AMENAZAS A LA SEGURIDAD Y PRIVACIDAD: LA DIFICULTAD DEL EQUILIBRIO PERFECTO

Alicia González Monje
Profesora Asociada. Área de Derecho Procesal
Universidad de Salamanca

SUMARIO: I. Del riesgo a la amenaza: hacia un nuevo concepto de seguridad. 1. El terrorismo yihadista: ¿una brecha en las Estrategias de Seguridad? II. El uso por el aparato del estado de las nuevas tecnologías con fines de investigación penal. 1. Sistemas de interceptación masiva de comunicaciones. III. La posición del tribunal europeo de derechos humanos. IV. ¿Quién vigila a los que nos vigilan?

Palabras claves
Amenazas a la seguridad; Vigilancia masiva; Privacidad.

Resumen
El objetivo de este trabajo es analizar la existencia de un nuevo concepto de seguridad que permita hacer frente a las amenazas de la actual criminalidad, así como el cambio que el terrorismo internacional ha supuesto en la percepción de ese concepto desde el año 2001. Se examina si este nuevo orden mundial legitima el uso por parte de los Estados de sistemas de vigilancia masiva de comunicaciones, con un estudio detallado de las resoluciones del Tribunal Europeo de Derechos Humanos en la materia, a fin de que se pueda apreciar con claridad la dimensión de la injerencia de estas técnicas en la vida privada de los ciudadanos.

I. DEL RIESGO A LA AMENAZA: HACIA UN NUEVO CONCEPTO DE SEGURIDAD

La Estrategia Española de Seguridad de 2011 define el riesgo como «la contingencia o probabilidad de que una amenaza se materialice produciendo un daño»; mientras que la amenaza es conceptuada como «toda circunstancia o agente que ponga en peligro la seguridad o estabilidad de España»[1].

[1] España, *Estrategia Española de Seguridad. Una responsabilidad de todos*, 2011, p. 41. Disponible en: http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEs-

Como pone de manifiesto González Cussac[2], nos encontramos en un momento en que «los viejos fenómenos de delincuencia común, particularmente terrorismo y delincuencia organizada, han pasado de ser considerados como simples «riesgos» a la seguridad nacional hasta alcanzar la máxima categoría de «amenaza». Junto a los riesgos y amenazas, hay otros factores potenciadores[3] que pueden producir un doble efecto: crear nuevos riesgos y amenazas o agravar los efectos de los ya existentes[4].

El ciberespacio es, sin duda, el nuevo escenario donde confluyen gran número de las amenazas actuales, que Davara Rodríguez[5] clasifica en:

- Agentes de perfil bajo: individuos aislados o poco organizados normalmente con fines exclusivamente personales (hackers, crackers y otros tipos de delincuentes del ciberespacio).
- Cibercrimen o crimen organizado: organizaciones mafiosas o criminales organizados que pretenden obtener un beneficio económico o provocar daños de acuerdo con sus intereses.
- Ciberterrorismo: organizaciones terroristas y extremismo político e ideológico en acciones de propaganda, reclutamiento y atentados contra sistemas de información.
- Estados: utilizan el ciberespacio para dar continuidad a los conflictos físicos en el mundo virtual (ciberguerra y guerra de la información).

El contexto expuesto ha propiciado que los Estados sean cada vez más conscientes «de la estrecha interdependencia existente entre la seguridad interior (*homeland security*)

panolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423 [Última consulta: 25-02-2017].

[2] J.L. González Cussac, «Tecnocrimen», en J.L. González Cussac, y M.L. Cuerda Arnau (dirs.), *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* Tirant lo Blanch, Valencia, 2013, p. 208.

[3] Para un estudio detallado de los mismos, ver: L. de la Corte Ibáñez y J.M. Blanco Navarro, «Potenciadores de riesgo. Una visión ampliada para un mundo global», en L. De la Corte Ibáñez y J.M. Blanco Navarro, *Seguridad nacional, amenazas y respuestas*, LID Editorial Empresarial, Madrid, 2014, pp. 55-78.

[4] Entre esos factores potenciadores, la Estrategia de Seguridad Nacional de 2013, actualmente en vigor, destaca, entre otros, «la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos, el cambio climático o la generalización del uso nocivo de las nuevas tecnologías». España, *Estrategia de Seguridad Nacional. Un proyecto compartido*, 2013, p. 21. Disponible en: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf [Última consulta: 25-02-2017].

[5] F. Davara Rodríguez, «Las TIC y las amenazas a la seguridad nacional; ciberseguridad», en J.L. González Cussac, y M.L. Cuerda Arnau (dirs.), *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* Tirant lo Blanch, Valencia, 2013, p. 153.

y la seguridad exterior (*foreign security*)»[6], situación que demanda una creciente cooperación para atajar este tipo de fenómenos, teniendo en cuenta que «afrontamos amenazas y riesgos transversales, interconectados y transnacionales», hasta el punto de que «los límites entre la seguridad interior y la seguridad exterior se han difuminado»[7].

Ello supone también el avance hacia un nuevo concepto de seguridad, en la medida en que «se está sustituyendo el enfoque tradicional y unidimensional de la seguridad, dirigido hacia la seguridad del territorio, del Estado y del régimen político, por un enfoque más amplio que, sin olvidar estos aspectos, se centre en la seguridad y el bienestar de la población, incorpore nuevos asuntos y adopte una perspectiva multilateral e incluso mundial»[8].

Acorde con esta perspectiva se encuentra la definición de seguridad utilizada por Feliu Ortega, como «el estado deseado por una sociedad en el que pueda ésta desarrollarse y prosperar libre de amenazas»[9].

1. El terrorismo yihadista: ¿una brecha en las estrategias de seguridad?

Si hay una amenaza que preocupa de manera especial en las estrategias de seguridad nacional, internas y externas, es la del terrorismo islamista o yihadista.

No hay duda de que los atentados del 11 de septiembre de 2001 en Nueva York, marcan un antes y un después en la lucha contra el terrorismo[10]. Es a partir de ese momento cuando las amenazas se percibirán de forma global, estableciéndose «el modelo de Inteligencia que habría de sustituir al de la guerra fría»[11].

---

[6] A.V. Carvalho y M.Á. Esteban Navarro, «Los servicios de inteligencia: entorno y tendencias», en J.L. González Cussac, (coord.), *Inteligencia*, Tirant lo Blanch, Valencia, 2012, p. 74.

[7] M.L. Cuerda Arnau, «Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes», en J.L. González Cussac y M.L. Cuerda Arnau (dirs.), *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* Tirant lo Blanch, Valencia, 2013, p. 105.

[8] A.V. Carvalho y M.Á. Esteban Navarro, «Los servicios de inteligencia…» *cit.,* p. 76.

[9] L. Feliu Ortega, «La ciberseguridad y la ciberdefensa», *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Centro Superior de Estudios de la Defensa Nacional, Ministerio de Defensa, Madrid, núm. 126, febrero 2012, p. 39.

[10] Ver I. Blanco Cordero, «Terrorismo internacional: La amenaza global», en M.R. Diego Díaz-Santos y E.A. Fabián Caparrós (coords.), *El sistema penal frente a los retos de la nueva sociedad*, Colex, Madrid, 2003, pp. 209-210.

[11] M.Á. López Espinosa, «Inteligencia y terrorismo internacional. Un panorama de cambios», *La inteligencia, factor clave frente al terrorismo internacional*, Cuadernos de Estrategia, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, Madrid, junio 2009, p. 198. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3077905 [Última consulta: 25-02-2017].

Sin embargo, serán los atentados ocurridos en Madrid, el 11 de marzo de 2004[12] y en Londres, el 7 de julio de 2005[13], los que confirman la evolución constante[14] de la amenaza que para el mundo supone el «terrorismo yihadista» vinculado al autoproclamado «Estado islámico o Daesh»[15], que ha recrudecido sus actuaciones en 2015 y 2016, especialmente en Europa:

— El 7 de enero de 2015, dos encapuchados entraron en la sede del semanario satírico *Charlie Hebdo,* al grito de «Alá es grande». Doce personas son asesinadas y otras once resultaron heridas[16].
— El 8 de enero de 2015, un ciudadano francés de origen maliense mató a una policía municipal, hiriendo gravemente a otra persona, y al día siguiente tomó varios rehenes en un supermercado judío, resultando muertos 4 rehenes.
— El 13 de noviembre de 2015, seis ataques en París provocaron la muerte de 130 personas, hiriendo a más de 350[17].
— El 22 de marzo de 2016, dos ataques prácticamente simultáneos en el aeropuerto *Zaventem*, a 7 kilómetros de Bruselas y en el metro de la capital, tuvieron como resultado 31 muertos y 270 heridos[18].

---

12 El 11 de marzo de 2004 en Madrid murieron 192 personas y hubo más de 1800 heridos.

13 El 7 de julio de 2005, cuatro explosiones tuvieron lugar en medios de transporte público de Londres, con más de 56 muertos y 700 heridos.

14 Los datos más recientes se pueden consultar en los informes de EUROPOL sobre el terrorismo en Europa (*Terrorism Situation and Trend*, TE-SAT) de 2010 a 2016. Disponibles en: https://www.europol.europa.eu/category/publication-category/strategic-analysis/eu-terrorism-situation-trend-report-te-sat. El citado informe confirma que un número no insignificante de radicales viajan desde la UE a zonas conflictivas o asisten a campos de adiestramiento terroristas y regresan a Europa, lo que indica que los riesgos de que la juventud se radicalice y cometa delitos de terrorismo siguen siendo considerables. [Última consulta: 25-02-2017].

15 Para un estudio de su origen y trayectoria, ver: J. Jordán Enamorado, «El Daesh», *La Internacional yihadista*, Cuadernos de Estrategia, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, Madrid, núm. 173, septiembre 2015, pp. 109-147; L. de la corte Ibáñez, «Yihadismo global: una visión panorámica», *Yihadismo en el mundo actual*, Documentos de Seguridad y Defensa, Escuela de Altos Estudios de la Defensa, Ministerio de Defensa, Madrid, núm. 62, septiembre 2014, pp. 43-84; I. Fuente Cobo, *Aproximación histórica al fenómeno del yihadismo*, Instituto Español de Estudios Estratégicos, Documento de análisis, 28/2015, de 13 de mayo de 2015, pp. 1-16.

16 «Doce muertos en un atentado en la revista "Charlie Hebdo" en París», *El País*, 8 de enero de 2015. Disponible en: http://internacional.elpais.com/internacional/2015/01/07/actualidad/1420629274_264304.html [Última consulta: 25-02-2017].

17 «Cronología de la matanza terrorista en París: 130 muertos y más de 350 heridos», *20 minutos*, 18 de noviembre de 2015. Disponible en: http://www.20minutos.es/noticia/2604691/0/matanza-terrorista-paris/cadena-atentados/francia-bataclan/ [Última consulta: 25-02-2017].

18 «Lo que se sabe de los ataques en el aeropuerto y en el metro de Bruselas reivindicados por Estado Islámico», *BBC News*, 22 de marzo de 2016. Disponible en: http://www.bbc.com/mundo/noticias/2016/03/160322_bruselas_dos_explosiones_aeropuerto_lv [Última consulta: 25-02-2017].

— El 14 de julio de 2016, un ciudadano francés de origen tunecino, atropelló en Niza a una multitud de personas, con un balance de 84 muertos y más de 200 heridos[19].
— El 26 de julio de 2016, dos hombres entraron en una iglesia católica en Normandía, asesinando al sacerdote encargado de la misma e hiriendo a una mujer, habiendo tomado cinco rehenes[20].
— El 19 de diciembre de 2016, un hombre irrumpió en el mercado navideño en pleno centro de Berlín, arrollando a decenas de personas y provocando la muerte de 12 de ellas, con 48 heridos[21].
— El 22 de marzo de 2017, un ciudadano británico atropella a los viandantes en las inmediaciones del Parlamento británico, causando la muerte de varias de cuatro personas y decenas de heridos[22].

Estas acciones terroristas han propiciado, en mayor o menor medida «no sólo un reforzamiento de las medidas jurídicas para combatirlas, sino la aparición de una auténtica legislación de emergencia permanente cuya vis expansiva y excepcionalidad han convertido a la legislación antiterrorista en uno de los mejores bancos de prueba que se puede utilizar para conocer el estado de salud de que goza un Estado democrático, pues es precisamente en esta materia donde el sistema político, incluso el más democrático, muestra de modo más patente una tendencia claramente autoritaria que lesiona de manera muy grave la eficacia de las garantías individuales»[23].

Además de todos los problemas asociados a este tipo de terrorismo, tales como la rápida radicalización de sus seguidores[24], los terroristas suicidas o «lobos solitarios»[25] o

[19] «El Gobierno francés eleva a 84 los muertos en el ataque con un camión en Niza», *El País,* 18 de julio de 2016. Disponible en: http://internacional.elpais.com/internacional/2016/07/14/actualidad/1468532799_683242.html [Última consulta: 25-02-2017].

[20] «Un cura degollado y una rehén en estado crítico en una ataque del IS en una iglesia de Normandía», *El Mundo,* 26 de julio de 2016. Disponible en: http://www.elmundo.es/internacional/2016/07/26/5797245a46163f54238b4597.html [Última consulta: 25-02-2017].

[21] «Un hombre mata a 12 personas con un camión en Berlín y reaviva el miedo al terrorismo en Europa», *El País,* 20 de diciembre de 2016. Disponible en: http://internacional.elpais.com/internacional/2016/12/19/actualidad/1482176155_449814.html [Última consulta: 25-02-2017].

[22] «Ataque terrorista en Londres: Cuatro muertos, entre ellos el atacante y 40 heridos», *El Mundo,* 23 de marzo de 2017. Disponible en: http://www.elmundo.es/internacional/2017/03/22/58d28f57e5fdea6d448b4579.html [Última consulta: 23-03-2017].

[23] C. Lamarca Pérez, «Terrorismo transnacional», en A.I. Pérez Cepeda (dir.), *Política criminal ante el reto de la delincuencia transnacional*, Tirant lo Blanch, Valencia, 2016, p. 460.

[24] Sobre este tema, ver: M.Á. Cano Paños, «El caso «Khaled Kelkal». Una clave para entender la radicalización islamista en la Europa del año 2015», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 17-09, 2015, pp. 1-28.

[25] Definidos por Lejarza Illaro como aquel individuo que no pertenece «de manera directa a ninguna organización terrorista pero habría sido adiestrado, reclutado y radicalizado en las redes sociales». E. Lejarza

el relativo a los llamados «combatientes extranjeros»[26], cobra especial relevancia el uso que de internet realizan estos grupos para difundir su mensaje[27], así como el uso que de las nuevas tecnologías de la información y la comunicación hacen los terroristas en la preparación y perpetración de los atentados.

En el ámbito de la Unión Europea, la lucha contra el terrorismo y la radicalización ha propiciado la elaboración de la Agenda Europea de Seguridad, que se diseñó para llevar a cabo acciones operativas específicas en áreas de riesgo concretas a fin de lograr mejoras inmediatas en las capacidades conjuntas de lucha contra el terrorismo de la UE[28].

A pesar de ello, los recientes ataques han puesto de manifiesto algunas de las siguientes lagunas[29]:

Illaro, *Terrorismo islamista en las redes - La yihad electrónica*, Instituto Español de Estudios Estratégicos, Documento de Opinión, 100/2015, de 15 de septiembre de 2015, p. 8. Para un estudio detallado del problema, ver: L. de la Corte Ibáñez, «Misiones suicidas al servicio de objetivos insurgentes y terroristas», *Cuadernos de Estrategia,* núm. 141, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, Madrid, 2009, pp. 111-159. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3077905 [Última consulta: 01-03-2017].

[26] Según un estudio reciente, de los 4.000 combatientes extranjeros que proceden presuntamente de Estados miembros de la UE, alrededor del 30% han regresado a sus países de origen. Estos combatientes extranjeros retornados han estado vinculados a los atentados terroristas de 2015 y 2016. Algunos han recibido instrucciones específicas de volver a Europa a cometer atentados terroristas, difundir propaganda de Daesh y radicalizar y reclutar a más personas. B. Van Ginkel y E. Entenmann (eds.), *The Foreign Fighters Phenomenon in the European Union*, *Profiles, Threats* & *Policies*, ICCT International Centre for Counter-Terrorism, The Hague, april 2016. Disponible en: https://www.icct.nl/wp-content/uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_1-April-2016_including-AnnexesLinks.pdf [Última consulta: 01-03-2017].

[27] Es la llamada guerrilla informativa o *netwar*. Para un estudio detallado del tema, a título de ejemplo, ver: M.Á. Cano Paños, «Internet y terrorismo islamista. Aspectos criminológicos y legales», *Eguzkilore*: *Cuaderno del Instituto Vasco de Criminología,* San Sebastián, núm. 22, diciembre 2008, pp. 67-88; A. Chicharro Lázaro, «Respuesta internacional al desafío de la estrategia mediática del Estado Islámico», *Revista Electrónica de Estudios Internacionales*, núm. 29, 2015, pp. 1-28; G. Weimann, «www.terror.net. How Modern Terrorism Uses the Internet», *United States Institute of Peace*, Special Report 116, march 2014, pp. 1-12. Disponible en: www.usip.org; Naciones Unidas. UNODC, *El uso de internet con fines terroristas*, Nueva York, 2013. Disponible en: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf [Última consulta: 01-03-2017]; M.E. Tapia Rojo, *Análisis de la estrategia comunicativa del terrorismo yihadista: el papel de las redes sociales*, Instituto Español de Estudios Estratégicos, Documento de Opinión, 2/2016, de 4 de enero de 2016, pp. 1-15.

[28] Para una mejor comprensión de sus objetivos, ver, a título de ejemplo: C. Jones, «Full compliance: the EU's new security agenda», *Statewatch*, [en línea], may, 2015, pp. 1-10. Disponible en: http://statewatch.org/analyses/no-268-eu-security-agenda.pdf [Última consulta: 05-03-2017]; Unión Europea. Comisión Europea, Agenda Europea de Seguridad: preguntas y respuestas, Estrasburgo, 28 de abril de 2015. Disponible en: http://europa.eu/rapid/press-release_MEMO-15-4867_es.htm [Última consulta: 05-03-2017].

[29] Unión Europea. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo, Aplicación de la Agenda Europea de Seguridad para luchar contra el terrorismo y allanar el camino hacia una Unión de la Seguridad genuina y efectiva, COM(2016) 230 final, Bruselas, de 20 de abril de

1. En muchos casos, los atentados fueron perpetrados por individuos radicalizados conocidos, a menudo con un historial en delincuencia organizada, que presentaban un riesgo para la seguridad por su capacidad para circular sin trabas dentro y entre los Estados miembros o para regresar de terceros países.
2. En algunos casos, incluso, sus movimientos habían sido notificados en las bases de datos policiales o eran conocidos por los servicios de inteligencia.
3. Algunas de las personas implicadas en los ataques ya eran perseguidas por las autoridades policiales y, a pesar de ello, pudieron beneficiarse del apoyo logístico de redes locales, que les permitieron permanecer ocultas y planificar los ataques.
4. Los ataques también se caracterizaron por la capacidad de los autores para fabricar grandes cantidades de explosivos, al tener acceso a grandes cantidades de precursores y productos pirotécnicos.
5. Los terroristas también tuvieron acceso ilegal a una gran cantidad de armas y municiones militares.
6. Los atentados han demostrado la capacidad de los autores para definir y atacar infraestructuras críticas y grandes espacios públicos en varios Estados miembros, a pesar de las medidas de protección existentes.

La situación la define muy gráficamente Montero Gómez, cuando señala que estos fenómenos criminales tienen unos rasgos de personalidad distintivos: «son transnacionales, son de estructura horizontal, difusa, interconectada y son inteligentes». Haciendo un símil darwiniano que responde perfectamente a la situación actual, añade el citado autor que «la inteligencia de la delincuencia organizada o del terrorismo la entenderemos como su capacidad para adaptarse a un ecosistema hostil, aquél vigilado y escudriñado por dispositivos de seguridad permanente, a fin de lograr propósitos que vulneran los límites establecidos por unas reglas de conducta, que en este caso están orientadas hacia el cumplimiento de la ley»[30].

Sin duda, lo anterior revela una importante laguna en el intercambio de información para detectar eficazmente a las personas involucradas en actividades terroristas, pero también revela a mi juicio, la capacidad de los terroristas para comunicarse entre ellos sin que sus comunicaciones sean detectadas ni por los servicios de inteligencia de los distintos Estados, ni por sus autoridades policiales.

2016, pp. 4-5. Disponible en: http://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0014.02/DOC_1&format=PDF [Última consulta: 05-03-2017].

[30] A. Montero Gómez, *Inteligencia Prospectiva de seguridad*, Real Instituto Elcano, Documento de Trabajo (DT) 24/2006, de 5 de octubre de 2006, p. 3. Disponible en: www.realinstitutoelcano.org [Última consulta: 05-03-2017].

Tengamos en cuenta dos datos: de un lado, el Ministro de Interior belga, Jan Jambon, aseguró en una declaración a los medios, días antes de los brutales atentados terroristas de París de 13 de noviembre de 2015, que los terroristas yihadistas podrían estar usando para comunicarse entre ellos los canales o chat privados de la plataforma de juego *PlayStation* 4[31].

De otro, la policía francesa ha descubierto en sus investigaciones del ataque terrorista a una iglesia en Normandía, que los autores de la misma ni siquiera se conocían hasta cuatro días antes del ataque, pero sin embargo estaban en comunicación a través del sistema de mensajería instantánea «Telegram»[32], caracterizado por ser uno de los más inexpugnables para las Fuerzas de Seguridad.

Así, se ha llegado al punto de afirmar que «compañías norteamericanas como Twitter, Facebook, Google, Apple, Microsoft, Yahoo y otros servicios populares, incluyendo Youtobe, WhatsApp, Skype, Tumblr e Instagram están facilitando la yihad global»[33].

Estos foros actúan como un «firewall virtual para ayudar a proteger las identidades de los que participan, y ofrecen a los suscriptores la oportunidad de establecer un contacto directo con representantes terroristas, hacer preguntas, e incluso contribuir y ayudar a la ciber-yihad»[34].

Lo cierto es que redes sociales como Facebook o Twitter, son la puerta de entrada a la radicalización de los jóvenes, que una vez introducidos en la misma, pasan a utilizar canales privados de comunicación como Kick, WhatsApp o Telegram[35].

El hecho de que estos avances tecnológicos, que tanto han aportado a la sociedad en los últimos años, se estén utilizando para fines tan deleznables, es lo que debe llevar a plantearnos si la dificultad de control del uso de las TICs por los terroristas está supo-

---

31 «Cómo funciona el sistema de mensajería de la PS4 que podrían estar usando los terroristas», *El País,* 17 de noviembre de 2015. Disponible en: http://verne.elpais.com/verne/2015/11/16/articulo/1447671328_905417.html [Última consulta: 05-03-2017].

32 «Telegram, la aplicación preferida de la yihad», *La Razón,* 8 de agosto de 2016. Disponible en: http://www.larazon.es/internacional/telegram-la-aplicacion-preferida-de-la-yihad-AB13301405#.Ttt1meBVZmTYW2B [Última consulta: 05-03-2017].

33 «Terrorist Use of U.S. Social Media is a national security threat», *Forbes,* 30 de enero de 2015. Disponible en: http://www.forbes.com/sites/realspin/2015/01/30/terrorist-use-of-u-s-social-media-is-a-national-security-threat/#7e819c8012d0 [Última consulta: 05-03-2017].

34 G. Weimann, «New Terrorism and New Media», *Commons Lab of the Woodrow Wilson International Center for Scholars*, Washington, 2014, p. 1. Disponible en: https://www.wilsoncenter.org/publication/new-terrorism-and-new-media [Última consulta: 07-03-2017]. La traducción es mía.

35 USA Government, «Testimony before the House Foreign Affairs Committee Subcommittee on Terrorism, Nonproliferation, and Trade, The Honorable Mark D. Wallace», CEO, Counter Extremism Project, January 27, 2015, p. 2. Disponible en: http://docs.house.gov/meetings/FA/FA18/20150127/102855/HHRG-114-FA18-Wstate-WallaceM-20150127.pdf [Última consulta: 07-03-2017].

niendo una brecha en las estrategias de seguridad[36], y si es necesario un replanteamiento en materia de interceptación de esas comunicaciones, propugnando la monitorización continua de las mismas y de las redes sociales.

En 2011, Brian Michael Jenkins, Asesor del Presidente de los Estados Unidos, señalaba en el Congreso norteamericano que la estrategia para hacer frente a estos grupos terroristas, pasaba, entre otras medidas, «por la monitorización continua de los chats *on line* o la infiltración en las páginas webs»[37].

En abril de 2015, el ejército británico creaba una unidad, bajo el nombre de «Brigada 77», compuesta por 1.500 efectivos, expertos en operaciones psicológicas y uso de los medios sociales para participar en la guerra no convencional en la era de la información, los llamados «guerreros de Facebook» (*Facebook warriors*). La brigada será responsable de lo que se describe como una *guerra no letal*[38].

En la misma línea, en julio de 2015, se ponía en marcha, por parte de Europol, un nuevo equipo policial cuyo objetivo es el rastreo y bloqueo de cuentas de redes sociales vinculadas al Estado Islámico[39].

II. EL USO POR EL APARATO DEL ESTADO DE LAS NUEVAS TECNOLOGÍAS CON FINES DE INVESTIGACIÓN PENAL

Después de lo expuesto y en el contexto marcado, es el momento de preguntarnos hasta dónde llegan los límites de la utilización de las nuevas tecnologías por parte del Estado, en la lucha contra amenazas como el terrorismo, el crimen organizado y la ciber-

36 «El terrorismo pone en jaque la estrategia europea de seguridad», *El País,* 31 de julio de 2016. Disponible en: http://internacional.elpais.com/internacional/2016/07/30/actualidad/1469873907_441312.html [Última consulta: 07-03-2017].

37 Textualmente señala que «Theoretically, the strategies may include monitoring on-line chatter, disrupting or infiltrating websites, intervening overtly or covertly to challenge jihadist arguments, even setting up false-front networks to attract would-be terrorists». USA, «Jihadist Use of Social Media - How to prevent Terrorism and Preserve Innovation», Hearing before the Subcommittee on Counterterrorism and Inteligence of the Committe on Homeland Security, House of Representatives, December 6, 2011, Serial núm. 112-62. Disponible en: https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74647/html/CHRG-112hhrg74647.htm [Última consulta: 07-03-2017].

38 «British army creates team of Facebook warriors», *The Guardian,* 31 de enero de 2015. Disponible en: https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade [Última consulta: 07-03-2017].

39 BBC News, «Islamic State web accounts to be blocked by new police team», de 22 de junio de 2015. Disponible en: http://www.bbc.com/news/world-europe-33220037 [Última consulta: 07-03-2017].

delincuencia, en aras de proteger a los ciudadanos y mediante la invocación del concepto de seguridad nacional[40].

Partimos de que, como señala Cuerda Arnau[41] «el recurso a las nuevas tecnologías por el aparato estatal es la contrapartida del uso que de las mismas hace el delincuente y resultaría absurdo volverles la espalda en tanto que útiles instrumentos de la prevención del delito y, por ende, de la tutela de bienes jurídicos».

Se recrudece, por tanto, la tensión entre seguridad, como bien colectivo, y el respeto a los derechos fundamentales, si bien teniendo en cuenta que como señala Maculan, «el equilibrio entre estos intereses opuestos se desliza decididamente hacia la protección de la seguridad, con base en la presunta *excepcionalidad* de la amenaza a la que hay que hacer frente»[42].

1. **Sistemas de interceptación masiva de comunicaciones**

El avance de los medios tecnológicos de vigilancia ha permitido en los últimos años, el control de las comunicaciones de los ciudadanos en aras de la seguridad nacional de distintos Estados.

Es el denominado control estratégico de comunicaciones[43], destinado, según Cuerda Arnau, «al servicio de las funciones atribuidas a las agencias de inteligencia, o sea, las destinadas a prevenir y neutralizar amenazas a la defensa y seguridad nacional»[44], y que se diferencia de la vigilancia de las comunicaciones como medida de investigación utilizada por las Fuerzas y Cuerpos de Seguridad, generalmente[45], una vez producido el delito, para

[40] Abarca mucho más que la perspectiva nacional de seguridad, pasando a tener en la actualidad una «dimensión holística, esto es, múltiple y global». J.L. González Cussac, B. Larriba Hinojar y A. Fernández Hernández, «Seguridad Nacional y Derechos Fundamentales», en J.L. González Cussac (coord.), *Inteligencia*, Tirant lo Blanch, Valencia, 2012, p. 312.

[41] M.L. Cuerda Arnau, «Intervenciones prospectivas…» *cit.,* p. 117.

[42] E. Maculan, «Seguridad y globalización», en E. Maculan (ed.), *Seguridad internacional en un orden mundial de transformación*, Instituto Universitario General Gutiérrez Mellado de Investigación sobre la Paz, la Seguridad y la Defensa, Madrid, 2014, pp. 17-18.

[43] También denominado, «exploratorio, táctico, preventivo, general, prospectivo, (…)». R. Serra Cristóbal, «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», *Revista de Derecho Político,* UNED, núm. 92, enero-abril 2015, p. 81.

[44] M.L. Cuerda Arnau, «Intervenciones prospectivas…» *cit.,* p. 109.

[45] Vervaele advierte como es cada vez más frecuente el flujo libre de información derivada de las investigaciones secretas hacia los procedimientos penales. J.A.E. Vervaele, «Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal», en J. Pérez Gil (coord.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, Editorial La Ley, Madrid, 2012, p. 51.

el esclarecimiento del mismo, con la finalidad de incorporar su resultado a un proceso penal en curso.

Más ampliamente, se puede decir que la vigilancia estratégica es sólo una parte de una tendencia general hacia una vigilancia más activa de la población, mediante la recopilación de datos sobre un gran segmento de la población, reteniéndolo durante un período de años y a disposición para realizar las búsquedas oportunas [46].

A nadie se le escapa que la permanente vigilancia, así entendida, supone una injerencia intolerable en el derecho fundamental al secreto de las comunicaciones y el derecho a la vida privada de los ciudadanos.

La implementación de los mencionados sistemas se justifica en su finalidad proactiva, de prevención de ataques terroristas, adquiriendo lo que Maculan denomina «cierto rasgo probabilista y coercitivo» [47].

Los Estados tienen cada vez una mayor capacidad para realizar vigilancias simultáneas o en tiempo real, invasivas, específicas y a gran escala, con la particularidad de que el individuo vigilado desconoce que lo es y por lo tanto, no puede oponerse a tal práctica de manera alguna [48].

Naciones Unidas ya puso de manifiesto en 2013 que los Estados están buscando cada vez más para justificar el uso de las nuevas tecnologías, apoyarse en los viejos marcos legales existentes, sin reconocer que las capacidades ampliadas que ahora poseen van mucho más allá de lo previsto dichos marcos. Al mismo tiempo, las leyes están siendo adoptadas para ampliar el alcance de las excepciones de seguridad nacional, que prevén la legitimación de las técnicas de vigilancia intrusiva y sin supervisión o revisión independiente [49], esto es, sin autorización judicial. Se ponen al respecto varios ejemplos [50]:

— En la India se permite la interceptación de las comunicaciones en el interés de, entre otras cosas, la soberanía, la integridad o la defensa de la India, las relaciones de amistad con otros Estados, el orden público y la investigación de cualquier delito.

---

[46] Consejo de Europa, «The democratic oversight of signals intelligence agencies». Report of the European Commission for Democracy through Law (Venice Commission), Venice, 20-21 march 2015, párrafo 57, *Mass surveillance. Who is watching the watcher?*, Council of Europe, april, 2016, p. 67.

[47] E. Maculan, «Seguridad…» *cit.,* p. 18.

[48] Naciones Unidas. Asamblea General, «Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression», Frank La Rue, A/HRC/23/40, de 17 de abril de 2013, párrafo 33, p. 10. Disponible en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [Última consulta: 12-03-2017].

[49] Naciones Unidas. Asamblea General, «Report of the Special…» *cit.,* párr. 50, p. 13.

[50] Naciones Unidas. Asamblea General, «Report of the Special…» *cit.,* párrafos 58-59, p. 15.

— En Suecia se autoriza a la agencia de inteligencia sueca para interceptar sin orden judicial todo el tráfico telefónico y de Internet que tienen lugar dentro de las fronteras de Suecia.
— En Tanzania se permite que los servicios de inteligencia del país puedan llevar a cabo investigaciones de cualquier persona o entidad respecto de la que se tenga motivos razonables para considerarla un riesgo o una fuente de riesgo o una amenaza para la seguridad del Estado.
— La legislación alemana permite las escuchas telefónicas automatizadas de comunicaciones nacionales e internacionales, sin orden judicial, por parte de los servicios de inteligencia del Estado, a efectos de proteger el libre orden democrático, la existencia o la seguridad del Estado.

No obstante, esta tendencia no es algo nuevo.

El 6 de junio de 2013, el periódico británico *The Guardian* publicaba en exclusiva que la Agencia de Seguridad Nacional de Estados Unidos (NSA)[51], tenía acceso, mediante una orden judicial secreta, a registros telefónicos y de internet de millones de usuarios de la operadora de telefonía norteamericana *Verizon*[52].

El gobierno americano defiende la interceptación de las comunicaciones, por considerarlo esencial en la lucha contra el terrorismo. Así mismo, explica que el sistema «permite al personal especializado en antiterrorismo descubrir si terroristas conocidos o sospechosos han estado en contacto con otras personas que pueden estar implicadas en actividades terroristas, particularmente aquellas localizadas dentro de Estados Unidos»[53].

Después de la promulgación de la *USA Patriot Act*[54], el Secretario de Justicia, John Ashcroft, anunciaba una «segunda ofensiva» de medidas antiterroristas, en una declaración en la que ya se podía perfilar el cambio que se avecinaba en la materia: «El juicio de la historia nos condenaría si no utilizáramos todas las armas a nuestro alcance para proteger Estados Unidos del terrorismo. Vamos a usar todas las tácticas de inteligencia, de procedimiento criminal o de inmigración. Vamos a perseguir el terrorismo en Internet,

51 En inglés: *National Security Agency*, también conocida como NSA.

52 «NSA collecting phone records of millions of Verizon customers daily», *The Guardian*, 6 de junio de 2013. Disponible en: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [Última consulta: 12-03-2017].

53 «La Casa Blanca asegura que el registro de llamadas es vital para combatir el terrorismo», *20 minutos,* 6 de junio de 2013. Disponible en: http://www.20minutos.es/noticia/1836328/0/casa-blanca/registro-llamadas/terrorismo/ [Última consulta: 12-03-2017].

54 Acrónimo de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*.

vamos a abrir sus correos electrónicos antes de que ellos lo hagan, a escuchar sus mensajes telefónicos, a interceptar sus conversaciones»[55].

Las revelaciones realizadas por los periódicos *The Guardian* y *The Washington Post,* procederían de la filtración de distinta documentación proporcionada por Edward Snowden[56], consultor de la NSA[57].

El programa utilizado para las mencionadas prácticas, respondía al nombre de *PRIMS,* y permitía a la NSA desde 2007, captar correos electrónicos, videos, fotografías, llamadas de voz e imagen, actividad en las redes sociales, contraseñas y otros datos de usuarios, centrándose en comunicaciones extranjeras que a menudo se canalizan a través de las principales empresas de internet en Estados Unidos[58].

La recopilación de información estaría amparada, según la Casa Blanca, por la Ley de Vigilancia de Inteligencia Extranjera (FISA)[59] de 1978[60], aprobada durante el mandato del Presidente Jimmy Carter[61], de conformidad con el art. 215 de la *USA Patriot Act*[62].

La orden no afectaría al contenido de las comunicaciones ni a los datos personales de los usuarios, pero sí incluye el número de origen y de destino de las llamadas, cuando se llevaron a cabo o la duración de la conversación, en definitiva, los metadatos, que pueden

---

55 «Bush planea rediseñar y controlar el tráfico en Internet», *El País,* 26 de octubre de 2001. Disponible en: http://elpais.com/diario/2001/10/26/internacional/1004047211_850215.html [Última consulta: 12-03-2017].

56 Para ver la cronología de las revelaciones: «Cronología del "caso Snowden", el joven que reveló el espionaje masivo de Estados Unidos», *20 minutos,* 7 de julio de 2013. Disponible en: http://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/ [Última consulta: 12-03-2017].

57 «Edward Snowden: the whistleblower behind the NSA surveillance revelations», *The Guardian,* 11 de junio de 2013. Disponible en: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [Última consulta: 12-03-2017].

58 «U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program», *The Washington Post,* 7 de junio de 2013. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 [Última consulta: 13-03-2017].

59 *Foreing Intelligence Surveillance Act.*

60 USA, *Foreign Intelligence Surveillance Act* (FISA), de 25 de octubre de 1978. Disponible en: http://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf [Última consulta: 12-03-2017].

61 En 2012, el Senado estadounidense votó por mayoría la ampliación de los poderes concedidos por la Ley FISA por cinco años más, es decir, hasta 2017.

62 Aprobada por el Congreso de los Estados Unidos el 24 de octubre de 2001, representa, según Perarnau Moya, la nueva mentalidad americana, «hacer prevalecer la seguridad», añadiendo el autor que «Responde, pues, a la idea que una mayor información supone necesariamente una mayor seguridad, y que dadas las actuales circunstancias, ésta debe prevalecer frente a los principios fundamentales de libertad e intimidad». J. Perarnau Moya, «Internet amenazada», *Internet y Derecho penal,* Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, núm. 10, 2001, p. 137.

ser conservados por la NSA durante un periodo de cinco años, a fin de poder realizar, incluso, un análisis retrospectivo de los mismos.

El sistema funciona de la siguiente manera: los analistas de la NSA acceden a la información recopilada mediante un buscador en la base de datos. Se realiza una consulta en ese buscador a través de un «identificador», por ejemplo un número de teléfono concreto y todos sus datos asociados. Al identificador usado para empezar la consulta en la base de datos, se le denomina «semilla», y su uso debe ser aprobado por uno de los veintidós funcionarios designados por la NSA. Esa aprobación sólo se producirá cuando el funcionario en cuestión entienda que existe una sospecha razonable de que el dato concreto objeto de la consulta (ej. número de teléfono), se asocia a alguna organización terrorista extranjera.

Cuando los analistas consultan una «semilla», los resultados de la consulta se limitan a tres «saltos» o niveles desde la misma.

El primer salto o nivel incluye, por tanto, la «semilla» y los metadatos asociados a la misma. Siguiendo con el ejemplo, si la semilla es un número de teléfono, este primer nivel de consulta incluirá todos los metadatos asociados al mismo, esto es, todos los números de teléfono a los que ha realizado llamada y todos de los que la ha recibido en los últimos cinco años (para verlo gráficamente, pongamos que 100 en total). El segundo nivel de consulta incluiría todos los número de teléfono a los que cada uno de esos 100 números han llamado o de los que han recibido llamada en los últimos cinco años (lo que haría un total de 10.000). El tercer y último nivel de consulta incluiría por tanto, todos los números de teléfono a los que cada uno de esos 10.000 números ha llamado o de los que han recibido llamada en los últimos cinco años (lo que haría un total de 1.000.000)[63].

Con esta explicación se puede llegar a apreciar la dimensión y capacidad operativa del sistema, a lo que habría que añadir, que al recabarse autorización judicial para la primera «consulta», el resto, que como vemos se multiplican exponencialmente, estarían amparadas por esa autorización judicial inicial y genérica; en definitiva, «permite actuar contra ciudadanos no norteamericanos sin la necesidad de una orden judicial individual»[64].

El escándalo también salpicó al Reino Unido. *The Guardian* reveló que la agencia de espionaje británica, conocida por sus siglas en inglés GCHQ, estaba «pinchando» cables de fibra óptica que transportan comunicaciones electrónicas y que estaba compartiendo

[63] Sistema de funcionamiento explicado en la primera demanda civil presentada ante los Tribunales estadounidenses, tras las revelaciones de las prácticas de la NSA. USA, Civil Action núm. 13-0851 (RJL), *Klayman vs. Obama*, Courts for the District of Columbia, december 16, 2013.

[64] A. Sorroza y C. García Encina, «Las filtraciones de la NSA: entre lo transatlántico y lo doméstico», *Real Instituto Elcano,* Comentario Elcano 43/2013, 28 de julio de 2013, p. 1. Disponible en: www.realinstitutoelcano.org [Última consulta: 12-03-2017].

grandes cantidades de datos con su homóloga norteamericana, a través de un programa conocido como *Tempora*[65].

Las investigaciones posteriores a raíz de las revelaciones mencionadas, ponen de manifiesto la existencia de numerosos programas de vigilancia masiva, utilizados de manera habitual por la NSA norteamericana y también por otros países aliados. En este punto destacan, entre otros, además de *Prism* y *Tempora*:

— *Xkeyscore*: permite a la NSA buscar, sin previa autorización, en sus bases de datos correos electrónicos, conversaciones en línea e historiales de navegación de millones de personas, así como sus metadatos[66]. La propia NSA ha confirmado su existencia[67].

— *Bullrun*: para la elusión del cifrado en línea, permitiría burlar la encriptación en línea empleada por millones de personas en sus transacciones *on line* y correos electrónicos[68].

— *Boundless Informant:* permite seleccionar un país en el mapa, ver el volumen de metadatos y seleccionar los detalles de las recopilaciones de ese país[69]. Mediante la extracción de datos, permitiría a la NSA registrar y analizar la información electrónica mundial[70].

— *Muscular*: permite interceptar, de enlaces privados, el tráfico de datos que fluye entre los servidores de Yahoo, Google, Microsoft, Hotmail y Windows Live Messenger, entre otros[71]. Según el Parlamento Europeo, «El punto de acceso, DS-200B, se encuentra fuera de los Estados Unidos, lo que hace que el programa

---

65 «GCHQ taps fibre-optic cables for secret access to world's communications», *The Guardian,* 21 de junio de 2013. Disponible en: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Última consulta: 12-03-2017].

66 «XKeyscore: NSA tool collects "nearly everything a user does on the internet"», *The Guardian,* 31 de julio de 2013. Disponible en: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [Última consulta: 12-03-2017].

67 USA. NSA, *Press Statement on 30 July 2013.* Disponible en: https://www.nsa.gov/news-features/press-room/public-announcements/2013/30-july-2013.shtml [Última consulta: 12-03-2017].

68 «N.S.A. Able to Foil Basic Safeguards of Privacy on Web», *The New York Times,* 5 septiembre de 2013. Disponible en: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=1 [Última consulta: 12-03-2017].

69 «Boundless Informant: the NSA's secret tool to track global surveillance data», *The Guardian,* 11 de junio de 2013. Disponible en: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [Última consulta: 12-03-2017].

70 Unión Europea. Parlamento Europeo. Comisión de libertades civiles, justicia y asuntos de interior, *Documento de Trabajo 1, sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos*, de 11 de diciembre de 2013, p. 4.

71 «NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say», *The Washington Post,* 30 de octubre de 2013. Disponible en: https://www.washingtonpost.com/world/national-

esté fuera de la jurisdicción del Tribunal de Vigilancia de Inteligencia Extranjera (FISC) y depende de un proveedor de telecomunicaciones anónimo para proporcionar un acceso secreto a un cable o conmutador por el que pasa el tráfico de comunicaciones»[72].

— *Edgehill*: programa de descifrado, dirigido por la agencia de seguridad británica GCHQ.
— *Quantumtheory y Foxacid*: para el ataque selectivo mediante intermediarios contra sistemas de información.
— *Dishfire*: permite la recopilación y retención de 200 millones de mensajes de texto diarios[73].

A pesar de lo que pudiera parecer a simple vista, en el sentido de que los ciudadanos del mundo parecen haber abierto los ojos ante el uso por parte de los Estados de sistemas de vigilancia masiva desde las revelaciones de Edward Snowden[74], lo cierto es que más de una década antes de las mismas, en 2001, ya se puso de manifiesto tales prácticas a través de un programa con nombre en clave *Echelon*, liderado también por Estado Unidos[75].

Echelon es considerado por Cuerda Arnau como «la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia». Es controlada por Estados Unidos, Canadá, Gran Bretaña, Australia, y Nueva Zelanda, actualmente conocidos como

security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [Última consulta: 12-03-2017].

72 Unión Europea. Parlamento Europeo. Comisión de libertades civiles, justicia y asuntos de interior, *Documento de Trabajo 1, sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos*, de 11 de diciembre de 2013, p. 4.

73 Unión Europea. Parlamento Europeo. Comisión de libertades civiles, justicia y asuntos de interior, «Informe 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, Ponente: Claude Moraes, de 21 de febrero de 2014, p. 22. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES [Última consulta: 12-03-2017].

74 Ya el propio Parlamento Europeo reconoce que «la vigilancia no es nueva, pero hay pruebas suficientes de una escala sin precedentes en el alcance y la capacidad de las agencias de inteligencia que hacen preciso que la UE actúe». Unión Europea. Parlamento Europeo. Comisión de libertades civiles, justicia y asuntos de interior, «Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU…» *cit.,* p. 54.

75 Ver: D. Murakami Wood y S. Wright, «Before and after Snowden», *Surveillance & Society,* Vol. 13, núm. 2, 2015, pp. 132-138. Disponible en: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/snowden_editorial/snowden_ed [Última consulta: 15-03-2017].

Five Eyes[76]. El sistema permite la captura de comunicaciones por radio y satélite, llamadas de teléfono, faxes y e-mails en casi todo el mundo e incluye el análisis automático y clasificación de las interceptaciones.

Su funcionamiento es descrito por Cuerda Arnau: «En sus numerosas estaciones de interceptación captura las conversaciones y, después, cada estación selecciona dicha información pasada por el tamiz de lo que podría denominarse «diccionarios de palabras clave» (sospechosas o peligrosas) diseñados por los Estados en función de los concretos intereses que cada uno pueda tener en ese particular momento. Posteriormente, la referida información o bien se transcribe y registra o bien se elimina, que es, al parecer, lo que sucede con la mayoría ante las dificultades para hacer frente a su almacenamiento y procesamiento» [77].

El Parlamento Europeo ya puso de manifiesto, en relación a este sistema, varias cuestiones[78]:

1. Únicamente se permite este tipo de intervenciones cuando se trata de garantizar la seguridad nacional y siempre que las normas por las que se rigen estén previstas en el Derecho nacional, sean accesibles a todos y precisen en qué circunstancias y bajo qué condiciones pueden efectuarlas las autoridades.
2. Tales intervenciones deben ser proporcionadas, por lo que debe establecerse un equilibrio entre los intereses en juego, ya que según la jurisprudencia del Tribunal Europeo de Derechos Humanos no es suficiente que estas medidas sean necesarias o deseables.
3. Un sistema de inteligencia que interceptase aleatoria y permanentemente todos los mensajes violaría el principio de proporcionalidad y sería contrario al art. 8 del Convenio Europeo de los Derechos Humanos.
4. Para que las actividades jurídicamente legitimadas de los servicios de inteligencia sean compatibles con los derechos fundamentales es necesaria, además, la existencia de suficientes mecanismos de control para contrarrestar los peligros que conllevan las actividades secretas de determinados segmentos del aparato de la Administración.

---

[76] Aunque hay más «ojos» en Europa. Al respecto ver: Consejo de Europa, Recommendation 2067 (2015), Explanatory memorándum, on 21 April 2015, *Mass surveillance. Who is watching the watcher?*, Council of Europe, April, 2016, p. 18-19.

[77] M.L. Cuerda Arnau, «Intervenciones prospectivas…» *cit.,* pp. 109-110.

[78] Unión Europea. Parlamento Europeo. Comisión temporal sobre el sistema de interceptación Echelon, «Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON)» (200112098(INI)), Ponente: Gerhard Schmid, FINAL AS-0264/2001PARTE 1, de 11 de julio de 2001, pp. 16-17.

Así mismo alertaba de los peligros de un sistema como *Echelon* para la vida privada y la economía, no sólo basados en sus capacidades técnicas, que se demuestran a nivel mundial, sino también y sobre todo de su funcionamiento en un «ámbito carente casi por completo de regulación jurídica»[79].

Debemos partir de que la vigilancia e interceptación masiva de las comunicaciones debe ser considerada como un acto altamente intrusivo, que potencialmente interfiere con el derecho a la vida privada y amenaza los cimientos de una sociedad democrática.

Las revelaciones de sistemas de interceptación del que forman parte Estados repartidos por varios continentes, pone de manifiesto una tendencia preocupante, «la ampliación de las competencias de vigilancia más allá de las fronteras territoriales»[80]. A ello hay que añadir que muchas de esas comunicaciones, con independencia del lugar en que se originen, pasan por servidores ubicados en territorio americano.

Así mismo, ha quedado demostrado que algunos Estados de la Unión Europea, como Alemania o Reino Unido, han permitido la instalación en su territorio de las estaciones terrestres o mecanismos tecnológicos adecuados para permitir esas interceptaciones[81], a la par que se beneficiaban de los resultados.

Ello ha llevado a entender que la NSA y sus socios extranjeros, el llamado grupo *Five Eyes*, eluden las restricciones nacionales mediante el intercambio de datos sobre los ciudadanos de cada uno[82].

III. PARÁMETROS DEL TEDH RESPECTO A LA INJERENCIA EN EL DERECHO A LA VIDA PRIVADA POR SISTEMAS DE VIGILANCIA E INTERCEPTACIÓN MASIVA DE COMUNICACIONES

Después de analizar la polémica que envuelve el uso de técnicas de investigación tan intrusivas, debemos plantearnos si, a pesar de lo dicho, las mismas deben ser o no utilizadas en la lucha contra el terrorismo internacional.

Siguiendo a Sottiaux, «la cuestión fundamental consiste en considerar si los estándares de privacidad propios de las investigaciones criminales ordinarias deben ser los mismos

[79] Unión Europea. Parlamento Europeo. Comisión temporal sobre el sistema de interceptación Echelon, «Informe sobre…» *cit.,* p. 29.

[80] Naciones Unidas. Asamblea General, «Report of the Special…» *cit.*, párr. 64, p. 17.

[81] Unión Europea. Parlamento Europeo. Comisión temporal sobre el sistema de interceptación Echelon, «Informe sobre…» *cit.,* p. 95.

[82] Consejo de Europa. Committee on legal affairs and human rights, *Mass surveillance*, AS/Jur (2015) 01, de 26 enero 2015, p. 2.

que para la prevención del terrorismo donde, por su naturaleza y gravedad, se ven implicadas además agencias de seguridad o servicios secretos»[83].

Para tratar de dar respuesta a esta cuestión, es necesario analizar la jurisprudencia del TEDH en la materia[84].

El punto de partida es entender que la vigilancia masiva de comunicaciones constituye una injerencia en el derecho a la privacidad contenido en el art. 8 CEDH, si bien la misma podría tolerarse por las razones contenidas en el apartado segundo: «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».

El TEDH ya hizo referencia a estas cuestiones, por ejemplo en el caso *Klass y otros c. Alemania,* donde establece que los poderes de vigilancia secreta de los ciudadanos sólo son tolerables en el marco del CEDH, en la medida en que sean estrictamente necesarios para salvaguardar las instituciones democráticas[85].

Reconoce que las sociedades democráticas están amenazadas por el terrorismo y que el Estado debe ser capaz, con el fin de contrarrestar de manera eficaz esa amenaza, de llevar a cabo una vigilancia secreta de los «elementos subversivos» que operan en su territorio. Sobre esa base, el Tribunal acepta que, bajo circunstancias excepcionales, este tipo de vigilancia es necesaria en una sociedad democrática y en interés de la seguridad nacional[86]. No obstante, cualquiera que sea el sistema de vigilancia que se adopte, deben existir garantías adecuadas y efectivas contra el abuso[87].

Posteriormente ha habido otros importantes pronunciamientos en materia de vigilancia e interceptación masiva de comunicaciones[88]: caso *Weber y Saravia c. Alemania*, con sentencia de 29 de junio de 2006; el caso *Liberty y otros c. Reino Unido*, con sentencia de

---

83 S. Sottiaux, *Terrorism and the limitation of rights. The ECHR and the US Constitution,* Hart Publishing, Oxford, 2008, p. 274.

84 En el contexto de la protección de datos, ver: E. Salamanca Aguado, «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones», *Revista del Instituto Español de Estudios Estratégicos*, (IEEE), núm. 4, 2014, pp. 151-175.

85 Sentencia TEDH de 4 de julio de 1978, *Klass y otros c. Alemania,* párrafo 42.

86 *Ibídem*, párrafo 48.

87 *Ibídem,* párrafo 50.

88 Otros casos, que versan sobre esta materia, están pendientes en el momento actual de una resolución por parte del TEDH: *Hannes Tretter y otros c. Austria*, comunicado al gobierno austriaco el 5 de mayo de 2013; *Big Brother Watch y otros c. Reino Unido*, comunicado al gobierno británico el 7 de enero de 2014; *Association confraternelle de la presse judiciaire y otros c. Francia*, presentado el 3 de octubre de 2015.

1 de julio de 2008; el caso *Shimovolos c. Russia,* con sentencia de 21 de junio de 2011; el caso *Zakharov c. Rusia*, con sentencia de 4 de diciembre de 2015; y el caso *Szabó y Vissy c. Hungría*, con sentencia de 12 de enero de 2016.

A) En el caso *Weber y Saravia c. Alemania,* el TEDH se ocupa de la llamada vigilancia estratégica o *strategic monitoring,* utilizada para identificar y evitar un ataque armado o un ataque terrorista.

Aunque el derecho a la intimidad no es absoluto, esto no implica una suspensión automática por motivos de seguridad nacional[89]. El Tribunal hace referencia a que la mera existencia de una ley que permite la vigilancia secreta de las comunicaciones, implica que cualquiera puede ser objeto de esa vigilancia, añadiendo que «Esta amenaza afecta necesariamente a la libertad de comunicación entre los usuarios de los servicios de telecomunicaciones y de este modo equivale en sí misma a una injerencia en el ejercicio de los derechos de los demandantes en virtud del art. 8, con independencia de las medidas efectivamente adoptadas contra ellos»[90].

Entiende por tanto, que la injerencia en el derecho a la vida privada entendido de conformidad con el art. 8 CEDH, se ha producido. No obstante, señala que esa injerencia está prevista en una ley nacional alemana, y por ello, existe una base jurídica suficiente para la adopción de las medidas que en el caso se impugnan[91].

Que esté prevista por la ley exige, además, «que sea compatible con la preeminencia del derecho y accesible a la persona afectada quien, asimismo, ha de poder prever sus consecuencias»[92]. Ahora bien, esa previsibilidad «no puede significar que una persona debe ser capaz de prever cuando las autoridades van a interceptar su comunicaciones para que pueda adaptar su conducta en consecuencia, sino que está destinada a evitar la arbitrariedad y el abuso por parte del Estado, de manera que «el derecho interno debe ser suficientemente claro en sus términos para dar a los ciudadanos una indicación adecuada en cuanto a en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas»[93].

Entiende que el objetivo de la vigilancia era preservar la seguridad nacional[94], y reitera que, al valorar el interés del Estado en la protección de su seguridad nacional a través de medidas de vigilancia secretas frente a la injerencia al respeto de la vida privada, se ha

---

89 Unión Europea. Parlamento Europeo. Comisión de libertades civiles, justicia y asuntos de interior, *Documento de Trabajo 1, sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos*, de 11.12.2013, p. 8.

90 Sentencia TEDH de 29 de junio de 2006, *Weber y Saravia c. Alemania,* párrafo 78.

91 *Ibídem,* párrafos 85-91.

92 *Ibídem,* párrafo 84.

93 *Ibídem,* párrafo 93.

94 *Ibídem,* párrafo 104.

reconocido siempre a las autoridades nacionales, que gozan de un amplio margen libertad en la elección de los medios que permitan alcanzar ese objetivo legítimo.

Por ello, el Tribunal ha de valorar:

1. Si la injerencia es necesaria en una sociedad democrática para la defensa de la seguridad nacional[95]. En esa valoración se tienen en cuenta todas las circunstancias del caso, como la naturaleza, el alcance y la duración de las posibles medidas, las razones necesarias para su adopción, las autoridades competentes para su autorización, práctica y supervisión, y el tipo de recurso previsto por la legislación nacional para los afectados por las mismas[96]. En relación a este último punto, el Tribunal, entendiendo que el carácter secreto de la vigilancia es consustancial a la misma, recuerda que la cuestión de la notificación posterior de las medidas de vigilancia está inextricablemente ligada a la eficacia de los recursos ante los tribunales y por lo tanto a la existencia de una protección eficaz contra el abuso de las facultades de control. Por ello, entiende que tan pronto como la notificación puede llevarse a cabo sin poner en peligro la finalidad de la restricción, después de la terminación de la medida de vigilancia, la información debe proporcionarse a las personas afectadas[97].
2. Si la injerencia es proporcionada a la finalidad legitima perseguida[98].

En definitiva, el TEDH aplica a las llamadas vigilancias estratégicas las mismas salvaguardas que a cualquier otro tipo de interceptación de comunicaciones[99], para concluir con la desestimación de la demanda, al haberse dado cumplimiento a las mismas por el Estado demandado.

B) En el caso *Liberty y otros c. Reino Unido,* el TEDH reproduce los argumentos anteriormente reseñados, esto es, la existencia de la injerencia a la vida privada de conformidad con el art. 8.1 CEDH por parte del Reino Unido. Sobre si esa injerencia está o no justificada de acuerdo a los criterios del apartado segundo del mencionado precepto, también entiende que «no considera que exista ninguna razón para aplicar unos principios diferentes respecto a la accesibilidad y claridad de las normas que rigen la intervención de

95 *Ibídem,* párrafo 105.
96 *Ibídem,* párrafo 106.
97 *Ibídem,* párrafo 135.
98 *Ibídem,* párrafo 107.
99 Según el párrafo 95, la naturaleza de las infracciones que puedan dar lugar a una orden de interceptación; la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento que deberá seguirse para el examen, uso y conservación de los datos obtenidos; las precauciones que se han de tomar al comunicar los datos a otras partes; las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de las cintas. Sentencia TEDH de 29 de junio de 2006, *Weber y Saravia c. Alemania,* párrafo 95.

las comunicaciones individuales, de un lado, y a programas de vigilancia más generales, de otro»[100].

A pesar de ello, el Tribunal no considera que la legislación interna indicara con la suficiente claridad el alcance o el ejercicio de la amplia discreción conferida al Estado para interceptar y examinar las comunicaciones externas, como para ofrecer la adecuada protección contra el abuso de poder. En particular, no indicaba de forma accesible al público, tal y como exige la jurisprudencia del Tribunal, ningún procedimiento a seguir para seleccionar y examinar, intercambiar, conservar y destruir la información interceptada. Por tanto, la injerencia en los derechos de los demandantes en virtud del art. 8 no estaba «prevista por la Ley»[101].

C) En el caso *Shimovolos c. Russia,* el Tribunal afirma que allí donde existe un poder que se ejerce en secreto por el ejecutivo, los riesgos de arbitrariedad son evidentes. Por tanto, es esencial contar con reglas claras y detalladas sobre la aplicación de las medidas de vigilancia secreta, sobre todo porque la tecnología disponible para su uso es cada vez más sofisticada.

La ley debe ser lo suficientemente clara en sus términos para dar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades tienen el poder de recurrir a una medida de vigilancia secreta y de recogida de datos.

Además, debido a la falta de escrutinio público y el riesgo de abuso intrínseco a cualquier sistema de vigilancia secreta, deberá plasmarse en una ley interna las siguientes garantías mínimas para evitar abusos: la naturaleza, el alcance y la duración de las posibles medidas, las razones necesarias para su adopción, las autoridades competentes para su autorización, práctica y supervisión, y el tipo de recurso previsto por la legislación nacional para los afectados por las mismas[102].

D) En el caso *Zakharov c. Rusia,* a diferencia de los casos anteriores, el demandante afirma que ha habido una injerencia en sus derechos como consecuencia de la mera existencia de una legislación que permite la intercepción secreta de las comunicaciones telefónicas móviles y el riesgo de ser sometido a esas medidas de interceptación, pero la demanda no se produce como consecuencia de haber sido víctima de una concreta interceptación[103].

Es de destacar los pronunciamientos del Tribunal en cuanto al control y supervisión de los sistemas de vigilancia masiva, incardinados, como ya puso de manifiesto anteriormente, en el requisito de «necesidad en una sociedad democrática». A este respecto

100 Sentencia TEDH 1 de julio de 2008, *Liberty y otros c. Reino Unido*, párrafo 63.
101 *Ibídem*, párrafo 69.
102 Sentencia TEDH 21 de junio de 2011, *Shimovolos c. Russia*, párrafo 68.
103 Sentencia TEDH 4 de diciembre de 2015, *Zakharov c. Rusia*, párrafo 163.

entiende que la supervisión y control de las medidas de vigilancia secreta se puede producir en tres etapas[104]:

— cuando se ordena la vigilancia,
— cuando se está llevando a cabo,
— cuando ya ha finalizado.

El carácter secreto de una vigilancia de estas características hace consustancial a la misma, que las dos primeras etapas se desarrollen sin conocimiento del individuo. Dado, por tanto, que estas circunstancias le impedirán tomar parte en cualquier procedimiento de revisión, es esencial que los procedimientos establecidos proporcionen garantías adecuadas para salvaguardar sus derechos.

En un campo donde el abuso es potencialmente tan fácil en casos individuales y podría tener consecuencias nocivas para la sociedad democrática en su conjunto, es en principio deseable confiar el control y supervisión a un juez, en la medida en que el control judicial ofrece las mejores garantías de independencia, imparcialidad y un procedimiento adecuado.

En cuanto a la tercera etapa, después de que la vigilancia se ha terminado, ya se había sostenido por el Tribunal que la cuestión de la notificación posterior de las medidas de vigilancia está inextricablemente ligada a la eficacia de los recursos ante los tribunales y, por tanto, a la existencia de una protección eficaz contra el abuso de las facultades de control.

En el caso concreto, el Tribunal observa que en Rusia las personas cuyas comunicaciones han sido interceptadas, no son notificadas de este hecho en ningún momento y bajo ninguna circunstancia. De ello se desprende que, a menos que el proceso penal se llegue a abrir en contra del sujeto de la interceptación y los datos interceptados sean utilizados como pruebas, es poco probable que la persona en cuestión llegue a saber que se han interceptado sus comunicaciones[105].

También se destaca que, en el presente caso, el control judicial se limita a la fase de autorización inicial, quedando el control del resto de las etapas mencionadas en manos de distintas autoridades del poder ejecutivo[106], por lo que el Tribunal entiende que la legislación rusa en materia de interceptación de comunicaciones, no alcanza los estándares exigidos de respeto a la vida privada.

E) En el caso *Szabó y Vissy c. Hungría,* sobre la legislación húngara en materia de vigilancias secretas antiterroristas, por medio de la cual se habilita la interceptación masiva de datos, se aplica toda la doctrina sentada por la Corte en las resoluciones anteriores.

104 *Ibídem*, *Zakharov c. Rusia*, párrafo 233.
105 *Ibídem*, *Zakharov c. Rusia*, párrafo 289.
106 *Ibídem*, párrafos 274-285.

En el examen de la «previsibilidad de la ley», entiende que la redacción de la ley húngara que autoriza la interceptación de las comunicaciones en relación a las personas que pueden ser objeto de la misma, es demasiado amplia, contribuyendo a allanar el camino para interceptar las comunicaciones de cualquier ciudadano[107].

El Tribunal entiende normal que, teniendo en cuenta las circunstancias del terrorismo actual, los gobiernos recurran a las tecnologías de vanguardia para adelantarse a los ataques terroristas, incluyendo el monitoreo masivo de comunicaciones susceptibles de contener indicios de incidentes inminentes.

Las técnicas aplicadas en tales operaciones de seguimiento han demostrado un progreso y sofisticación notable en los últimos años, especialmente respecto a la generalización de la recopilación sistemática y automatizada de datos.

A la vista de estos avances, la Corte debe examinar la cuestión de si el desarrollo de métodos de vigilancia que tienen como resultado la recopilación de grandes cantidades de datos, se ha visto acompañado por un desarrollo simultáneo de las salvaguardas jurídicas que garanticen el respeto de los derechos de los ciudadanos garantizados por el CEDH[108].

Dado el carácter particular de la injerencia en cuestión y el potencial de las tecnologías de vigilancia de última generación para invadir la privacidad de los ciudadanos, la Corte considera que el requisito de «necesarias en una sociedad democrática» del art. 8.2 CEDH, debe interpretarse en el sentido de que se exige «estricta necesidad» en un doble sentido:

— si es estrictamente necesaria, en términos generales, para la salvaguarda de las instituciones democráticas y,
— si es estrictamente necesaria, en términos particulares, para la obtención de inteligencia vital en una operación individual.

En opinión del Tribunal, cualquier medida de vigilancia secreta que no sea conforme a estos criterios, será propensa al abuso por parte de las autoridades de la tecnología que tienen a su disposición[109].

A ello hay que añadir la ausencia de autorización judicial previa para las interceptaciones, siendo autorizadas por el Ministro de Justicia, lo que no ofrece las suficientes garantías en orden a valorar la necesidad de las medidas a adoptar, a juicio del Tribunal[110].

La práctica cada vez más generalizada de los gobiernos de transferir y compartir entre ellos la inteligencia obtenida en virtud de vigilancia secreta, hace que el control *a posteriori* de las actividades de vigilancia, preferentemente judicial, adquiera verdadera importancia

107 Sentencia TEDH 12 de enero de 2016, *Szabó y Vissy c. Hungría*, párrafos 66-67.
108 *Ibídem*, párrafo 68.
109 *Ibídem*, párrafo 73.
110 *Ibídem*, párrafos 75-77.

en el reforzamiento de la confianza de los ciudadanos en el respeto de sus garantías en un Estado de Derecho[111].

Se reconoce que las especiales características del terrorismo actual puede llevar a situaciones de emergencia en que la exigencia de autorización judicial no sea factible, o incluso contraproducente por la necesidad de conocimientos especiales, o simplemente supondría la pérdida de un tiempo precioso. En estos casos en que no es posible una autorización judicial previa, y en que las medidas son adoptadas por una autoridad del ejecutivo, es necesaria una revisión *post factum,* por medio de una autoridad judicial[112].

En definitiva, la Corte no está convencida de que la legislación húngara ofrezca garantías suficientemente precisas, eficaces e integrales de la ordenación, la ejecución y el potencial de reparación de los tales medidas.

Dado que el alcance de las medidas podría incluir prácticamente a cualquier persona, que la ordenación se lleva a cabo en su totalidad en el ámbito del poder ejecutivo y sin una evaluación de estricta necesidad, que las nuevas tecnologías permiten al gobierno interceptar grandes cantidades de datos relativos incluso a personas ajenas a la operación investigada en cuestión, y dada la ausencia de medidas correctivas eficaces, lejos del ámbito judicial, la Corte concluye que ha habido una violación del art. 8 de la Convención[113].

En conclusión, partiendo, por tanto, de que los sistemas de vigilancia masiva de comunicaciones representan por sí mismos una injerencia en el derecho a la vida privada de conformidad con el apartado primero del art. 8 CEDH, y sosteniendo que en casos como el terrorismo, esa injerencia puede estar justificada en virtud del apartado segundo del citado artículo, se pueden enumerar las siguientes condiciones que ha de reunir un sistema de estas características para ser conforme a derecho, según la jurisprudencia del TEDH:

A) Previsibilidad de la ley: Implicaría la concurrencia de los siguientes requisitos:
   1. Ha de estar previsto en una ley interna.
   2. Ha de especificar de manera clara en qué circunstancias y bajo qué condiciones se habilita a los poderes públicos a tomar tales medidas. En este sentido, son de aplicación las garantías mínimas que deben figurar en la ley para cualquier intervención de comunicaciones, fijadas por la jurisprudencia del TEDH, a fin de ofrecer la adecuada protección contra el abuso de poder:
      a) la naturaleza de las infracciones que puedan dar lugar a una orden de interceptación;
      b) la definición de las categorías de personas susceptibles de ser sometidas a vigilancia;

111 *Ibídem*, párrafo 79.
112 *Ibídem*, párrafos 80-81.
113 *Ibídem*, párrafo 89.

c) la fijación de un límite a la duración de la ejecución de la medida;
d) el procedimiento que deberá seguirse para el examen, uso y conservación de los datos obtenidos;
e) las precauciones que se han de tomar al comunicar los datos a otras partes;
f) las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de las cintas.

B) Necesidad en una sociedad democrática:

1. La defensa de la seguridad nacional es un fin legítimo para justificar la injerencia en el derecho a la vida privada, siempre que sea necesaria y proporcional a aquél fin.
   De esta manera, sólo bajo circunstancias excepcionales, como el terrorismo, este tipo de vigilancia es necesaria en interés de la seguridad nacional.
   Teniendo en cuenta lo anterior, esa necesidad exigiría un doble test:
   a) si la medida es estrictamente necesaria, en términos generales, para la salvaguarda de las instituciones democráticas y,
   b) si la medida es estrictamente necesaria, en términos particulares, para la obtención de inteligencia vital en una operación individual.
2. La valoración de la necesidad ha de realizarse por un autoridad judicial previa o posteriormente a la adopción de la medida.
3 Han de existir garantías adecuadas y suficientes de control y supervisión contra el abuso de poder por parte del Estado.

En conclusión, como señala Górriz Royo, «puede entenderse que el TEDH no proscribe con carácter general las investigaciones prospectivas, sino que analiza si la legislación que las regula es acorde al art. 8 CEDH es decir, si cumple con los requisitos de accesibilidad, previsibilidad, unas «garantías mínimas» para evitar arbitrariedades y persigue un fin legítimo» [114].

IV. ¿QUIÉN VIGILA A LOS QUE NOS VIGILAN?

La protección de la intimidad constituye una norma fundamental, de rango constitucional, propia de las sociedades democráticas, siendo su salvaguarda esencial en un Estado de Derecho.

[114] E.M. Górriz Royo, «Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas», en J.L. González Cussac y M.L. Cuerda Arnau (dirs.), *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* Tirant lo Blanch, Valencia, 2013, p. 272.

El hecho de que en la actualidad nos enfrentemos a una amenaza como el terrorismo de los últimos años, no puede hacernos caer en la tentación de generalizar la excepcionalidad.

Como sostienen Carvalho y Esteban Navarro «la presunta oposición entre seguridad y derechos se revela incorrecta. Seguridad y libertad no son conceptos incompatibles», sino «dos principios complementarios, cuya relación se caracteriza en democracia por una situación de equilibrio y de mutua garantía» [115].

Los programas de vigilancia indiscriminada, sin el necesario control judicial, nos pueden conducir al establecimiento de un «estado preventivo de pleno derecho»[116], en el que todos somos «presuntos» delincuentes, lo cual lejos de generar la tan pretendida seguridad, avocará a los ciudadanos a una sensación de inseguridad sin precedentes, al haber sido conscientes de que ahora no sólo podemos estar siendo vigilados por nuestro gobierno, sino también por otros gobiernos extranjeros. Esa pérdida de confianza en las instituciones minará los principios y valores que deben primar en una sociedad democrática y supondrá la quiebra de la presunción de inocencia.

Por otro lado, se ha puesto de manifiesto en esta investigación la cada vez más difusa línea entre la seguridad interior y exterior, entre las actividades policiales y las de inteligencia, entre intervención de comunicaciones e intervenciones estratégicas de las mismas. En esta «zona gris» de actuación en aras de la seguridad, es donde debemos preguntarnos en qué tipo de sociedad queremos vivir.

A pesar de ello, es posible regular la interceptación masiva de comunicaciones o vigilancia estratégica como algo sujeto al imperio de la ley, con las garantías y controles que se han señalado a lo largo de esta exposición, en salvaguarda del derecho a la vida privada de los ciudadanos, pues en caso contrario, ¿quién vigilaría a los que nos vigilan?

TITLE

THREATS TO SECURITY AND PRIVACY: THE DIFFICULTY OF PERFECT BALANCE

SUMMARY

I. From risk to threat: towards a new concept of safety. 1. Jihadist terrorism: a breach in security strategies? II. The use of the new technologies for criminal investigation purposes by the state. 1. Mass surveillance systems. III. European court human rights position. IV. Who is whatching the whatchers?

115 A.V. Carvalho y M.A. Esteban Navarro, «Los servicios de inteligencia…» *cit.*, p. 87.

116 Unión Europea. Parlamento Europeo. Comisión de libertades civiles, justicia y asuntos de interior, «Informe sobre el programa de vigilancia…» *cit.*, p. 24.

KEY WORDS

Threats to security; Mass surveillance; Privacy.

ABSTRACT

The aim of this paper is analyze the new concept of security that allows to face the threats of the current criminality, as well as the change that the international terrorism has assumed in the perception of that concept since 2001. It examines if this new world order legitimizes the use of mass communications surveillance systems by States, with a detailed study of the relevant European Court of Human Rights decisions about it, in order to be able to clearly appreciate the dimension of the interference of these techniques in the private lives of citizens.

Fecha de recepción: 28/03/2017 Fecha de aceptación: 04/04/2017