Esther Salamanca Aguado
Doctora y profesora de la Universidad de Valladolid. Facultad de CC. Sociales, Jurídicas y de la Comunicación. Campus María Zambrano de Segovia.
Correo: festher_salamanca@yahoo.com

- Artículo recibido: Septiembre de 2014.
- Artículo aceptado: Octubre de 2014.

EL RESPETO A LA VIDA PRIVADA Y A LA PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO DE LA VIGILANCIA MASIVA DE COMUNICACIONES

Resumen

La información filtrada por Edward Snowden, sobre el uso por los Estados Unidos de América y el Reino Unido de tecnologías que permiten la captura indiscriminada de grandes cantidades de datos de comunicación ha suscitado en toda Europa una gran inquietud y un debate sobre el impacto de los programas de vigilancia masiva de comunicaciones en los derechos humanos. Según la jurisprudencia del Tribunal Europeo de Derechos Humanos, ese tipo de actividades suponen una injerencia en la vida privada de miles de ciudadanos europeos. El presente artículo analiza las garantías que el artículo 8 del Convenio Europeo de Derechos Humanos ofrece para que dicha injerencia esté justificada y valora si dichas salvaguardas son suficientes en los casos de una vigilancia extraterritorial. También plantea si los Estados miembros del Convenio están obligados a adoptar medidas para proteger a sus ciudadanos de la vigilancia contraria a los requisitos establecidos.

Palabras clave

Derecho al respeto de la vida privada, derecho a la protección de datos, vigilancia masiva de comunicaciones, obligaciones positivas, seguridad nacional

Abstract

The information leaked by Edward Snowden, on the use by the United States and the United Kingdom of technologies that allow the indiscriminate capture of large amounts of data communications has caused great concern across Europe and it has opened a debate on the impact of programs of mass surveillance of communications on human rights. According to the jurisprudence of the European Court of Human Rights, such activities are interference in the private lives of thousands of European citizens. This article analyzes the guarantees that Article 8 of the European Convention on Human Rights provides for such interference and it assesses whether these safeguards are sufficient in the case of extraterritorial surveillance. It also asks whether the member States of the Convention are obliged to take measures to protect their citizens from the surveillance contrary to the requirements.

Keywords

Right to privacy, right to data protection, mass surveillance, positive obligations, national security

Este trabajo ha sido realizado en el marco del proyecto de investigación: "El diálogo judicial multinivel en Espacio Europeo Multinivel: Las relaciones del TJUE con los tribunales constitucionales, el TEDH y otros tribunales internacionales" (DER 2012-36703) Plan Nacional de I+D+I (2004-2007), Ministerio de Ciencia y Tecnología. Investigador principal: Dr. José Martín y Pérez de Nanclares (Universidad de Salamanca).

EL RESPETO A LA VIDA PRIVADA Y A LA PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO DE LA VIGILANCIA MASIVA DE COMUNICACIONES

1. LOS PROGRAMAS DE VIGILANCIA MASIVA DE COMUNICACIONES Y SU IMPACTO EN EL EJERCICIO DE LOS DERECHOS HUMANOS

En un momento en que la amenaza de nuevos atentados terroristas se cierne sobre Europa, la divulgación de programas secretos de vigilancia[1] destinados a la lucha contra el terrorismo y a la defensa de la seguridad nacional ha abierto un debate a escala global sobre sus consecuencias en la esfera de los derechos humanos[2] y ha puesto en evidencia que, en la mayoría de los Estados, los marcos normativos son inadecuados. Tampoco están claras las vías de protección internacional de derechos como el derecho al respeto a la vida privada o la protección de datos personales, debido, principalmente, al componente de extraterritorialidad que caracterizan dichas actividades.[3] Es un hecho que los Estados no habían tenido nunca la capacidad de que

1 Se trata de los programas de vigilancia de la NSA (Agencia de Seguridad Nacional de Estados Unidos) y del GCHQ (Cuartel General de Comunicaciones del Gobierno del Reino Unido): PRISM, XKeyscore, Bullrun, MUSCULAR, Tempora y Edgehill. Sobre los detalles de los mismos véase BOWDEN, C. *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Study for the European Parliament, PE 474.405, Brussels: September 2013.

2 Sobre la protección de los derechos humanos en la lucha contra el terrorismo existe abundante bibliografía, véase, en particular, PÉREZ GONZÁLEZ, M., "Derechos humanos y lucha contra el terrorismo", en A. Pastor Palomar (coord.), C. Escobar (dir.), Los derechos humanos en la sociedad internacional del siglo XXI, Madrid: Escuela Diplomática, 2009, pp. 39-62; COSTAS TRASCASAS, M., "Seguridad nacional y derechos humanos en la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) en materia de terrorismo internacional: ¿hacia un nuevo equilibrio?", E. Conde Pérez (dir.), Terrorismo y legalidad internacional, Madrid: Dykinson, 2012, pp. 187-207; CORNAGO PRIETO, N., "Lucha contra el terrorismo y derechos humanos", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz* 2009, 2010, pp. 347-361; SHEININ, M. (coord.), "European and United States Counter-Terrorism Policies, the rule of law and Human Rights", RSCAS Policy Papers 2011/03, European University Institute, 2011; COUNCIL OF EUROPE, Human Rights and the fight against terrorism: the Council of Europe guidelines, Strasbourg: Council of Europe Publishing, 2005.

3 Véanse las conclusiones del Relator Especial de Naciones Unidas para la Libertad de opinión y de expresión (Frank La Rue) en su *Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40 y los informes del Relator Especial sobre la

disponen actualmente para realizar actividades de vigilancia simultáneas, invasivas, con objetivos precisos y a gran escala".[4]

Tras las primeras revelaciones de Edward Snowden, ex administrador de sistemas de la Agencia de Seguridad Nacional de Estados Unidos (NSA),[5] los relatores especiales para la protección del derecho a la libertad de opinión y de expresión de Naciones Unidas y de la Organización de Estados Americanos manifestaron, en una declaración conjunta, "su preocupación por la existencia de programas y prácticas de seguridad que pueden generar un perjuicio serio a los derechos a la intimidad y a la libertad de pensamiento y expresión", y en la que "instan a las autoridades correspondientes a que revisen la legislación pertinente y modifiquen sus prácticas, con la finalidad de asegurar su adecuación a los principios internacionales en materia de derechos humanos".[6]

promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo (Martin SCheinin), en los que ya se pone de manifiesto que "la mayoría de las leyes antiterroristas promulgadas desde los acontecimientos del 11 de septiembre de 2001 se han centrado en ampliar el poder de vigilancia de los gobiernos", y que según los Estados "al ser el terrorismo una actividad mundial, la búsqueda de terroristas debe realizarse también más allá de las fronteras nacionales, con ayuda de terceras partes que dispongan de información abundante sobre ciertos individuos, que se pueda utilizar como recurso para identificar y vigilar a terroristas sospechosos", A/HRC/13/37, 28 de diciembre de 2009, párr. 20. Véase igualmente la "Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión, A/HRC/14/46, 17 de mayo de 2010 y los Principios Globales sobre seguridad nacional y derecho de la información ("Los Principios Tshwane") emitidos el 12 de junio de 2013.

4 A/HRC/23/40, párr. 33.

5 Véanse los artículos publicados en *The Guardian y The Washington Post*, entre junio y agosto de 2013, entre otros, "NSA collecting phone records of millions of Verizon customers daily", Glenn Greenwald , The Guardian, Thursday 6 June 2013; "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", Barton Gellman and Laura Poitras, The Washington Post, June 7, 2013; "NSA Prism program taps in to user data of Apple, Google and others", Glenn Greenwald and Ewen MacAskill, The Guardian, 7 June 2013; "UK gathering intelligence via covert NSA operation", Nick Hopkins, The Guardian, 7 June 2013; "GCHQ tapped fibre optic cables for data, says newspaper", The Guardian, 22 June 2013; "GCHQ taps fibre optic cables for secret access to world's communications", Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, The Guardian, 21 June 2013; "The legal loopholes that allow GCHQ to spy on the world", Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, The Guardian, 21 June 2013; "GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency", Nick Hopkins, Julian Borger and Luke Harding, The Guardian, 1 August 2013; "BT and Vodafone among telecoms companies passing details to GCHQ", James Ball, Luke Harding and Juliette Garside, The Guardian, 2 August 2013.

6 *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*, 21 de junio de 2013, (disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&).

A raíz de la preocupación expresada por los Estados Miembros de Naciones Unidas por las repercusiones negativas de esas prácticas de vigilancia para los derechos humanos, el 18 de diciembre de 2013 la Asamblea General aprobó, sin votación, su resolución 68/167, "sobre el derecho a la privacidad en la era digital". En la resolución, que fue copatrocinada por 57 Estados Miembros, la Asamblea afirmó que los derechos de las personas también debían estar protegidos en Internet, y exhortó a todos los Estados a respetar y proteger el derecho a la privacidad en las comunicaciones digitales. También a que examinaran sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, haciendo hincapié en la necesidad de que los Estados velasen por que se dé cumplimiento pleno y efectivo a sus obligaciones, en virtud del derecho internacional de los derechos humanos.[7]

En el marco de la Unión Europea, las revelaciones producidas desde junio de 2013 han suscitado gran inquietud[8] y están teniendo especial trascendencia política y jurídica.[9] El Parlamento Europeo (PE) aprobó el 4 de julio de 2013 una resolución en

7 "El derecho a la privacidad en la era digital", A/RES/68/167, 21 de enero de 2014. Véase también el *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, "El derecho a la privacidad en la era digital", A/HRC/27/37, 30 de junio de 2014. Véase, además, AKRIVOPOULOU, CH. (ed.), *Human rights and risks in the digital era: globalization and the effects of information technologies,* Hershey, PA: Information Science Reference, 2012; KLANG. M/ MURRAY, A. *Human rights in the digital age,* London; Portland, Or.; GlassHouse, 2005; DAVIS, F. *Surveillance, counter-terrorism and comparative constitutionalism,* Abingdon, Oxon: Routledege, 2014 (especialmente páginas 93 a 152).

8 Véase el *Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, 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*. ("Informe Moraes") A7-0139/2014, 21.2.2014.

9 Véanse las Declaraciones de 10 de junio de 2013 de la Vicepresidenta de la Comisión Europea, Viviane Reding, exigiendo explicaciones al gobierno de los Estados Unidos sobre el programa PRISM y las declaraciones posteriores: "Mass surveillance is unacceptable – U.S. action to restore trust is needed now", 9 December 2013 (SPEECH/13/1048); "Protecting EU citizens' data from mass surveillance", 11 March 2014 (SPEECH/14/209). Véase, también la declaración del Supervisor Europeo de Protección de Datos (EDPS) sobre la necesidad de restaurar la confianza entre Estados Unidos y la Unión Europea en la transferencia de datos: "EDPS: Enforcing EU data protection law essential for rebuilding trust between EU-US", 21 february 2014 (EDPS/2014/04). Véanse también el *Report of 27 November 2013 on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection,* 16987/13 y las comunicaciones presentadas por la Comisión Europea el 27 de noviembre de 2013: *Communication from the Commision to the European Parliament and the Council: Rebuilding trust in EU-UE data flows*, COM (2013) 846 final; *Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU,* COM (2013) 847 final; *Communication from the Commission to the European Parliament and the Council on the joint report from the Commission and the US Treasury Department regarding the value of TFTP provided data,* COM (2013) 843 final. Se puede consultar también el Informe Anual de 2013 de la Agencia Europea de Derechos Fundamentales, Fundamental

la que encargaba a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE), que llevara a cabo una investigación exhaustiva.[10] En su informe de 21 de febrero de 2014 ("Informe Moraes"), la Comisión LIBE considera probada:

"la existencia de sistemas tecnológicamente muy avanzados, complejos y de amplio alcance diseñados por los servicios de inteligencia de los Estados Unidos y de algunos Estados miembros, para recopilar, almacenar y analizar datos de comunicaciones, incluidos datos de contenido y datos y metadatos de localización de todos los ciudadanos en todo el mundo a una escala sin precedentes y de una manera indiscriminada y no basada en sospechas".[11]

Entre sus recomendaciones, pide a los Estados miembros de la UE que prohíban las actividades de vigilancia masiva generalizada y que se aseguren de que todos sus marcos legislativos y mecanismos de control actuales y futuros por las que se rigen las actividades de los servicios de inteligencia se atengan a los estándares del Convenio Europeo de Derechos Humanos (CEDH) y a la legislación en materia de protección de datos de la Unión Europea.[12]

El asunto *Big Brother Watch y otros contra Reino Unido*[13] es la primera demanda presentada ante el Tribunal Europeo de Derechos Humanos (TEDH) que tiene su origen en la información filtrada por Edward Snowden, sobre el uso por los Estados Unidos de América y el Reino Unido de tecnologías que permiten la captura indiscriminada de grandes cantidades de datos de comunicación y su intercambio entre los dos Estados.[14] Los demandantes alegan

rights: challenges and achievements in 2013, el capítulo que lleva por título "Information society, respect for private life and data protection", pp. 81 -100.

10 Resolución de 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE, el PE encargó a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior [P7_TA-PROV (2013)0322].

11 A7-0139/2014 (1ª Conclusión). Se refiere, en concreto, a los programas de inteligencia de la Agencia Nacional de Seguridad estadounidense que permiten la vigilancia masiva de ciudadanos de la UE mediante un acceso directo a los servidores centrales de empresas estadounidenses líderes en Internet (programa PRISM); el análisis de contenido y metadatos (programa Xkeyscore); la elusión del cifrado en línea (BULLRUN); el acceso a redes informáticas y telefónicas y el acceso a los datos de localización, así como algunos sistemas de la agencia de inteligencia británica GCHQ, como por ejemplo la actividad preliminar de vigilancia (programa Tempora), el programa de descifrado (Edgehill; los ataques selectivos con intermediarios contra sistemas de información (programas Quantumtheory y Foxacid) y la recopilación y retención de 200 millones de mensajes de texto al día (programa Dishfire). Ibíd. 2ª Conclusión.

12 *Ibíd.* 22ª, 23ª y 27ª Conclusiones.

13 Application no. 58170/13 presentada el 4 de septiembre de 2013 y comunicada al gobierno del Reino Unido el 9 de enero de 2014. Los demandantes son las ONG británicas *Big Brother Watch, English Pen y Open Rights Group*, junto a la activista alemana Dr. Constanze Kurz.

14 En concreto, se hace referencia a los programas PRISM Y TEMPORA.

que es probable que hayan sido objeto de una vigilancia genérica por el Cuartel General de Comunicaciones del Gobierno del Reino Unido (GCHQ) y que los servicios de seguridad del Reino Unido pueden haber accedido a información interceptada por servicios de inteligencia extranjeros relacionada con sus comunicaciones electrónicas. Los demandantes sostienen que ha existido una injerencia no prevista por la ley en sus derechos garantizados por el artículo 8 del CEDH.[15]

El objeto de nuestro trabajo no es analizar en profundidad los términos de esta demanda; tampoco anticipar los posibles argumentos que pueda esgrimir el TEDH. Más bien, nos proponemos esclarecer cuales son los estándares mínimos de protección que exige el artículo 8 del CEDH y su adecuación a las nuevas circunstancias derivadas de la vigilancia masiva (nacional y extraterritorial) de las comunicaciones. Nos ocuparemos, en primer lugar, del alcance del derecho al respeto de la vida privada y del derecho a la protección de datos personales en dicho contexto, prestando especial atención a las condiciones que se exigen para limitar el ejercicio de estos derechos. Es decir, cualquier injerencia en estos derechos debe estar prevista por la ley, perseguir un fin legítimo y ser necesaria en una sociedad democrática. En segundo lugar, plantearemos la cuestión de si los Estados miembros del CEDH están obligados a adoptar medidas para proteger a sus ciudadanos de la vigilancia extraterritorial realizada por terceros Estados y contraria a los requisitos establecidos.

15 En su opinión, no hay ninguna base en el derecho interno para la recepción de información de las agencias de inteligencia extranjeras. Se denuncia la ausencia de control legislativo y de garantías en relación con las circunstancias en las que los servicios de inteligencia del Reino Unido pueden solicitar a los servicios de inteligencia extranjeros la interceptación de comunicaciones para dar acceso a los datos almacenados por el Reino Unido, obtenidos por la interceptación, y el grado en que los servicios de inteligencia británica pueden utilizar, analizar, difundir y almacenar los datos solicitados o recibidos de las agencias de inteligencia extranjeras y el proceso por el cual estos datos deben ser destruidos. Además, en relación a la interceptación de las comunicaciones directamente por el GCHQ, los demandantes alegan que el régimen legal aplicable a las órdenes de comunicaciones externas no cumple con los estándares mínimos establecidos por el Tribunal en su jurisprudencia. Por último, sostienen que la interceptación genérica de las comunicaciones por el GCHQ, simplemente sobre la base de que dichas comunicaciones han sido transmitidos a través de cables de fibra óptica transatlánticos, es una injerencia intrínsecamente desproporcionada con la vida privada de millones de personas, *Fourth Section, Application no. 58170/13, Big Brother Watch and others against the United Kingdom lodged on 4 September 2013. Statement of facts*, (disponible en, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713#{"itemid":["001-140713"]}).

2. DERECHOS GARANTIZADOS POR EL ARTÍCULO 8 DEL CEDH

El derecho internacional de los derechos humanos no solo reconoce el derecho al respeto de la vida privada y familiar como un derecho humano fundamental,[16] sino que también se le considera un derecho humano que sirve de apoyo a otros derechos humanos y forma la base de toda sociedad democrática.[17] En virtud del mismo, toda persona tiene derecho a ser protegida respecto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o sus comunicaciones, así como de ataques ilegales a su honra y reputación. Este derecho debe estar garantizado respecto de todas esas injerencias y ataques, provengan de las autoridades estatales o de personas físicas o jurídicas. Por lo tanto, el Estado está obligado a adoptar medidas legislativas y de otra índole para hacer efectiva la prohibición de esas injerencias y ataques.[18]

El desarrollo de la tecnología de la información y el aumento de la capacidad informática han permitido formas inimaginables de reunir, almacenar e intercambiar datos personales. Se han desarrollado así, principios internacionales de protección de datos fundamentales al amparo de la protección del derecho a la vida privada.[19] Entre estos principios figuran la obligación de obtener la información personal por

16 En la Declaración Universal de los Derechos Humanos (art. 12), en el Pacto Internacional de Derechos Civiles y Políticos (art. 17), en la Convención de los Derechos del Niño (art. 16), en la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares (art. 14), en la Convención Americana sobre Derechos Humanos (art. 11), en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (art. 8) y en la Carta de Derechos Fundamentales de la Unión Europea (art. 7).

17 A/HRC/13/37, p. 6.

18 Comité de Derechos Humanos, *Observación General Nº 16*, párr. 1. Por lo que se refiere al *derecho al respeto de las comunicaciones*, tres son los requisitos que determinan su ejercicio. En primer lugar, el carácter privado, es decir: que las personas sean capaces de intercambiar información e ideas en un espacio que está más allá del alcance de los otros miembros de la sociedad, del sector privado, y en última instancia, del propio Estado. En segundo lugar, el carácter seguro de las comunicaciones, vinculado a que las personas sean capaces de verificar que sus comunicaciones se reciben únicamente por sus destinatarios, sin interferencia o alteración, y que las comunicaciones que reciben son igualmente libres de la intrusión. Por último, el carácter anónimo de las comunicaciones, es decir: el anonimato, si se desea, permite a las personas expresarse libremente sin temor a represalias o condenas. A/HRC/23/40, párr. 23.

19 *Observación General*, Nº 16, "La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto", párr. 10. Véase también, Council of Europe, Research Division. *Internet: case law of the European Court of Human Rights*, 2011.

procedimientos legales y justos; limitar el ámbito de su uso a los fines inicialmente especificados; asegurar un tratamiento adecuado, pertinente y no excesivo; garantizar su exactitud; mantenerla en seguridad; suprimirla cuando deja de ser necesaria y garantizar al individuo el derecho de acceder a los datos sobre su persona y a solicitar las correcciones oportunas.[20]

En el sistema regional europeo de protección de derechos humanos se reconoce, junto al derecho fundamental del respeto a la vida privada, el derecho a la protección de los datos de carácter personal y el TEDH ha desarrollado al respecto una sólida jurisprudencia al amparo del artículo 8 del CEDH.[21]

2.1. El derecho al respeto de la vida privada

El derecho de toda persona a la vida privada y familiar, así como de su domicilio y de su correspondencia se encuentra protegido por el artículo 8 del CEDH. Por lo que se refiere al ámbito de la vida privada,[22] el TEDH ha interpretado de forma amplia

20 Véanse las *Directrices sobre la protección de la intimidad y de los flujos transfronterizos de datos personales* (1980) de la Organización de Cooperación y Desarrollo Económicos; y los *Principios rectores para la reglamentación de los ficheros computadorizados de datos personales* (resolución 45/95 de la Asamblea General y E/CN.4/1990/72).

21 Los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconocen el respeto de la vida privada y la protección de los datos de carácter personal como derechos fundamentales estrechamente relacionados, pero independientes. Por su parte, el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos.

22 El TEDH ha declarado reiteradamente que "la vida privada es un término amplio no susceptible de una definición exhaustiva. Aspectos como identidad de género, nombre, orientación y vida sexual, son elementos importantes de la esfera personal protegidos por el artículo 8. El artículo protege también el derecho a la identidad y al desarrollo personal, y el derecho a establecer y desarrollar relaciones con otras personas y con el mundo exterior y puede incluir actividades de naturaleza profesional o comercial. Por lo tanto, existe una zona de interacción de una persona con las otras, incluso en un contexto público, que puede entrar en el ámbito de «vida privada»", *Caso Perry c. Reino Unido*. Sentencia de 17 de julio de 2003, ap. 36. Véase también el *Caso Niemietz c. Alemania*. Sentencia de 16 de diciembre de 1992, ap. 29; *Caso Peck. c. Reino Unido*. Sentencia de 28 de enero de 2003, ap. 57. Sobre el concepto de vida privada, véanse, en particular, Rubenfeld, J. «The Right of Privacy», *Harvard Law Review*, 1989, vol. 102, p. 737; De Schutter, O. «La vie privée entre droit de la personnalité et liberté», *Revue trimestrielle des droits de l'homme*, 1999, p. 827; Wachsmann, P. «Le droit au secret de la vie privé», en Sudre F.: *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 119, y Rigaux, F.: «La protection de la vie privée en Europe», *en Le droit commun de l'Europe et l'avenir de l'enseignement juridique*, de Witte B. y Forder, C., eds., Metro, Kluwer, 1992, p. 185.

el artículo 8, entendiendo que las nociones de «vida privada» y «correspondencia» incluyen las comunicaciones por teléfono, fax o correo electrónico.[23] Así mismo, ha considerado que la información derivada del seguimiento del uso personal de Internet,[24] el almacenamiento en un registro secreto y la comunicación de datos relativos a la vida privada de un individuo entran en el campo de aplicación del artículo 8.[25]

El CEDH recoge, asimismo, la posibilidad de limitar el ejercicio de este derecho en el párrafo segundo del artículo 8:

"No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

En el contexto de la interceptación de comunicaciones por los servicios de inteligencia, el TEDH ha considerado que el poder de vigilar en secreto a los ciudadanos, característico del Estado policial, sólo es tolerable conforme al CEDH como medida estrictamente necesaria en la salvaguarda de las instituciones democráticas. En el caso *Klass y otros contra Alemania*, el TEDH reconoció que un Estado democrático "debe ser capaz de vigilar en secreto a los elementos subversivos que operan en su territorio". Y reconoció que el legislador nacional disfruta de un cierto poder discrecional, aunque éste no es ilimitado, ya que "consciente del peligro de minar, de ver destruir la democracia con el motivo de defenderla (…) no podrían tomar, en nombre de la lucha contra el espionaje y el terrorismo, cualquier medida que juzguen apropiadas". Por este motivo, cualquiera que sea el sistema de vigilancia adoptado, el Tribunal debe convencerse de que existen garantías adecuadas y suficientes contra los abusos.[26]

En el caso de autos, los demandantes (nacionales alemanes) no rebatían el derecho del Estado a recurrir a las medidas de vigilancia secreta previstas por la legislación interna ("G 10"[27]), pero consideraban que esta última, al permitir estas medidas sin

23 *Caso Liberty y otros contra Reino Unido*. Sentencia de 1 julio 2008, apdo. 57. Véase también *Weber y Saravia contra Alemania*. Sentencia de 29 junio 2006, apdo. 77; *Caso Klass y otros contra Alemania*. Sentencia de 6 septiembre 1978, apdo. 41; *Caso Malone c. Reino Unido*. Sentencia de 2 de agosto de 1984, apdo. 64; *Caso Valenzuela Contreras contra España.* Sentencia de 30 de julio de 1998, apdo. 64.

24 *Caso Copland contra Reino Unido*. Sentencia de 3 abril 2007, apdo. 41.

25 *Caso Rotaru contra Rumanía*. Sentencia de 4 mayo 2000, apdo. 43; *Caso Leander contra Suecia*. Sentencia de 26 de marzo de 1987, apdo. 48.

26 *Caso Klass y otros contra Alemania*. Sentencia de 6 septiembre 1978, apdos. 42, 48, 49 y 50.

27 Ley de 13 de agosto de 1978, relativa a la restricción del secreto de la correspondencia, de los envíos postales y de las telecomunicaciones, promulgada en virtud del artículo 10.2 de la Ley Fundamental.

obligar a las autoridades a avisar *a posteriori*, y en todos los casos a los interesados y por excluir cualquier recurso a los tribunales contra la adopción y ejecución de medidas semejantes violaba el artículo 8. Examinada dicha legislación y su interpretación por el Tribunal Constitucional Federal alemán, el TEDH juzgó inherente al sistema del CEDH una cierta forma de conciliación entre los imperativos de la defensa de la sociedad democrática y aquellos otros de la salvaguarda de los derechos individuales. En el contexto del artículo 8, esto significa "que hay que buscar un equilibrio entre el ejercicio por el individuo del derecho que le garantiza el párrafo 1 y la necesidad, según el párrafo 2, de imponer una vigilancia secreta para proteger a la sociedad democrática en su conjunto".[28] Finalmente, el TEDH consideró la injerencia resultante de la legislación alemana en el ejercicio del derecho consagrado por el artículo 8, como necesaria en una sociedad democrática, para la seguridad nacional, la defensa del orden y la prevención de los delitos.[29]

Con posterioridad, la legislación alemana que permite la vigilancia secreta de las comunicaciones por el Servicio Federal de Inteligencia fue examinada de nuevo por el TEDH, al amparo del artículo 8.[30] En el asunto *Weber y Saravia c. Alemania*, el Tribunal se ocupa por primera vez de lo que denomina "vigilancia estratégica generalizada" (*strategic monitoring*), así como la obtención de datos personales y su transmisión a otras autoridades.[31] En primer lugar, afirma que la mera existencia de una legislación que autoriza un sistema para la vigilancia secreta de las telecomunicaciones implica una amenaza de control para todos aquellos susceptibles de que se les aplique la legislación. Esta amenaza lesiona necesariamente la libertad de comunicación entre los usuarios de los servicios de telecomunicaciones y constituye una injerencia en el ejercicio de los derechos de las demandantes, en virtud del artículo 8.[32] Esta consideración la encontramos de nuevo, dos años más tarde, en el caso *Liberty y otros c. Reino Unido*[33] en el que el TEDH juzga si la legislación inglesa aplicable en los años 90

28 *Caso Klass y otros contra Alemania,* apdo. 59.

29 *Ibíd.,* apdo. 60.

30 "G 10" modificada por la Ley de lucha contra la criminalidad, de 28 de octubre de 1994. El 29 de junio de 2001 entró en vigor una nueva versión de la ley G 10 y la ley de 1994 dejó de aplicarse.

31 "Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences (see in detail "Relevant domestic law and practice" below, paragraphs 18 *et seq.*). In contrast, so-called individual monitoring, that is, the interception of telecommunications of specific persons, serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed". *Caso Weber and Saravia v. Germany*, apdo. 4.

32 *Caso Weber and Saravia c. Alemania*, ap. 78. Véase también *Caso Klass y otros contra Alemania*, apdo. 41 y *Caso Malone c. Reino Unido*, apdo. 64.

33 *Caso Liberty y otros c. Reino Unido*. Sentencia de 1 julio 2008, apdo. 56.

y que permitía, a través de una Utilidad de Prueba Electrónica (*Electronic Test Facility* «ETF»), interceptar 10.000 canales telefónicos simultáneos desde Dublín a Londres y al continente, cumplía las salvaguardas del artículo 8.[34]

En ambos asuntos, el TEDH examina -aunque con distinto resultado- si tal injerencia está justificada, es decir: si cumple los requisitos del párrafo 2 del artículo 8: estar "prevista por la ley", perseguir uno o más de los fines legítimos a los que hace referencia el apartado 2 y ser «necesaria en una sociedad democrática» al objeto de lograr dichos fines.[35]

2.1.1. *Previsibilidad de la ley*

La expresión «prevista por la Ley» requiere no sólo que la medida de vigilancia impugnada tenga alguna base en el derecho interno, sino que se refiere también a la calidad de la ley en cuestión, exigiendo "que sea compatible con la preeminencia del derecho y accesible a la persona afectada quien, además, ha de poder prever sus consecuencias".[36] En el contexto particular de las medidas secretas de vigilancia la previsibilidad no significa que una persona pueda prever cuándo es probable que las autoridades intercepten sus comunicaciones para adaptar su comportamiento en consecuencia; sino que, para evitar la arbitrariedad del Estado, y dado el carácter secreto de las medidas, "el derecho interno ha de emplear términos claros para indicar a todos de manera suficiente en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas".[37] Además, "ha de indicar el alcance y las modalidades de ejercicio de dicha facultad con suficiente claridad –teniendo en

34 Durante el período en cuestión la legislación aplicable eran los artículos 1-10 de la *Interception of Communications Act* 1985 («la Ley de 1985»), que entró en vigor el 10 de abril de 1986 y fue derogada por la *Regulation of Investigatory Powers Act* 2000 (Ley de Regulación de las Facultades de Investigación «la Ley de 2000»). La Ley de 2000 entró en vigor el 15 de diciembre de 2000. La memoria explicativa describía que el objetivo principal de la Ley era asegurar que las facultades de investigación pertinentes se usaran de conformidad con los derechos humanos. En cuanto a la intervención de las comunicaciones, la Ley de 2000 derogó, entre otros, los artículos 1-10 de la Ley de 1985, estableciendo un nuevo régimen para la intervención de las telecomunicaciones.

35 *Caso Weber and Saravia c. Alemania,* apdo. 80 -138; *Caso Liberty c. Reino Unido*, apdo. 58 – 70.

36 *Caso Weber and Saravia c. Alemania,* apdo. 84. Ver, entre otros, *Caso Kruslin contra Francia.* Sentencia de 24 abril 1990, apdo. 27; *Caso Huvig contra Francia.* Sentencia de 24 abril 1990, apdo. 26; *Caso Lambert contra Francia*. Sentencia de 24 agosto 1998, ap. 23; *Caso Perry contra Reino Unido*, apdo. 45; *Caso Dumitru Popescu contra Rumania.* Sentencia de 26 abril 2007, apdo. 61.

37 *Caso Weber and Saravia c. Alemania,* apdo. 93.

cuenta la legítima finalidad que se persigue– para facilitar así al individuo la adecuada protección contra las injerencias arbitrarias".[38]

En reiterada jurisprudencia sobre la intervención de las comunicaciones individuales, el TEDH ha exigido unas garantías mínimas que deben figurar en la ley: (1) la naturaleza de las infracciones que puedan dar lugar a una orden de interceptación; (2) la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial; (3) la fijación de un límite a la duración de la ejecución de la medida; (4) el procedimiento que deberá seguirse para el examen, uso y conservación de los datos obtenidos; (5) las precauciones que se han de tomar al comunicar los datos a otras partes; (6) las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de las cintas.[39] Pues bien, el TEDH no considera que exista ninguna razón para aplicar unos principios diferentes respecto a la accesibilidad y claridad de las normas a los programas de vigilancia generalizada,[40] y los aplica a las situaciones creadas por el desarrollo de nuevas tecnologías de vigilancia que, por ejemplo, en el caso británico, permitían interceptar todos los cables comerciales submarinos con una terminal en el Reino Unido y que llevan comunicaciones comerciales externas a Europa. De hecho, el Gobierno británico reconoció que, en principio, toda persona que enviase o recibiese algún tipo de telecomunicación fuera de las Islas británicas durante el período en cuestión, podía tener dicha comunicación físicamente interceptada.[41] Además, la ley inglesa confería una amplia discreción a las autoridades del Estado en lo concerniente a qué comunicaciones del volumen total físicamente interceptado, habían de leerse o escucharse.

El TEDH recuerda su jurisprudencia, según la cual los procedimientos para examinar, utilizar y almacenar la información interceptada debían exponerse de forma que se sometiesen al escrutinio y el conocimiento del público.[42] Además, pone como ejemplo la ley alemana, que establecía que "el Servicio Federal de Inteligencia estaba autorizado a controlar las comunicaciones con la única ayuda de términos de búsqueda que sirviesen, y fuesen adecuados, para la investigación de los riesgos descritos en la orden de vigilancia y cuyos términos habían de enumerarse en dicha orden"; esta ley, además, contiene "las normas de conservación y destrucción de los datos obtenidos a través de la vigilancia estratégica". Las autoridades que almacenaban los datos habían de verificar cada seis meses si seguían siendo necesarios para lograr los fines previstos cuando habían sido obtenidos o transmitidos. En caso contrario, habían de ser destruidos y borrados de los archivos o, en última instancia, se debía

38 *Caso Weber and Saravia c. Alemania,* apdo. 94.

39 *Ibíd.,* apdo. 95.

40 *Caso Liberty c. Reino Unido*, apdo. 63.

41 *Ibíd.*, apdo. 64.

42 *Ibíd.*, apdo. 67.

bloquear el acceso; la destrucción debía hacerse constar en acta y, en algunos casos, debía supervisarla el personal cualificado con capacidad para el ejercicio de funciones jurisdiccionales. Además, la Ley G10 establecía detalladamente las disposiciones que regían la transmisión, conservación y uso de los datos obtenidos a través de la intervención de las comunicaciones externas. A juicio del TEDH, en el Reino Unido ahora son del dominio público extensos fragmentos del *Code of Practice,* establecido en virtud del artículo 71 de la Ley de 2000, lo que sugiere que es posible para un Estado hacer públicos algunos detalles del funcionamiento de un esquema de vigilancia externa sin por ello comprometer la seguridad nacional.[43]

En conclusión, en el *asunto Liberty c. Reino Unido*, a diferencia del asunto *Weber and Saravia c. Alemania*, el TEDH no considera que la legislación interna indicara con la claridad necesaria, para ofrecer la adecuada protección contra el abuso de poder, el alcance o el ejercicio de la amplia discreción conferida al Estado para interceptar y examinar las comunicaciones externas. En particular, "no indicaba de forma accesible al público, ningún procedimiento a seguir para seleccionar y examinar, intercambiar, conservar y destruir la información interceptada". Por tanto, "la injerencia en los derechos de las demandantes, en virtud del artículo 8, no estaba prevista por la ley".[44]

En suma, si comparamos la aplicación del requisito de la previsibilidad de la ley en ambos asuntos observamos cómo el TEDH considera que la legislación alemana contiene las salvaguardas mínimas contra las interferencias arbitrarias según están definidas en su jurisprudencia y ofrece por tanto a los ciudadanos una indicación adecuada sobre las circunstancias y condiciones en que fueron habilitados los poderes públicos para recurrir a medidas de control, así como, el alcance y la forma de ejercicio de la discreción de las autoridades,[45] mientras que la legislación británica no las cumplía.

2.1.2. *Necesidad en una sociedad democrática*

La defensa de la seguridad nacional constituye, según el párrafo 2 del artículo 8, un fin legítimo que justifica una injerencia en la vida privada (secreto de las comunicaciones). Sin embargo, no basta con que los gobiernos invoquen este fin sino que deben justificar que dichas injerencias son necesarias en una sociedad democrática para lograr dicho fin (test de necesidad) y proporcionadas al fin perseguido (test de proporcionalidad).[46]

43 *Ibíd.*, apdo. 68.

44 *Ibíd.*, apdo. 69.

45 *Caso Weber and Saravia c. Alemania,* apdo. 101.

46 *Caso Klass y otros contra Alemania* apdo. 49 y 50; *Caso Weber and Saravia c. Alemania,* apdos. 105 y 107.

En el asunto antes citado, *Weber and Saravia c. Alemania* el TEDHl recuerda que las autoridades nacionales disfrutan de cierto poder discrecional para elegir las modalidades del sistema de vigilancia, pero que, como estableció en el caso *Klass y otros,* los Estados contratantes no disponen de una discreción ilimitada. Cualquiera que sea el sistema de vigilancia adoptado, el TEDH debe convencerse de la existencia de garantías adecuadas y suficientes contra los abusos.[47] El gobierno alemán alegó que las medidas de vigilancia autorizadas por la ley G 10 (tras la reforma de 1994) eran necesarias para luchar contra el terrorismo internacional, por el contrario, los demandantes consideraban que el alcance de la vigilancia prevista era demasiado amplio[48] y el sistema de autorización y supervisión no eran adecuados.[49] Examinado el sistema alemán de vigilancia estratégica generalizada, el TEDH concluye, al igual que en el asunto *Klass y otros*, que en la legislación alemana existían garantías adecuadas y efectivas contra los abusos de los poderes de control estratégicos del Estado. Por tanto, se considera que el Estado demandado, dentro de su relativamente amplio margen de apreciación en la materia, tenía derecho a considerar las interferencias con el secreto de las telecomunicaciones que resulten de las disposiciones impugnadas siendo necesarias en una sociedad democrática, en interés de la seguridad nacional y para la prevención de la delincuencia.[50]

2.2. El derecho a la protección de datos de carácter personal

Según reiterada jurisprudencia del TEDH la protección de datos personales pertenece al ámbito de aplicación del artículo 8. El Tribunal realiza una interpretación extensiva de la noción "vida privada" que concuerda con la del *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal*, de 28 de enero de 1981,[51] cuyo fin es «garantizar, en el territorio de cada una de las partes, a toda persona física (...) el respeto a los derechos y libertades fundamentales, y especialmente su derecho a la vida privada, respeto al tratamiento automatizado

47 *Caso Weber and Saravia c. Alemania,* ap. 106; *Caso, y otros contra Alemania* apdo. 49 y 50.

48 *Caso Weber and Saravia c. Alemania* "The Federal Intelligence Service was entitled to monitor all telecommunications within its reach without any reason or previous suspicion. Its monitoring powers therefore inhibited open communication and struck at the roots of democratic society. It was irrelevant whether or not it was already possible from a technical point of view to carry out worldwide monitoring (apdo. 111). "In the applicant's view, these wide monitoring powers did not correspond to a pressing need on the part of society for such surveillance" (apdo. 112).

49 *Ibíd.*, apdo. 113.

50 *Caso Weber and Saravia c. Alemania,* apdo. 137.

51 *Caso Amman contra Suiza*. Sentencia de 16 febrero 2000, apdo. 65.

de datos de carácter personal que le conciernan» (artículo 1), siendo estos últimos definidos como «toda información concerniente a una persona física identificada o identificable» (artículo 2).

En al asunto *S. y Marper C. Reino Unido*, el TEDH recuerda que "el mero hecho de memorizar datos relativos a la vida privada de una persona constituye una injerencia en el sentido del artículo 8 (…),[52] precisando que "poco importa que la información memorizada se utilice o no posteriormente".[53] Y añade, que

"para determinar si la información de carácter personal conservada por las autoridades hace que entre en juego [algún aspecto] de la vida privada, el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados y los resultados que pueden extraerse de ellos".[54]

En el caso de autos, el TEDH señala que "las huellas dactilares, los perfiles de ADN y las muestras celulares, constituyen datos de carácter personal en el sentido de la Convención sobre la protección de datos, puesto que se refieren a personas identificadas o identificables".[55] También ha considerado una injerencia en la vida privada dentro de la aplicación del artículo 8 la conservación por una autoridad pública de datos relativos a la vida privada de una persona por motivos de seguridad nacional,[56] memorizar datos relativos a la vida privada de un individuo obtenidos a través de intervenciones telefónicas,[57] la protección de datos médicos,[58] el seguimiento de un individuo por GPS y el tratamiento y utilización de los datos obtenidos de este modo,[59] la inclusión de información acerca de los movimientos por tren y avión de un individuo en la base de datos de la policía[60] o la inscripción de un individuo en los expedientes de un (antiguo) servicio de seguridad del Estado como «agente» de dicho organismo.[61]

52 Caso *S. y Marper c. Reino Unido*. Sentencia de 4 diciembre 2008, apdo. 67. Véase también caso *Leander c. Suecia*. Sentencia de 26 marzo 1987, apdo. 48.

53 *Ibíd.* Véase también *Caso Amman contra Suiza*. Sentencia de 16 febrero 2000, apdo. 69.

54 *Ibíd.*

55 *Ibíd.* ap. 68 y ap. 86. Véase también *Caso M.K. c. Francia*. Sentencia de 18 de abril de 2013, apdo. 26.

56 *Caso Leander c. Suecia,* ap. 48. Véase también asunto *Rotaru c. Rumanía,* apdo. 43.

57 *Caso Amman c. Suiza*. Sentencia de 16 febrero 2000, apdos. 65, 69 y 80.

58 *Caso L.H. c. Letonia*, Sentencia de 29 de abril de 2014, apdo. 56.

59 *Caso Uzun c. Alemania*. Sentencia de 2 septiembre 2010. apdo. 52.

60 *Caso Shimovolos c. Rusia*. Sentencia de 21 junio 2011, apdo. 66.

61 *Caso Turek c. Eslovaquia*. Sentencia de 14 febrero 2006, apdo. 110.

El TEDH también ha entendido que "hay datos de naturaleza pública que pueden hacer referencia a la vida privada cuando, de manera sistemática, se recogen y se almacenan en ficheros llevados por los poderes públicos. Esto es todavía más relevante cuando los datos se refieren al pasado lejano de una persona",[62] "tales informaciones (estudios, actividades políticas y antecedentes penales), cuando son, de manera automática, recogidas y almacenadas en un fichero llevado por agentes del Estado, afectan a la «vida privada» en el sentido del artículo 8.1 del CEDH".[63] Además, en el asunto *Weber y Saravia* antes citado, el TEDH entendió que la transmisión de datos (obtenidos por los servicios de inteligencia) y su uso por otras autoridades, que amplía el grupo de personas con conocimiento de los datos interceptados, constituye una injerencia autónoma en el ejercicio del derecho garantizado por el artículo 8.[64]

Una vez determinada la aplicación del artículo 8 a la protección de datos de carácter personal, y la existencia de una injerencia en el disfrute de ese derecho, el TEDH aplica los requisitos exigidos en el párrafo 2, es decir, si esa injerencia está prevista por la ley, persigue un fin legítimo y es necesaria en una sociedad democrática para alcanzar tal fin.

2.2.1. *Previsibilidad de la ley*

Al igual que en el supuesto anterior, es constante la jurisprudencia del TEDH según la cual los términos «previstos por la Ley» significan que la medida litigiosa ha de tener una base en el derecho interno y ser compatible con la preeminencia del derecho, expresamente mencionada en el preámbulo del CEDH e inherente al objeto y fin del artículo 8. La ley ha de ser así suficientemente accesible y previsible, es decir: ha de estar enunciada con la suficiente precisión para permitir que la persona regule su conducta. Para que se la pueda juzgar conforme a estas exigencias, debe ofrecer una protección adecuada contra lo arbitrario; y, en consecuencia, definir con suficiente claridad el alcance y las modalidades de ejercicio de la facultad que se confiere a las autoridades competentes.[65] El nivel de precisión que requiere la legislación interna depende en gran medida del contenido del texto considerado, del ámbito que supuestamente

62 *Caso Rotaru c. Rumanía.* Sentencia de 4 mayo 2000, apdo. 43.

63 *Caso Rotaru c. Rumanía.* Sentencia de 4 mayo 2000, apdo. 44.

64 *Ibíd.*, apdo. 79.

65 Caso *S. y Marper c. Reino Unido*, ap. 95. Véase también Caso Malone c. Reino Unido, apdos. 66 – 68; Caso *Rotaru c. Rumanía*. Sentencia de 4 mayo 2000, apdo. 55; *Caso Amann c. Suiza*. Sentencia de 16 de febrero de 2000, apdo. 56.

cubre y del número y la calidad de sus destinatarios.[66]

El TEDH ha tenido la oportunidad de aplicar estos principios generales a la ley rumana que autoriza al Servicio Rumano de Información (SRI) a recoger, almacenar y utilizar informaciones relativas a la seguridad nacional. En el *caso Rotaru c. Rumania* el TEDH expresa sus dudas en cuanto a la pertinencia para la seguridad nacional de las informaciones guardadas con respecto al demandante. Sin embargo, recuerda que incumbe en primer lugar a las autoridades nacionales, y sobre todo a los tribunales, interpretar y aplicar el derecho interno y señala, a este respecto, que en su Sentencia de 25 de noviembre de 1997, el Tribunal de Apelación de Bucarest confirmó la legalidad de la posesión por parte del SRI de esos datos como depositario de los archivos de los antiguos servicios de seguridad. Así, el TEDH concluye que "el almacenamiento de datos sobre la vida privada del demandante tenía una base en el derecho rumano".[67] En cuanto a la accesibilidad de la ley, el TEDH estima que esta exigencia se cumple ya que la ley rumana fue publicada en el Boletín Oficial Rumano el 3 de marzo de 1992.[68]

El TEDH examina, a continuación, la calidad de las normas jurídicas invocadas en este caso, buscando en particular si el derecho interno rumano fijaba con una precisión suficiente en qué condiciones el SRI podía almacenar y utilizar las informaciones relativas a la vida privada del demandante. El Tribunal señala a este respecto que:

"la legislación interna no define ni el tipo de informaciones que pueden ser registradas, ni las categorías de personas susceptibles de ser objeto de medidas de vigilancia, tales como la recogida y conservación de datos, ni las circunstancias en las que se pueden tomar dichas medidas, ni el procedimiento que debe seguirse. Asimismo, la ley no fija límites en cuanto a la antigüedad de las informaciones que se poseen ni a la duración de su conservación".[69]

En cuanto a la existencia de garantías adecuadas y suficientes contra los abusos el TEDH considera, para que los sistemas de vigilancia secreta sean compatibles con el artículo 8 del CEDH: "deben contener las garantías establecidas por la ley y ser aplicables al control de las actividades de los servicios implicados". Esto supone, entre otras cosas, "que una injerencia del ejecutivo en los derechos del individuo esté sometida a un control eficaz que debe normalmente garantizar, por lo menos en última instancia, el poder judicial, ya que ofrece las mejores garantías de independencia, de imparcialidad y de procedimiento regular".[70] En el caso de autos, el TEDH señala que el sistema

66 Caso *S. y Marper c. Reino Unido*. Sentencia de 4 diciembre 2008, apdo. 96. Véase también *Caso Hassany Tchaouch contra Bulgaria*, apdo. 84.

67 *Caso Rotaru c. Rumanía,* apdo. 53.

68 *Ibíd.*, apdo. 54.

69 *Caso Rotaru c. Rumanía,* apdos. 56 – 58.

70 *Ibíd.,* apdo. 59. Véase también *Caso Klass y otros c. Alemania,* apdo. 55.

rumano de recogida y archivo de informaciones no aporta tales garantías, ya que la ley no prevé ningún procedimiento de control, ya sea mientras la medida ordenada esté en vigor, ya sea posteriormente. Así, el Tribunal estima que el derecho interno no indica con suficiente claridad la extensión y las modalidades de ejercicio del poder de apreciación de las autoridades en el campo considerado. El TEDH concluye que la posesión y la utilización por parte del SRI de informaciones sobre la vida privada del demandante no estaban «previstas por la Ley», lo que basta para constituir un desconocimiento del artículo 8.[71] En varios asuntos posteriores contra Rumanía, el TEDH vuelve a examinar estos requisitos e insiste en la ausencia de garantías en el derecho interno rumano.[72]

2.2.2. *Necesidad en una sociedad democrática*

Como se viene indicando, junto al requisito de la previsibilidad de la ley, la recogida, utilización, almacenamiento etc. de datos personales debe perseguir un fin legítimo y ser necesario en una sociedad democrática para alcanzar dicho fin. En el *caso Leander y Segerstedt contra Suecia*, el TEDH se ocupa de examinar si una injerencia prevista en la ley, es necesaria en una sociedad democrática para la defensa de la seguridad nacional. Por necesidad se entiende "una necesidad social imperiosa y sobre todo proporcionada al fin legítimo perseguido".[73] A este respecto, el TEDH reconoce "que las autoridades nacionales gozan de un margen de apreciación cuya amplitud depende no solo de la finalidad, sino también del propio carácter de la injerencia", y que hay "que sopesar el interés del Estado demandado de proteger su seguridad nacional con la gravedad de la vulneración del derecho del demandante al respeto de su vida privada".[74] El TEDH insiste en que aun siendo amplio ese margen de apreciación en materia de seguridad nacional, "debe estar convencido de la existencia de garantías adecuadas y suficientes contra los abusos".[75] En el caso de autos el TEDH entendió que el Gobierno sueco "estaba en su derecho de considerar que los intereses de la seguridad nacional prevalecían sobre los intereses individuales del demandante", en consecuencia, la injerencia que el demandado sufrió "no podría, ser considerada como desproporcionada al fin legítimo

71 *Ibíd.*, apdos. 60 – 63.

72 Véase *Caso Dumitru Popescu contra Rumania*. Sentencia de26 de abril de 2007; *Caso Haralambie contra Rumania*. Sentencia de 27 de octubre de 2009; *Caso Asociación 21 de diciembre de 1989 y otros c. Rumanía.* Sentencia de 24 de mayo de 2011; *Caso Ioan Jarnea contra Rumania*. Sentencia de 19 de julio de 2011.

73 Caso *Leander contra Suecia*, apdo. 58.

74 *Ibíd.*, apdo. 59.

75 *Ibíd.*, apdo. 60.

perseguido".[76] La legislación sueca que permite almacenar datos personales por los servicios de inteligencia (*Security Police*) en la lucha contra el terrorismo y el espionaje fue examinada de nuevo en el asunto *Segerstedt-Wiberg y otros.*[77] En esta ocasión, sin embargo, el TEDH concluye que el almacenamiento de datos por motivos de seguridad nacional fue necesario solo con respecto a uno de los demandantes pero no con respecto a los demás.[78]

3. LAS OBLIGACIONES POSITIVAS DE LOS ESTADOS INHERENTES AL ARTÍCULO 8 DEL CEDH

El apartado 2 del artículo 8 del CEDH se refiere a las condiciones que se exigen para que las injerencias de las autoridades públicas en los derechos garantizados por el apartado 1 estén justificadas.[79] Pero, ¿qué ocurre cuando las injerencias provienen de terceros, sean estos particulares o Estados? En el contexto de la vigilancia masiva de comunicaciones, el PE ha pedido a los Estados miembros de la UE que:

"cumplan de inmediato con su obligación positiva, a tenor del Convenio Europeo de Derechos Humanos, de proteger a sus ciudadanos de la vigilancia contraria a los requisitos establecidos – incluso cuando su objetivo sea salvaguardar la seguridad nacional – llevada a cabo por terceros países (…) y garanticen que el Estado de Derecho no se vea debilitado por la aplicación extraterritorial de la legislación de un tercer país[80]".

Las obligaciones positivas consisten en un deber de actuar con el objeto de garantizar la efectividad de los derechos enunciados en el CEDH.[81] Estas obligaciones resultan

76 *Ibíd.*, apdo. 67.

77 *Caso Segerstedt-Wiberg y otros contra Suecia*. Sentencia de 6 junio 2006, apdo. 87.

78 *Ibíd.*, apdo. 92.

79 Sobre las obligaciones de los Estados en virtud del Convenio, en general, véase FERNÁNDEZ SÁNCHEZ, P. A., *Las obligaciones de los Estados en el marco del Convenio Europeo de Derechos Humanos*, Ministerio de Defensa, Madrid, 1987.

80 Informe Moares, apdo. 27.

81 Sobre las obligaciones positivas de los Estados en el marco del CEDH véase, entre otros, FERNÁNDEZ SÁNCHEZ, P. A. *Las obligaciones de los Estados en el marco del Convenio Europeo de Derechos Humanos*, Madrid, 1987; PAVAGEAU, S. "Les obligations positives dans les jurisprudences de cours européenne et ineraméricaine des droits de l'homme", *Revista Colombiana de Derecho Internacional,* Nº 6, julio-diciembre de 2005, pp. 201-246; XENOS, D. *The Positive Obligations of the*

de una interpretación dinámica del contenido, y corresponde al TEDH determinar su existencia y definir su alcance.[82] El TEDH ha interpretado que aunque la principal finalidad del artículo 8 es proteger a la persona contra las intromisiones arbitrarias de los poderes públicos, puede imponer además obligaciones positivas inherentes a un respeto efectivo de la vida privada y familiar".[83] En el *Caso X e Y contra Países Bajos,* el Tribunal recuerda que el artículo 8 no se limita a obligar al Estado a abstenerse de tales injerencias, "a esta obligación negativa pueden añadirse otras positivas, inherentes a un respeto efectivo de la vida privada o familiar. Pueden implicar la adopción de medidas tendentes a asegurar el respeto de la vida privada incluso en las relaciones de los individuos".[84]

Sin embargo, es difícil precisar cuándo el artículo 8 exige una acción positiva del Estado, se entiende que el Estado debe tener en cuenta si se ha alcanzado un justo equilibrio entre el interés general de la comunidad y los intereses del individuo.[85] En el *Caso Gaskin contra Reino Unido,* el TEDH considera que hay que averiguar en cada caso sí, teniendo en cuenta el margen discrecional del Estado, se ha mantenido un equilibrio justo entre los intereses opuestos, de una parte, el interés público en que funcione eficazmente el régimen de protección a la infancia; de otra, el propio del demandante en poder consultar una relación coherente de su historia personal.[86] Y añade que "en la búsqueda de este equilibrio, los fines enumerados en el apartado 2 del artículo 8 tienen su importancia, aunque en él se habla únicamente de las injerencias en el ejercicio del derecho protegido por el primer apartado y se refiere, por tanto, a las obligaciones negativas que del mismo se derivan".[87] En la práctica, la mayoría de los casos planteados al TEDH se refieren al respeto de la vida familiar, y en ellos parece tener mayor peso el interés general de la comunidad; de tal forma que corresponde al individuo probar que predomina su interés particular.[88]

No existe jurisprudencia en relación a la obligación positiva del Estado de asegurar el respeto a la vida privada de sus nacionales frente a las injerencias de un tercer

State under the European Convention of Human Rights, London and New York: Routledge, 2012.

82 PAVAGEAU, Stéphanie. "Les obligations positives…" *loc. cit.,* p. 206.

83 Véase, entre otros, *Caso Johnston y otros contra Irlanda*. Sentencia de 18 diciembre 1986, apdo. 55; *Caso Gaskin contra Reino Unido*. Sentencia de 7 julio 1989, apdo. 38.

84 *Caso X e Y contra Países Bajos*. Sentencia de 26 marzo 1985, apdo. 23.

85 *Caso Kroon y otros contra Países Bajos*. Sentencia de 27 octubre 1994, apdo. 31; *Caso Keegan contra Irlanda*. Sentencia de 26 mayo 1994, apdo. 21.

86 *Caso Gaskin contra Reino Unido*. Sentencia de 7 julio 1989, apdo. 40.

87 *Caso Gaskin contra Reino Unido*, apdo. 42.

88 KILKELLY, Ú. *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights*, Human Rights Handbooks, Nº 1, p. 21.

Estado y la doctrina no parece contemplar tal posibilidad. Así, Dimitris Xenos se refiere exclusivamente a la protección de los individuos frente a los actos de injerencia procedentes de particulares, incluyendo a actores estatales cuando actúan como tales.[89] Sin embargo, como se viene indicando uno de los elementos que caracterizan las actividades de vigilancia masiva y generalizada llevadas a cabo por los servicios de inteligencia de EEUU es la extraterritorialidad.[90] ¿Significa que si el acto de injerencia proviene de un Estado que no actúa como un particular no es responsable indirectamente el Estado territorial que debía haber protegido a sus ciudadanos? Según esta interpretación, nos moveríamos en el plano clásico del derecho internacional que exigiría al ciudadano recurrir ante los tribunales de un Estado extranjero por dicha injerencia en el ejercicio de sus derechos, con las dificultades que en el contexto de la acción de los servicios de inteligencia en el exterior conlleva.[91] O más bien, ¿podemos pensar que, hasta el momento, no ha existido un supuesto de hecho en el que poder afirmar la existencia de tal obligación de protección? En nuestra opinión, una interpretación finalista y teleológica del CEDH nos llevaría a sostener la necesidad de afirmar la obligación de adoptar medidas por parte de los Estados miembros del CEDH, para garantizar la protección efectiva del artículo 8 en el contexto de la vigilancia masiva de comunicaciones por terceros Estados; puesto que significa, en última instancia, hacer prevalecer los derechos humanos sobre la soberanía de los Estados, interpretación que ya se ha utilizado en otras ocasiones.[92]

89 XENOS, D. The *Positive Obligations of the State under the European Convention of Human Rights*, London and New York: Routledge, 2012.

90 Véase al respecto A/HRC/27/37, párrs. 31-36.

91 "Varios ordenamientos jurídicos distinguen entre las obligaciones para con los nacionales o las personas presentes en los territorios del Estado y las obligaciones para con los no nacionales y las personas que están fuera de dicho territorio, o establecen menores niveles de protección para las comunicaciones extranjeras o externas. En los casos en que no se sepa con certeza si los datos son extranjeros o nacionales, los servicios de inteligencia a menudo procesan los datos como extranjeros (ya que las comunicaciones digitales suelen cruzar las fronteras en algún momento), permitiendo así que sean recopilados y conservados. El resultado es un nivel de protección de la privacidad sustancialmente inferior —o incluso nulo— para los extranjeros y los no ciudadanos, en comparación con los ciudadanos", A/HRC/27/37, párr. 35.

92 Véase al respecto las valoraciones de PASTOR RIDRUEJO, J. A. "La reciente jurisprudencia del Tribunal Europeo de Derechos Humanos: Temas escogidos", *Curso de Derecho internacional y relaciones internacionales de Vitoria-Gasteiz,* 2007, p. 251.

4. CONCLUSIONES

A la luz de la jurisprudencia del TEDH estudiada es innegable que los programas de vigilancia masiva y generalizada de las comunicaciones, por parte de los servicios de inteligencia, constituyen una injerencia en la vida privada de los ciudadanos. Esta injerencia puede ser sin embargo necesaria en una sociedad democrática, en la lucha contra el terrorismo internacional y en la defensa de la seguridad nacional, si el Estado ofrece garantías adecuadas y suficientes contra los abusos. Tales medidas de vigilancia solo están justificadas si se basan en el derecho interno del Estado, el cual, a su vez, debe respetar los estándares mínimos de derechos humanos en esta materia. Esto significa que la regulación de los sistemas de vigilancia masiva debe ser accesible a la persona afectada, debe prever las consecuencias para dicha persona y debe ser compatible con la preeminencia del derecho. La accesibilidad implica que la Ley debe utilizar términos bastante claros para indicar en qué circunstancias, y bajo qué condiciones, faculta al poder público para recurrir a tales medidas. Teniendo en cuenta el riesgo de abusos inherente a cualquier sistema de vigilancia secreta, dichas medidas deben basarse en una ley muy precisa, sobre todo considerando que la tecnología disponible es cada vez más sofisticada. Por último, el derecho interno debe ofrecer una protección adecuada frente a las injerencias arbitrarias que incluya procedimientos de control.

Ahora bien, en la era digital algunos derechos humanos fundamentales, como el derecho al respeto a la vida privada o a la protección de datos, necesitan ser entendidos en una nueva dimensión. En el caso de la vigilancia masiva y generalizada de las comunicaciones, que incluye una vigilancia extraterritorial, las injerencias en el ejercicio de los derechos garantizados por el artículo 8 del CEDH pueden provenir de terceros Estados. Las garantías que exige el TEDH en su jurisprudencia parecen suficientes para la vigilancia nacional, pero son de difícil aplicación en el contexto de actividades extraterritoriales de terceros Estados. Es por este motivo, que es necesaria la adopción de medidas destinadas a garantizar que no se producirán actividades de vigilancia secreta y masiva en el territorio de un Estado sin cumplir con las garantías previstas en su derecho interno. Sobre todo si atendemos a los diferentes estándares de protección que existen a un lado y al otro del atlántico. Por otro lado, la recepción, utilización, almacenamiento, etc…, de datos por parte de las autoridades nacionales, obtenidos por los servicios de inteligencia extranjeros, debe basarse, de nuevo, en el derecho interno del Estado receptor, ofreciendo las mismas garantías que las exigidas a las medidas adoptadas por los propios servicios de inteligencia.

BIBLIOGRAFÍA

AKRIVOPOULOU, CH. (ed.), *Human rights and risks in the digital era: globalization and the effects of information technologies,* Hershey, PA: Information Science Reference, 2012.

BOWDEN, C. *The US surveillance programmes and their impact on EU citizens' fundamental rights, study for the European Parliament*, PE 474.405, Brussels, September 2013.

CORNAGO PRIETO, N., "Lucha contra el terrorismo y derechos humanos", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, 2010, pp. 347-361.

COSTAS TRASCASAS, M., "Seguridad nacional y derechos humanos en la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) en materia de terrorismo internacional: ¿hacia un nuevo equilibrio?", E. Conde Pérez (dir.), *Terrorismo y legalidad internacional*, Madrid: Dykinson, 2012, pp. 187-207.

COUNCIL OF EUROPE, *Human Rights and the fight against terrorism: the Council of Europe guidelines,* Strasbourg: Council of Europe Publishing, 2005.

DAVIS, F. *Surveillance, counter-terrorism and comparative constitutionalism,* Abingdon, Oxon: Routledege, 2014 (especialmente páginas 93 a 152).

FERNÁNDEZ SÁNCHEZ, P. A. *Las obligaciones de los Estados en el marco del Convenio Europeo de Derechos Humanos*, Ministerio de Defensa, Madrid, 1987.

KLANG. M/MURRAY, A. *Human rights in the digital age,* London; Portland, Or.; GlassHouse, 2005.

KILKELLY, Ú. "The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights", *Human Rights Handbooks*, Nº 1.

PASTOR RIDRUEO, J. A. "La reciente jurisprudencia del Tribunal Europeo de Derechos Humanos: Temas escogidos", *Curso de Derecho internacional y relaciones internacionales de Vitoria-Gasteiz,* 2007, pp. 240 – 276.

PAVAGEAU, S. "Les obligations positives dans les jurisprudences de cours européenne et ineraméricaine des droits de l'homme", *Revista Colombiana de Derecho Internacional,* Nº 6, julio-diciembre de 2005, pp. 201-246.

PÉREZ GONZÁLEZ, M. "Derechos humanos y lucha contra el terrorismo", en A. Pastor Palomar (coord.), C. Escobar (dir.), *Los derechos humanos en la sociedad internacional del siglo XXI*, Madrid: Escuela Diplomática, 2009, pp. 39-62.

RIGAUX, F. «La protection de la vie privée en Europe», *en Le droit commun de l'Europe et l'avenir de l'enseignement juridique*, de Witte B. y Forder, C., eds., Kluwer, 1992.

RUBENFELD, J. «The Right of Privacy», *Harvard Law Review*, 1989, vol. 102, pp. 737 – 807.

DE SCHUTTER, O. «La vie privée entre droit de la personnalité et liberté», *Revue trimestrielle des droits de l'homme*, n°40, octobre 1999, pp. 827-863.

SHEININ, M. (Coord.), "European and United States Counter-Terrorism Policies, the rule of law and Human Rights", *RSCAS Policy Papers 2011/03,* European University Institute, 2011.

WACHSMANN, P. «Le droit au secret de la vie privé», en Sudre F.: *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, pp. 119 – 156.

XENOS, D. *The Positive Obligations of the State under the European Convention of Human Rights*, London and New York: Routledge, 2012.