y factible es un juez u otro examen administrativo imparcial en el primer paso, cuando se ordena la vigilancia. Es decir, que conceda la autorización a una orden de vigilancia emitida por un tribunal u órgano independiente es suficiente para proteger la libertad de prensa. De hecho, este razonamiento es confirmado por las decisiones antes citadas en los casos Weber y Saravia y Telegraaf Media (TEDH, 2006; 2012b).

VI. BIBLIOGRAFÍA

Asamblea Parlamentaria del Consejo de Europa (2015a). Mass surveillance. Reporte de la Comisión de Asuntos Jurídicos y Derechos Humanos. Resolución provisional y recomendación provisional. 26 de enero de 2015.

Asamblea Parlamentaria del Consejo de Europa (2015b). Protection of the safety of journalists and of media freedom in Europe. Recomendación 2062 (2015). 29 de enero de 2015.

Bignami, Francesca E. (2007). Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law,* 8, 233-255.

Cate, Fred H. & otros (eds.) (2012). *Systematic Government Access to Private-Sector Data. International Data Privacy Law, 2 (4).*

Código de Procedimiento Penal (Polonia) (1997). Kodeks postępowania karnego.

Comité de Ministros del Consejo de Europa (2000). Recommendation R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information. 8 de marzo de 2000.

Dobbie, Mike (ed.) (2013). *Power, Protection & Principles. The State of Press Freedom in Australia 2013*. Redfern: Media, Entertainment & Arts Alliance. Recuperado el 26 de agosto de 2014 de http://issuu.com/meaa/docs/meaa_press_freedom_2013/1?e=1630650/2263927.

Kamiński, Ireneusz C. (2010). *Ograniczenia swobody dopuszczalne wypowiedzi w Europejskiej Konwencji Praw człowieka. Analiza krytyczna*. Varsovia: Wolters Kluwer.

NSA Insiders Reveal What Went Wrong (2014). *Consortiumnews.com, 7 de enero*. Recuperado de http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

Organización de las Naciones Unidas (ONU) (2014). El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. A/HRC/27/37.

Parlamento Europeo (2014a). Propuesta de Resolución del Parlamento Europeo sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior (2013/2188 (INI)). A7-0139/2014. Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior. 21 de febrero de 2014.

Parlamento Europeo (2014b). Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI).

Parlamento Europeo & Consejo de la Unión Europea (2006). Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. *Diario Oficial de la Unión Europea, L 105*, pp. 54-63.

Pearson, Siani & George Yee (eds.) (2013). *Privacy and Security for Cloud Computing*. Londres: Springer.

Rittinghouse, John W. & James F. Ransome (2010). *Cloud Computing: Implementation, Management, and Security*. Boca Raton: CRC Press.

Stalla-Bourdillon, Sophie (2014). Privacy versus security… Are we done yet? En Sophie Stalla-Bourdillon & otros, *Privacy vs. Security* (pp. 1-90). Londres/Heidelberg/Nueva York/Dordrecht: Springer.

Tribunal Constitucional de Polonia (2001). K 11/00. Sentencia. 4 de abril de 2001.

Tribunal Constitucional de Polonia (2004). SK 64/03. Sentencia. 22 de noviembre de 2004.

Tribunal Constitucional de Polonia (2005). Police Surveillance. K 32/04. Sentencia. 12 de diciembre de 2005.

Tribunal Constitucional de Polonia (2006). P 10/06. Sentencia. 30 de octubre de 2006.

Tribunal Constitucional de Polonia (2007). K 41/05. Sentencia. 2 de julio de 2007.

Tribunal Constitucional de Polonia (2011). K 33/08. Sentencia. 13 de diciembre de 2011.

Tribunal Constitucional de Polonia (2012). SK 3/12. Sentencia. 20 de noviembre de 2012.

Tribunal Constitucional de Polonia (2014). K 23/11. Sentencia. 30 de julio de 2014. No existe una versión oficial en inglés de la sentencia, tan solo existe un comunicado de prensa publicado después de la audiencia: Determining the catalogue of information on the individual, gathered by technical means in operational activities; rules for deleting obtained data. http://trybunal.gov.pl/en/news/press-releases/after-the-hearing/art/7005-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/. Fecha de consulta: 26 de agosto de 2014.

Tribunal Constitucional Federal Alemán (2010). 1 BvR 256/08. Sentencia. 2 de marzo de 2010.

Tribunal de Justicia de la Unión Europea (TJUE) (2014). Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung (C-594/12) y otros. Sentencia. 8 de abril de 2014.

Tribunal Europeo de Derechos Humanos (TEDH) (1978). Case of Klass and others v. Germany. Solicitud 5029/71. Sentencia. 6 de setiembre de 1978.

Tribunal Europeo de Derechos Humanos (TEDH) (1984). Case of Malone v. the United Kingdom. Solicitud 8691/79. Sentencia. 2 de agosto de 1984.

Tribunal Europeo de Derechos Humanos (TEDH) (1990). Case of Kruslin v. France. Solicitud 11801/85. Sentencia. 24 de abril de 1990.

Tribunal Europeo de Derechos Humanos (TEDH) (1992). Case of Open Door and Dublin Well Woman v. Ireland. Solicitud 14234/88; 14235/88. Sentencia. 29 de octubre de 1992.

Tribunal Europeo de Derechos Humanos (TEDH) (1996). Case of Goodwin v. the United Kingdom. Solicitud 17488/90. Sentencia. 27 marzo de 1996.

Tribunal Europeo de Derechos Humanos (TEDH) (1999). Case of Bladet Tromsø and Stensaas v. Norway. Solicitud 21980/93. Sentencia. 20 de mayo de 1999.

Tribunal Europeo de Derechos Humanos (TEDH) (2001). Case of P.G. and J.H. v. the United Kingdom. Solicitud 44787/98. Sentencia. 25 de setiembre de 2001.

Tribunal Europeo de Derechos Humanos (TEDH) (2003). Case of Roemen and Schmit v. Luxembourg. Solicitud 51772/99. Sentencia. 25 de febrero 2003.

Tribunal Europeo de Derechos Humanos (TEDH) (2005). Decision as to the admissibility of Application no. 40485/02 by Nordisk Film & TV A/S against Denmark. 8 de diciembre de 2005.

Tribunal Europeo de Derechos Humanos (TEDH) (2006). Decision as to the admissibility of Application no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany. 29 de junio de 2006.

Tribunal Europeo de Derechos Humanos (TEDH) (2007a). Affaire Heglas c. République Tchèque. Solicitud 5935/02. Sentencia. 1 de marzo de 2007.

Tribunal Europeo de Derechos Humanos (TEDH) (2007b). Case of the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria. Solicitud 62540/00. Sentencia. 28 de junio 2007.

Tribunal Europeo de Derechos Humanos (TEDH) (2007c). Case of Tillack v. Belgium. Solicitud 20477/05. Sentencia. 27 de noviembre de 2007.

Tribunal Europeo de Derechos Humanos (TEDH) (2009a). Case of Iordachi and others v. Moldova. Solicitud 25198/02. Sentencia. 10 de febrero de 2009.

Tribunal Europeo de Derechos Humanos (TEDH) (2009b). Case of Társaság a Szabadságjogokért v. Hungary. Solicitud 37374/05. Sentencia. 14 de abril de 2009.

Tribunal Europeo de Derechos Humanos (TEDH) (2009c). Case of Financial Times Ltd and others v. the United Kingdom. Solicitud 821/03. Sentencia. 15 de diciembre de 2009.

Tribunal Europeo de Derechos Humanos (TEDH) (2010a). Case of Uzun v. Germany. Solicitud 35623/05. Sentencia. 2 de septiembre 2010.

Tribunal Europeo de Derechos Humanos (TEDH) (2010b). Case of Sanoma Uitgevers B.V. v. the Netherlands. Solicitud 38224/03. Sentencia. 14 de septiembre 2010.

Tribunal Europeo de Derechos Humanos (TEDH) (2012a). Case of Hadzhiev v. Bulgaria. Solicitud 22373/04. Sentencia. 23 de octubre 2012.

Tribunal Europeo de Derechos Humanos (TEDH) (2012b). Case of Telegraaf Media Nederland Landelijke Media B.V. and others v. the Netherlands. Solicitud 39315/06. Sentencia. 22 de noviembre de 2012.

Tribunal Europeo de Derechos Humanos (TEDH) (2013a). Case of Youth Initiative for Human Rights v. Serbia. Solicitud 48135/06. Sentencia. 25 de junio de 2013.

Tribunal Europeo de Derechos Humanos (TEDH) (2013b). Case of Nagla v. Latvia. Solicitud 73469/10. Sentencia. 16 de julio de 2013.

Xu, Jennifer & otros (2004). Analyzing and Visualizing Criminal Network Dynamics: A Case Study. En Hsinchun Chen & otros (eds.), *Intelligence and Security Informatics* (pp. 359-377). Berlín/Heidelberg: Springer.

Zittrain, Jonathan L. (2008). *The Future of the Internet and How to Stop It*. New Haven/Londres: Yale University Press/Penguin UK.

Recibido: 08/09/2015
Aprobado: 15/10/2015