LA OPINIÓN PÚBLICA ANTE LA VIGILANCIA MASIVA DE DATOS. EL DIFÍCIL EQUILIBRIO ENTRE ACCESO A LA INFORMACIÓN Y SEGURIDAD NACIONAL

ROSARIO SERRA CRISTÓBAL

SUMARIO

1. LA AMENAZA DEL TERRORISMO INTERNACIONAL Y LAS MEDIDAS PARA PRESERVAR LA SEGURIDAD NACIONAL. 2. QUEREMOS SABER SI NOS ESPÍAN, PERO EL ACCESO A LA INFORMACIÓN TIENE SUS LÍMITES. EL SECRETO EN MATERIAL DE SEGURIDAD DEL ESTADO. 3. CUANDO LO SECRETO SE HACE PUBLICO. EL DEBATE SOBRE LAS MEDIDAS ADOPTADAS FRENTE AL RIESGO DEL TERRORISMO INTERNACIONAL. 4. LA IMPORTANCIA DE UNA OPINIÓN PÚBLICA INFORMADA. EL PAPEL DE LA PRENSA. 5. QUEREMOS SABER EN QUÉ MEDIDA NUESTROS DERECHOS PUEDEN QUEDAR AFECTADOS POR EL ESPIONAJE MASIVO. 5.1. La afección al derecho a la intimidad y al secreto de las comunicaciones. 5.2. La necesidad de habilitación legal y de intervención judicial. 5.3. El respeto de los principios que rigen el tratamiento de datos. 5.4. De nuevo el test de proporcionalidad. 6. REFLEXIONES FINALES. BIBLIOGRAFÍA. Fuentes provenientes de medios de comunicación.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

Fecha recepción: 24.04.2014
Fecha aceptación: 29.01.2015

LA OPINIÓN PÚBLICA ANTE LA VIGILANCIA MASIVA DE DATOS. EL DIFÍCIL EQUILIBRIO ENTRE ACCESO A LA INFORMACIÓN Y SEGURIDAD NACIONAL[1]

ROSARIO SERRA CRISTÓBAL

Profesora Titular de Derecho Constitucional
Universidad de Valencia

1. LA AMENAZA DEL TERRORISMO INTERNACIONAL Y LAS MEDIDAS PARA PRESERVAR LA SEGURIDAD NACIONAL

La preocupación por temas como el calentamiento global, los grandes riesgos medioambientales, las epidemias sanitarias, las crisis financieras o el terrorismo internacional constituye una constante para cualquier país hoy en día. La cuestión de los riesgos globales enfrenta a los Estados a un nuevo entorno estratégico cada vez más abierto e incierto que genera una sensación de inseguridad a la que se debe hacer frente. Las medidas a adoptar pueden ser de distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional.

Amparados en la obligación de proteger esa seguridad, muchos gobiernos han puesto en marcha medidas que, aún pensadas para dar cobertura a un bien a salvaguardar (la consabida seguridad), no resultan innocuas para otros intereses. Acaban erosionando e incluso dañando derechos fundamentales. Buena prueba

[1] Este trabajo se ha realizado en el marco del Proyecto de Investigación GVPROMETEOII 2014-078, financiado por la Generalitat Valenciana.

de ello lo constituyen las numerosas medidas que se adoptaron para hacer frente al terrorismo internacional tras los atentados del 11 de septiembre de 2001 (y posteriormente los de Madrid en 2004 y Londres en 2005). Éstos provocaron una auténtica conmoción que condujo a una particular voluntad de aumentar la seguridad mediante el combate del terrorismo internacional y llevó a la adopción de innumerables medidas que han producido restricciones considerables en el ejercicio de los derechos y libertades[2].

Tras los atentados del 11-S el Consejo de Seguridad de las Naciones Unidas reconoció que estos ataques constituían una amenaza contra la paz y la seguridad internacionales (Resolución número 1368, 2001) y, actuando en virtud del capítulo VII de la Carta de Naciones Unidas, adoptó la Resolución 1373 (2001), instando a todos los Estados a tomar medidas encaminadas a prevenir la comisión de actos terroristas, permitiéndoles una serie de intervenciones que, con el tiempo, han hecho difícil mantener el equilibrio entre las garantías de las libertades constitucionales y la seguridad. Muchos Estados privilegiaron esto último, con notables limitaciones para los derechos de los ciudadanos[3] (privaciones arbitrarias de libertad, torturas, asesinatos selectivos, procesos judiciales ante tribunales militares, denegación del acceso a la información, limitaciones de la libertad de expresión, vulneración de la intimidad y del derecho de autodeterminación informativa, y un largo etcétera)[4].

[2] Sobre las diferentes respuestas ofrecidas en la lucha contra el terrorismo internacional tras el 11-S puede verse, entre otros, el trabajo Roach, Kent (2014): «The 9/11 effect in comparative perspective: some thoughts on terrorism in Canada, Spain and the United States», en Miguel Revenga Sánchez (Director), *Terrorismo y Derecho bajo la estela del 11 de septiembre*, Valencia, Tirant lo Blanch, págs. 21-60.

[3] Muchos Estados en el mundo han recurrido a la regulación de regímenes de emergencia (estados de excepción) para hacer frente a supuestos de peligro para la comunidad provenientes del terrorismo. Sobre ello véase De Vergottini, Giuseppe (2004): «La difícil convivencia entre libertad y seguridad. Respuestas de las democracias al terrorismo», *Revista de Derecho Político*, n.º 61, especialmente págs. 18-20.

[4] El mundo entero conoció de los numerosos abusos a presos sospechosos de terrorismo ocurridos en Abu Ghraib, Guantánamo, Bagram y otros. Muchos de los detalles de esas torturas y confinamientos fueron conocidos después de la desclasificación de documentos secretos ordenada por la Administración Obama en abril de 2009. Esos documentos contienen información sobre terribles arrestos e interrogatorios realizados a los prisioneros por los servicios de EE. UU. durante el período comprendido entre 2002 y 2005. Acusaciones similares se vertieron contra el servicio secreto británico (M 16), por su complicidad con la CIA en las torturas contra presuntos terroristas. A finales de 2005, el director de la CIA informó a la Casa Blanca de la suspensión del programa de interrogatorios, aunque no hay confirmación de que esas prácticas hayan sido completamente abandonadas. Desde entonces se vienen utilizando nuevas técnicas, siendo menos utilizadas las de detención e interrogatorio y aumentando la práctica de los asesinatos selectivos

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

Así, por poner algún ejemplo, el Parlamento británico aprobó la *Anti-Terrorism, Crime and Security Act* en 2001, que se puso en tela de juicio por su incompatibilidad con determinados preceptos de la *Human Rights Act* de 1998[5]. Igualmente, en EE. UU. se plantearon dudas de constitucionalidad frente al exceso de medidas adoptadas en la lucha contra el terrorismo internacional (*Patriot Act I*[6], 2001, y otras)[7]. Otros países también implementaron programas antiterroristas muy agresivos[8] o permitieron el uso de sus espacios aéreos y/o aeropuertos para trasladar o entregar presuntos terroristas a EE. UU. para ser detenidos e interrogados (*extraordinary renditions*)[9]. Recuérdese ahora los documentos secretos que se hicieron públicos en 2008 y de los que presuntamente se deducía que España

de terroristas. Goldsmith, Jack (2012): «Power and Constraint: National Security Law After the 2012 Election», *Case Western Reserve Journal of International Law*, vol. 45, pág. 21.

[5] La ley fue declarada ilegal por la Cámara de los Lores en 2004 (asunto *Belmarsh)* en lo concerniente a los extranjeros. Y el Tribunal Europeo de Derechos Humanos declaró contrarias a la Convención algunas de las prácticas que de ella se derivaron, véase Asunto *A. y otros c. Reino Unido*, Stedh de 19 de febrero de 2009. Sobre este particular puede verse también el trabajo de Feldman, David (2005): «Terrorism, human rights and their Constitutional implications», *European Constitutional Law Review*, Vol 1 (3), págs. 531-552.

[6] Acrónimo de *Providing Apropriate Tools Required to Intercept and Obstruct Terrorism*.

[7] Así, El 12 de junio de 2008, el Tribunal Supremo norteamericano hizo pública la Sentencia del caso *Boumediene et al. contra Bush*. Se trata de otra más de las grandes decisiones del alto tribunal que afectan directa y principalmente a la política antiterrorista diseñada por la Administración Bush en respuesta a los ataques del 11 de septiembre. Recuérdense también otros casos como *Hamdi et al. c. Rumsfeld, Rumsfeld et al. c. Padilla*. *Vid.* Revenga Sánchez, Miguel (2008): «Tipos de discurso judicial en la guerra contra el terrorismo a propósito de la sentencia del Tribunal Supremo de Estados Unidos en el caso *Boumediene c. Bush*», *Pensar, Fortaleza*, vol 13, n. 2, págs. 175-188.

[8] En Canadá se aprobó en 2001 la *Antiterrorist Act*. En Italia se modificó la legislación penal y procesal en 2001 para introducir nuevas figuras delictivas, aunque con la exigencia de la intervención judicial. En Alemania en 2002 se introdujeron diversas medidas antiterroristas que aumentaron el poder de investigación sobre bancos, gestores de telecomunicaciones, sociedades financieras y compañías aéreas, limitando las garantías de protección de los datos personales. En Francia, en 2005 la Ley Antiterrorista significó un aumento del control de las comunicaciones privadas, de las posibilidades de actuación judicial sin mandato judicial y otras medidas preventivas por motivo de terrorismo.

Un trabajo muy interesante y completo sobre la respuesta dada por los tribunales de diversos países a las respectivas medidas adoptadas contra el terrorismo es el de Groppi, Tania (2013): «El papel de los tribunales en el control de las medidas contra el terrorismo internacional: ¿hacia un diálogo jurisprudencial?, *Revista de Derecho Político*, n.º 86, págs. 309-356.

[9] Sobre la cooperación de numerosos Estados con las denominadas *extraordinary renditions* puede verse el informe de la Open Society Justice Initiative (2013): *Globalizing torture CIA Secret Detention and Extraordinary rendition*, New York, Open Society Foundation.

> cedió el uso de alguno de sus aeropuertos para que los aviones estadounidenses que trasportaban prisioneros hacia la cárcel de Guantánamo pudiesen hacer escala en ellos[10].

Dejando a un lado la gravedad de algunas de las actuaciones que se han desarrollado en el ámbito de la lucha antiterrorista, otra de las cuestiones que más repercusión ha tenido recientemente es la que deriva de la información que salió a la luz en 2013 a raíz de las filtraciones del ex empleado de la *Agencia de Seguridad Nacional* estadounidense (NSA), Edward Snowden. Se hizo público algo que, en el marco de las acciones de inteligencia, había quedado cubierto por el secreto de Estado hasta ese momento. La ruptura de dicho secreto reveló que el gobierno de EE. UU. había estado espiando masivamente los datos de millones de ciudadanos, no sólo estadounidenses, sino también extranjeros, incluidos altos mandatarios de muchos Estados europeos y americanos, creando un general malestar. Inmediatamente después de los atentados del 11-S, la NSA fue autorizada por el Presidente George W. Bush (más tarde también por el Presidente Obama) y por el Congreso para implementar un programa de vigilancia de toda comunicación realizada por cualquier ciudadano a un sospechoso de terrorismo en cualquier parte del mundo[11] (una monitorización de comunicaciones que se ha estado realizando de un modo generalizado y a escala global). Cuando el escándalo saltó a la luz pública, los hechos fueron reconocidos por la NSA ante el Senado, alegando que la información obtenida no fue utilizada para ningún otro fin que no fuera garantizar la seguridad nacional. En respuesta al malestar internacional que ello generó, el Presidente Obama tuvo que hacer frente a las críticas internacionales a principios de 2014. La respuesta presidencial se mantuvo en la línea de defender la constitucionalidad de la medida y declaró que las intervenciones telefónicas sin orden judicial eran una «herramienta esencial» en la lucha contra el terrorismo y necesarias para el mantenimiento de la seguridad del Estado. No obstante, dijo que limitaría la capacidad de las agencias de inteligencia para tener acceso a los registros telefónicos, que sería necesaria la autorización judicial previa antes de que un agente de la NSA quisiese acceder a registros de llamadas, excepto en supuesto de emergencia, y añadió que había

[10] Por todos, González, Miguel: «Aznar dio vía libre al paso por España de presos hacia Guantánamo y lo ocultó», *El País*, 1 de diciembre de 2008; Agencias: «El PP reclama al Gobierno que explique todo lo que sabe de los vuelos de la CIA», *El Mundo*, 1 de diciembre de 2008. S. A: «De los 11 vuelos a Guantánamo con escala en España, 9 han sido bajo el mandato de Zapatero», *El confidencial*, 1 diciembre 2012.

[11] Así lo recordaba Fiss, Owen M. (2013): «El mundo en el que vivimos», *El Cronista del Estado social*, n.º 37, págs. 20-31.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

prohibido espiar a los líderes de los países aliados[12]. En marzo de 2014 la Administración Obama anunció que estaba preparando un proyecto legislativo desde esa perspectiva[13].

Con independencia de las limitaciones al espionaje que ahora vengan a imponerse o las garantías que hipotéticamente se anuncien, la inquietud está sembrada. Y no solo porque quien nos espíe sea un país extranjero, sino también si lo hace nuestro propio país. De hecho, pronto la prensa se apresuró a revelar que la práctica de recolección masiva de datos es habitual desde hace años por parte de los servicios de inteligencia de numerosos países, y en esto no podemos excluir al nuestro[14]. Como expresaba gráficamente Cuerda Arnau, «la idea de un Gran Hermano que nos vigila ya no es una quimera»[15].

Es cierto que desde tiempos inmemoriales los Estados han procurado recabar información, dentro del propio ámbito territorial y fuera de él, para analizarla y utilizarla de la forma más conveniente para la defensa o protección de los intereses nacionales de cualquier naturaleza. Y esto se ha realizado bajo el manto del principio del secreto, exento a todo conocimiento público y con escaso o nulo control judicial. Ya en uno de los escritos más antiguos que existen sobre estrategia en momentos de confrontación —*El arte de la guerra*, de Sun Tzu[16], que data del siglo V a. C.—, se aleccionaba sobre lo esencial que es el espionaje para conocer la situación del enemigo y sacar ventaja de ello en el enfrentamiento. Pero, recordando al mismo tiempo que «no hay asunto más secreto que el espionaje» (Cap. 13). En los Estados democráticos contemporáneos los denominados

---

[12] Presidential Policy Directive/PPD-28, «Signals Intelligence Activities», January 17, 2014.

[13] Savage, Charlie (2014). «Obama to Call for End to N. S. A.'s Bulk Data Collection», *The New York Times*, 24 de marzo de 2014.

[14] Por todos, Follorou, J. y Johannès, F.: «Révélations sur le Big Brother français», *Le Monde*, 4 de julio de 2013. Ackerman Spencer y Ball, James (2014): «Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ», *The Guardian*, 28 febrero de 2014. Europa Press, «El CNI colaboró con Reino Unido en operaciones encubiertas de vigilancia masiva en internet», *Público.es*, 17 de febrero de 2014. Galdón Clavell, Gemma: «Espionaje y derechos humanos: los límites a la intromisión de la intimidad», *eldiario.es*, 4 de agosto de 2013. Versión electrónica: http://www.eldiario.es/turing/Espionaje-derechos-humanos_0_159934512.html Del Pino, Daniel: «Londres también espía las comunicaciones españolas», *publico.es*, 4 de septiembre de 2013.

[15] Cuerda Arnau, M. Luisa (2013): «Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes», en González Cussac, José Luis y Cuerda, Arnau, M. Luisa (Dir.), *Nuevas amenazas a la seguridad nacional*, Valencia, Tirant lo Blanch, pág. 109. En este trabajo, el lector puede descubrir un amplio abanico de sistemas de vigilancia e interceptación de comunicaciones a los cuales podemos vernos sometidos los ciudadanos.

[16] TZU, Sun (2008), El arte de la Guerra (versión de Thomas Cleary), Madrid, EDAF S.L., 35.ª edición, págs. 121 y ss.

«servicios de inteligencia» han trabajado siempre en la obtención de información para analizarla, transformarla en conocimiento y ponerla a disposición de aquéllos que han de adoptar decisiones políticas, económicas, militares, etc. y para actuar frente a posibles futuras amenazas. Porque, como indicaba De Vergottini, la lucha contra las mismas «debe consistir no solamente en el *afrontamiento* de los eventos en el momento en que se producen, sino, sobre todo, en su *prevención*»[17]. De hecho, los servicios de inteligencia tienen como misión principal proporcionar a los Gobiernos la información necesaria para *prevenir y evitar* cualquier riesgo que amenace la seguridad, integridad o intereses del Estado[18]. Así, ante la omnipresente amenaza del terrorismo internacional, la recolección de información que permita conocer a los terroristas y, por tanto, actuar proactivamente, adelantándose a sus acciones, es considerada con frecuencia como el instrumento por excelencia de la lucha antiterrorista[19]. Aunque en esa lucha antiterrorista, junto a ello, han de concurrir igualmente actuaciones de otros servicios del Estado (fuerzas de seguridad).

La discusión se produce acerca de qué medios se pueden emplear para recabar información, concretamente la procedente de fuentes cerradas. Mucha de esa información se obtiene de internet y del tratamiento de los datos que circulan por sus páginas (fuentes abiertas) y también del control y acceso a fuentes no abiertas. Porque es en ese ámbito electrónico donde las organizaciones terroristas internacionales recaudan fondos para realizar atentados, recaban adeptos, hacen apología de su causa, o coordinan sus grupos y/o ataques terroristas[20].

En este campo, la tecnología cada día ofrece más y mejores instrumentos a los unos para delinquir y a los Estados para intentar evitar dichas actuaciones. El avance de las nuevas herramientas técnicas, la existencia de grandes proveedores de servicios de internet —que a su vez almacenan millones de datos de

[17] De Vergottini, Giuseppe (2004): «La difícil convivencia…», *op cit*, pág. 15.

[18] En este sentido, en el preámbulo de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, establece que «La principal misión del Centro Nacional de Inteligencia será la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones».

[19] Sansó-Rubert, Daniel (2004): «Seguridad vs. libertad: el papel de los servicios de inteligencia», *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, n.º 48, pág. 89. Indicaba este autor que el valor más importante de la Inteligencia en el contraterrorismo estriba en proporcionar un aviso táctico preventivo de una acción terrorista.

[20] Sobre ello puede verse el trabajo de Brown, Ian y Korff, Douwe (2009): «Terrorism and the proportionality of Internet Surveillance», *European Journal of Criminology*, vol. 6 (2), págs. 119-134.

clientes[21]—, y la realidad de programas informáticos muy elaborados y potentes que son capaces, no simplemente de recabar datos, sino de tratarlos y extraer una información de calidad, nos hace situarnos en un nuevo escenario. A la vez que es posible tecnológicamente interceptar comunicaciones telefónicas y electrónicas que se efectúen en cualquier parte del mundo. Ese control y esa recopilación de información aparentan ser cada vez menos selectivos en cuanto sus destinatarios. Se trata de una monitorización que puede ser muy incisiva (se recaban infinitos datos personales o de comunicaciones y se tiene la capacidad técnica de evaluarlos e interpretarlos con perspectiva) y se realiza de un modo globalizado.

Este trabajo se centra especialmente en ese tipo de vigilancia que llevan a cabo los servicios de inteligencia y que tiene como fin recabar información para prevenir los riesgos que pueden atentar a la seguridad del Estado. En concreto, constituirá nuestro objeto de análisis principalmente la que conduce a la prevención del terrorismo internacional, por constituir el detonante de la vigilancia masiva de datos que ha saltado a la luz pública. La modalidad de control de la que nos ocuparemos es de carácter estratégico, exploratorio, táctico, preventivo, general, prospectivo, —como prefiera denominarse[22]—, y se diferencia de la vigilancia que llevan a cabo las fuerzas de seguridad para investigar o perseguir el delito, que generalmente suele tener un tinte post-delictual, va destinada a incorporarse a un proceso penal y neutralizar la presunción de inocencia, supone la interceptación de individuos concretos y tradicionalmente no ha respondido al patrón de un programa de vigilancia general e indiscriminado (aunque también en esto las cosas parecen estar cambiando).

Es en este contexto donde los ciudadanos han empezado a ser conscientes por la prensa de la posibilidad de que sus datos estén siendo vigilados indiscriminadamente. Y, ante una información que es parcial y la falta de instrumentos necesarios para analizar y valorar cuestiones tan complejas como las estrategias de seguridad y defensa, esa ciudadanía no pueden más que inquietarse. Las preguntas que se hace el público[23] son muchas: ¿hasta qué punto estoy siendo con-

[21] Las filtraciones del ex empleado de la NSA Edward Snowden reveladas al rotativo británico *The Guardian*, pusieron de manifiesto la existencia de un programa secreto que permite a la NSA ingresar directamente en los servidores de Google, Facebook, Skype, Microsoft y Apple. Al igual que al servicio de transferencia de datos bancarios Swift.

[22] En el ámbito anglosajón, *strategic monitoring,* o *general programmes of surveillance.*

[23] Como indicaba Torres del Moral, las personas que atienden y se interesan por los acontecimientos y facetas integran el público. Para que alguien pueda ser considerado público de algo basta con que atienda a ese algo y se interese por lo que sucede en ese terreno; eso es suficiente para que emita opiniones sobre el particular, por elementales que fueren; pero seguramente esa atención e interés por informarse le llevará a conocer lo suficiente del asunto como para terminar formulando opiniones expertas. Torres del Moral, Antonio (2009): «El instituto jurídico de la opinión

trolado? ¿puede hacer esto el Estado?, si lo hacen para prevenir futuros riesgos, ¿están justificadas en todas las ocasiones las medidas que los Gobiernos adoptan?, ¿son ciertos esos riesgos o están sobrevalorados?, ¿cuándo están legitimados los Gobiernos para adoptar determinadas medidas que suponen cercenar mis libertades?, ¿tengo derecho a saberlo? Este trabajo pondrá de relieve las deficiencias del ordenamiento para la resolución de estos interrogantes y tratará de aportar criterios que ayuden a dar respuesta a los mismos.

2. QUEREMOS SABER SI NOS ESPÍAN, PERO EL ACCESO A LA INFORMACIÓN TIENE SUS LÍMITES. EL SECRETO EN MATERIA DE SEGURIDAD DEL ESTADO

Ante los hechos narrados más arriba, la ciudadanía quiere saber. Quiere conocer si está siendo espiada. Los ciudadanos necesitan poder emplazar a los gobiernos a informar sobre si efectivamente hicieron acopio masivo de sus datos, por qué lo hicieron y qué tratamiento se dio a los mismos. La democracia exige participación, y para participar hay que estar informado[24]. La democracia requiere una transparencia en la actuación de las instituciones públicas que permita el acceso de los ciudadanos a la información y garantice la ausencia de arbitrariedad en el ejercicio del poder público[25]. Queremos información para cubrir necesidades de naturaleza muy distinta, desde la defensa de nuestros propios intereses y la adopción de medidas de precaución ante los posibles peligros, —que conocemos que existen porque fluye la información—, hasta el poder ejercer un control-crítica sobre la respuesta de las instituciones públicas al delito o a las amenazas que se ciernen sobre el Estado, sus instituciones y sus ciudadanos.

pública libre», en Torres del Moral (Dir.), *Libertades informativas*, Madrid, Ed. Constitución y Leyes Colex, págs. 139.

[24] En este sentido véase también, Rallo Lombarte (2002): «Medios de comunicación y democracia. Apuntes para una reforma», en *Estudios de Derecho Constitucional homenaje a Joaquín García Morillo* (Coord. Luis López Guerra), Valencia, Tirant lo Blanch, págs. 223-250.

[25] El Tribunal Constitucional español desde sus primeras decisiones ha reconocido en la formación de una opinión pública libre uno de los requisitos esenciales de una democracia (entre esa primera jurisprudencia recuérdense las sentencias: SSTC 6/1981, de 6 de marzo; 12/1982, de 31 de marzo; 56/1983, de 28 de junio…). En el mismo sentido, Troncoso defiende que La transparencia es un requisito necesario para el ejercicio del derecho fundamental a la participación en asuntos públicos y facilita el control social de la actividad de los poderes públicos, Troncoso Reigada, Antonio (2008): «Acceso a la información administrativa y protección de datos personales», en Troncoso (Dir.): *Transparencia administrativa y protección de datos*, Madrid, Thomson-Civitas, especialmente págs. 35 a 39.

Pero, el derecho a ser informado sobre asuntos generales, como contenido del art. 20.1.d) CE, no ha sido concebido como un derecho de carácter prestacional. Se dirige fundamentalmente a evitar la injerencia en el libre flujo de la información[26]. Y no es un derecho ilimitado, ni incluye un derecho ilimitado de búsqueda y obtención de la información, solo cubre el derecho a recibir información sobre aquello que es de «interés público», y aún así, no siempre. Porque, la Constitución no impone la publicidad absoluta de toda actuación de los poderes públicos, —incluso en aspectos tan principales como el derecho a un proceso judicial público podemos encontrar excepciones a dicha publicidad—. Y si esta cuestión la referimos al tema que nos ocupa (la seguridad y defensa del Estado) encontraremos la primera gran excepción: la exclusión de las materias referidas a la inteligencia (las materias declaradas reservadas o secretas) del derecho de acceso de los ciudadanos a los archivos y registros públicos y, por lo tanto, del debate público (art. 105.b CE)[27].

Si algo ha caracterizado a la labor de inteligencia es el carácter secreto de la misma. Como indicaban Esteban y Carvalho, «en general, impera la convicción de que el secreto es un elemento indisociable de la naturaleza de la inteligencia, tan esencial como la trasformación de la información en conocimiento útil y aplicado o la investigación de las amenazas»[28]. El secreto es una forma de asegurar que determinadas fuentes, misiones, hechos, identidades, etc. no sean conocidos por quienes podrían valerse de esa información para actuar contra los intereses del país. La publicidad del objeto y de los métodos de investigación de los servicios secretos podría convertir en papel mojado su trabajo y ofrecer a terceros una información útil para atentar contra la seguridad nacional. Por lo tanto, si realmente está en juego ésta, la existencia de esos programas de vigilancia y recopilación de datos, los detalles acerca de los mismos y las actividades que llevan a cabo los servicios de inteligencia podrían y deben quedar sustraídos del público conocimiento.

---

[26] Entre otras, SSTC 105/1990, de 6 de junio; 172/1990, de 5 de noviembre; 240/1992, de 21 de diciembre.

[27] Igualmente, el art. 5 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, indica que toda la documentación y actividades que se realizan en el marco de sus funciones constituyen información clasificada, con el grado de secreto.

[28] Esteban Navarro, M. A. y Carvalho, A. V. (2012): «Inteligencia: concepto y práctica», en González Cussac, J. L. (Coord.): *Inteligencia*, Valencia, Tirant lo Blanch, pág. 43.

La Ley de Secretos Oficiales (Ley 9/1968)[29] establece que pueden ser declaradas «materias clasificadas»[30]: «los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por persona no autorizada pueda dañar o poner en riesgo la seguridad y defensa del Estado». Y añade que dichas materias no podrán ser comunicadas, difundidas, ni publicadas, ni utilizado su contenido fuera de los límites establecidos por la ley (arts. 2 y 13). Sí podrán, sin embargo, tener conocimiento de las materias «clasificadas» el Congreso de los Diputados y el Senado, en la forma que determinen los respectivos Reglamentos y, en su caso, en sesiones secretas, así como los órganos y las personas debidamente facultadas para ello, con las formalidades y limitaciones que en cada caso se determinen (arts. 8.a y 10.2)[31].

Ya puede intuir el lector que la previsión legal arriba citada sobre la potestad de clasificar una materia o una información como secreta es tan poco precisa que brindan al Gobierno amplísimas facultades de decisión sobre la exclusión de las mismas del general conocimiento.

Esta realidad es común en muchos países de nuestro entorno. El recurso al secreto de Estado para impedir el acceso del público a determinadas informaciones es algo generalizado. Especialmente desde los atentados del 11 de septiembre de 2001, el secreto y la seguridad nacional se han convertido en un argumento recurrente para impedir el acceso a la información sobre las pesquisas seguidas en la lucha antiterrorista. Estas limitaciones se han producido en general en todo Occidente, pero posiblemente su intensidad ha sido mayor en EE. UU., que venía haciendo de la seguridad nacional un pretexto desde el fin de la Segunda

[29] La normativa vigente en materia de secretos oficiales es el resultado de la ligera modificación de una ley preconstitucional (Ley 9/1968, de 5 de abril, desarrollada por Decreto 242/1969, de 20 de febrero, modificada por Ley 48/1978, de 7 de octubre). Esta normativa ha sido objeto de numerosas críticas por su absoluta generalidad e imprecisión: no se regula la duración del secreto, la determinación del objeto es ambigua y no se determina exactamente a quién se le permite conocer de esa materia ni a través de que procedimiento. Álvarez Conde, Enrique (1997): «El temor del Príncipe o el temor al Príncipe. Secretos de Estado y Constitución», *Anuario Jurídico de La Rioja*, n.º 3, págs. 349-364.

Un valioso comentario a la Ley de Secretos Oficiales puede verse en Cousido González, Pilar (1995): *Comentario a la Ley de Secretos Oficiales y su reglamento*, Barcelona, Bosch.

[30] Ese «secreto» puede tener grados distintos y estar justificado su mantenimiento con carácter temporal (y decidirse su desclasificación) o con carácter indefinido. Grados de clasificación: secreto (S), reservado (R), confidencial (C), de difusión limitada (DL).

[31] Sobre el carácter secreto de las actividades del Centro Nacional de Inteligencia véase art. 5 de la Ley 11/2002, que regula el Centro Nacional de Inteligencia. Y sobre el control de éste, la Ley 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

Guerra Mundial para ocultar aquellas actuaciones gubernamentales que querían sustraer del conocimiento público[32].

> Como han traído a colación González Cussac y otros[33], en algunas ocasiones el Tribunal Supremo norteamericano ha reconocido la capacidad del Gobierno de utilizar el privilegio del secreto de Estado para negarse a descubrir cierta información que podría afectar de manera adversa a la seguridad nacional en caso de divulgación de la misma. Dos casos controvertidos fueron el de *Center for National Security Studies v. US Department of Justice* (2004), en el que la Corte Suprema apoyó la decisión gubernamental de no revelar los nombres, lugares, horas de detención, o abogados de detenidos en las horas y días posteriores al 11S, y el caso *North Jersey Media Group and Detroit Free Press v. Ashcroft* (2003) donde también avaló la negación del gobierno a revelar a los medios información sobre las medidas adoptadas inmediatamente tras los atentados.
>
> Igualmente cabe citar la decisión del Tribunal Constitucional alemán en un supuesto de petición de acceso a información secreta por parte ciertos grupos parlamentarios. Éstos habían solicitado información sobre la supuesta colaboración producida entre los servicios de inteligencia alemanes y la CIA en materia de lucha contra el terrorismo tras el 11-S, pero el Gobierno se negó a conceder el acceso a parte de los documentos. El Tribunal Constitucional entendió que cierta información nuclear constituía competencia exclusiva del Gobierno y podía quedar exenta del conocimiento del Parlamento o de terceros[34].
>
> En Italia la Corte Constitucional también ha avalado el privilegio del secreto de los servicios de inteligencia en casos similares[35].
>
> Mayor controversia se produjo en Reino Unido en relación a las pruebas declaradas secretas que habían conducido a la detención de presuntos terroristas. Se estableció la prohibición de sus abogados de difundirlas e incluso de contactar con los propios detenidos tras acceder a los documentos secretos para evitar que pudieran transmitirles dicha información reservada[36].

---

[32] Revenga Sánchez, Miguel (1995): *El imperio de la política. Seguridad nacional y secreto de Estado en el sistema constitucional norteamericano*, Barcelona, Ariel, pág. 30.

[33] González Cussac, José Luis; Larriba Hinojar, Beatriz y Fernández Hernández, Antonio (2012): «Servicios de inteligencia y Estado de Derecho», en González Cussac (Coord.): *Inteligencia*, Valencia, Tirant lo Blanch, pág. 296.

[34] BVerfg, 2 BvE 3/07, 17 de junio de 2009, Vashakmadze, Mindia (2013). «Secrecy vs. Openness: counter-terrorism and the role of the German Federal Constitutional Court», en David Cole, Federico Fabbrini y Arianna Vedaschi (eds.), *Secrecy, national security and the vindication of Constitutional Law*, Cheltenham, Edwuard Elgar Publishing Limited, págs. 46-47.

[35] Vedaschi, Arianna (2013): «Arcana imperii and salus rei publicae: state secrets privilege and the Italian legal framework», en *Secrecy, national security*…, *op. cit.,* págs. 95-111.

[36] Roach, Kent (2013). «Managing secrecy and its migration in a post 9/11 world», en *Secrecy, national security*…, *op. cit.,* págs. 119-120.

Aunque la prohibición de acceso a una determinada información puedan estar justificada en muchos casos, lo cierto es que se corre el peligro de convertir esta prerrogativa en una especie de carta blanca a favor de los gobiernos. En general, las previsiones legales les otorgan gran capacidad de decisión sobre la declaración de una información como secreta. Y donde hay secreto falta el control, y sin controles no hay garantías para la efectividad de los límites que también tiene un gobierno para hacer uso del secreto.

Por ello, pese a que sean amparables en nuestro ordenamiento el secreto y la discrecionalidad que acompañan a la actividad de inteligencia y política de defensa, nuevas voces han empezado a oírse apelando al principio de transparencia, interdicción de la arbitrariedad, prohibición de abuso de poder y respeto a los derechos individuales[37]. Como recordaban Cole, Fabbrini y Vedaschi, el secreto se hace necesario para la gobernanza, especialmente en materia de seguridad nacional, pero, al mismo tiempo, la democracia representativa y el Estado de derecho exigen transparencia y responsabilidad, y el secreto ataca el núcleo de ambos valores[38].

En esa línea, el art. 14 de la Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno, indica que el derecho de acceso a la información podrá ser limitado cuando acceder a la información suponga un perjuicio, entre otras cosas, para la seguridad nacional o la defensa[39]. Aunque también añade que «la aplicación de los límites *será justificada y proporcionada* en su objeto y finalidad de protección y *atenderá a las circunstancias del caso concreto*…» (la cursiva es de la autora).

---

[37] Kempen, Piet Hein van (2013): «Four concepts of Security-A Human Rights Perspective», *Human Rights Law Review*, n.º 1, págs. 15-16; Guerrero Gutiérrez, Eduardo (2010): «Transparencia y seguridad nacional», *Cuadernos de Transparencia*, n.º 18, Instituto Federal de Acceso a la Información y Protección de datos, págs. 9-54. Sánchez Ferro, Susana (2009): «Libertades informativas y poder ejecutivo: secretos oficiales», en Torres del Moral (Dir.), *Libertades informativas*, Madrid, Ed. Constitución y Leyes Colex, págs. 1033. En el mismo sentido, Flores Giménez, Fernando (2013): «Somos transparentes, son opacos», *Al Revés y al Derecho*, 2 de septiembre de 2013, versión digital: http://alrevesyalderecho.infolibre.es/?p=1582

[38] Cole, David Cole; Fabbrini, Federico y Vedaschi, Arianna (eds.) (2013): «Introduction», en *Secrecy, national security and the vindication of Constitutional Law*, Cheltenham, Edwuard Elgar Publishing Limited, pág. 1.

[39] En este mismo sentido, el art. 3 de la Convención del Consejo de Europa sobre Acceso a los documentos públicos, de 18 de abril de 2009, dispone que: «Cada parte puede limitar el derecho de acceso a los documentos públicos. Los límites deberán estar previstos por una ley, ser necesarios en una sociedad democrática y tener como objetivo la protección de: a) la seguridad nacional, la defensa y las relaciones internacionales; b) la seguridad pública; c) la prevención la investigación y el procesamiento de actividades criminales…»

El Tribunal Supremo español ya abordó la cuestión de la justificación del secreto de Estado en el caso conocido como «los papeles del CESID»[40]. El Alto Tribunal consideró la constitucionalidad de la declaración de secreto de un conjunto de información, estudios, medidas, o acciones dirigidas a que el Estado hiciera frente a una actividad terrorista. La información en cuestión estaba relacionada con la seguridad y la defensa del Estado, y ello justificaba su secreto. Pero en el proceso se planteó también qué sucedía ante una colisión con otros intereses como el derecho a acceder a dicha información secreta para utilizarla como prueba en un proceso judicial. El Tribunal ponderó los beneficios del mantenimiento del secreto para la seguridad del Estado, con los derivados de la desclasificación de los mismos para la garantía de la defensa en el proceso y entendió que éstos últimos debían prevalecer, por lo que ordenó la desclasificación de aquella parte de los documentos que habían sido requeridos por el juez del proceso penal abierto. Aunque la decisión del tribunal no satisfizo a todos[41], se puso de manifiesto la necesidad de establecer pautas que regulen debidamente las colisiones que pueden producirse entre la necesidad de mantener una materia como reservada para salvaguardar la seguridad nacional y el respeto a los derechos fundamentales. Y se afirmó que la constitucionalidad de la posible existencia de secretos de Estado no implica automáticamente que el régimen jurídico concreto de regulación de los mismos y el uso concreto del secreto de Estado deba quedar exento de control. En síntesis, por primera vez se dispuso

[40] SSTS de 4 de abril de 1997 (Rec. 726/1996; Rec. 602/1996 y Rec. 634/1996) En dichas sentencias se recogen los criterios jurídicos que el Consejo de Ministros tuvo en cuenta, atendiendo a un informe jurídico previo de la Asesoría Jurídica General del Ministerio de Defensa y dictamen del Consejo de Estado, para denegar la desclasificación, y que son, sintéticamente, y en lo que ahora interesa, los siguientes:

a) Los documentos en cuestión afectan a la seguridad del Estado, que es la de todos los españoles.

b) La desclasificación implicaría un inadmisible deterioro del crédito de España en sus relaciones exteriores y, en particular, del intercambio de inteligencia o información clasificada con nuestros aliados y amigos.

c) La desclasificación pondría en peligro la eficacia, las fuentes de información, los medios y los procedimientos operativos del CESID, así como la integridad física y hasta la vida de quienes son o fueron agentes operativos del mismo, o de sus familiares o allegados.

Y d) La desclasificación se pide en el contexto de una investigación sumarial, por lo que, en caso de accederse a ella, no podría evitarse la divulgación fuera de la investigación criminal, al incorporarse los documentos a un proceso penal en el que rigen los principios de contradicción y publicidad.

[41] Se ha defendido que debiera ser el legislador y no los tribunales quienes establecieran esas pautas. SÁNCHEZ FERRO, Susana (2006): *El secreto de Estado*, Madrid, Centro de Estudios Políticos y Constitucionales, pág. 462.

que frente a derechos fundamentales sagrados en nuestra Constitución, no puede prevalecer ninguna «razón de Estado» y que las materias clasificas no pueden considerarse como una zona de inmunidad jurisdiccional.

Si traemos ese mismo razonamiento al tema que ahora nos ocupa, esto es, la resolución del conflicto entre la necesidad de que el Estado cumpla con sus funciones de salvaguardar la seguridad y lleve a cabo sus actuaciones con carácter secreto, por un lado, y, el derecho de los ciudadanos a ser informados de ello, por otro, también hemos de acudir al juicio constitucional de la ponderación.

En ese juicio, debemos partir de la idea de que el secreto es una excepción constitucional. Como recordaba De Lucas, «lo que constituye el secreto es la derogación del principio general de conocimiento»[42]. Por lo tanto, el recurso al mismo ha de producirse solo si es necesario e inevitable. En el mismo sentido defiende Revenga que «el secreto de Estado sólo es tolerable cuando se presenta en términos rigurosamente excepcionales y vinculados a la defensa de un manifiesto interés público»[43]. Por lo tanto, solo debería caber el secreto cuando una materia así lo requiera, o cuando el conocimiento de determinadas actuaciones haga que las actuaciones de la administración pierdan eficacia[44], o cuando algún otro supuesto legal habilitante así lo permita porque haya intereses constitucionalmente amparables que salvaguardar. Eso implica, a su vez, que no se pueden permitir interpretaciones o aplicaciones extensivas en su uso. Y, como apuntaba Sánchez Ferro, refiriéndose al secreto administrativo, «el poder político está obligado a justificar el uso dado al secreto de Estado en tanto que excepción al principio de publicidad y al derecho de acceso a los archivos y registros administrativos reconocidos en nuestro ordenamiento jurídico»[45].

La principal dificultad se encuentra en definir qué puede afectar a la seguridad y defensa del Estado y, en consecuencia, en ponderar cuándo el conocimiento público de determinadas actuaciones pueden poner en riesgo dicha seguridad.

Cuando hablamos de riesgo para la seguridad se está haciendo alusión no solo a la existencia de amenazas efectivas a valores nucleares de la sociedad o del

---

[42] De Lucas, Javier (1990): «Democracia y transparencia. Sobre poder, secreto y publicidad», *Anuario de Filosofía del Derecho*, vol. VII, pág. 24.

[43] Revenga Sánchez, Miguel (1998): «Razonamiento judicial, seguridad nacional y secreto de Estado», *Revista Española de Derecho Constitucional*, n.º 53, pág. 60.

[44] Indicaba Sánchez que en muchas ocasiones no es la materia el factor determinante para establecer el secreto, sino la protección del principio de eficacia de la actuación de la administración que viene reconocido en el art. 103 de la Constitución, Sánchez Ferro, Susana (2006): *El secreto de Estado*, Madrid, Centro de Estudios Políticos y Constitucionales, pág. 13.

[45] *Ibidem,* pág. 156.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

Estado, sino también al miedo a que tales valores se vean atacados (seguridad en sentido subjetivo). Además, estos valores pueden variar de unos Estados a otros, lo que explica que el concepto de seguridad no sea absolutamente homogéneo en todos los países. Porque, a los riesgos externos reales a los que se ve sometido un país hay que sumar otros factores internos (carácter nacional, tradición, preferencias, prejuicios, etc.) que influyen luego decisivamente en el nivel de seguridad que un gobierno decide establecer como objetivo de su política de seguridad y defensa[46]. A ello hemos de añadir que, más allá de los intereses nacionales, la visión de la seguridad y la defensa de un Estado no puede ya alejarse o eximirse de participar también en las necesidades de la seguridad y defensa europeas y de aquellas otras relaciones que se mantienen en el marco de las organizaciones y alianzas internacionales. Se habla entonces de una seguridad compartida o de seguridad colectiva. Así, cuando hablamos del terrorismo internacional, nos encontramos ante una amenaza cuyo origen es difícil de identificar y carece de un centro de gravedad único, por lo que la lucha contra el mismo ha de encauzarse en una estrategia de inteligencia y defensa global. Una estrategia que tiende a contemplar medidas que se anticipen a los peligros, esto es, que tratan de evitar que los posibles ataques terroristas se produzcan (Ésta es la filosofía de la Estrategia española de Seguridad Nacional[47]).

Con estos mimbres es fácil para un gobierno encontrar elementos que justifiquen que determinadas actuaciones o cierta información puede poner en riesgo la seguridad nacional o que puede conducir a la revelación de información cedida por otros Estados o que se ha obtenido en cooperación con servicios de inteligencia extranjeros. Y, por lo tanto, puede hacer caer el peso de la balanza a favor de la seguridad y en perjuicio de una sociedad (una opinión pública) lo más informada posible. El hecho es que quien decide es el propio Gobierno y la discrecionalidad que le otorga la ley puede autorizarle a retener aquella información cuyo conocimiento pueda entender (desde su propio punto de mira) que pone en peligro la seguridad del Estado, permitiéndole actuar sin control alguno por parte de la ciudadanía y con escaso control judicial.

La pobre concreción legal de los intereses que pueden ser protegidos por el secreto de Estado, la amplitud del término seguridad —que además, se desarrolla en un contexto internacional donde ha sido perfilado en términos muy amplios— y la imprecisión que deriva de la presunción de que existe un riesgo

[46] *Ibidem,* pág. 219.

[47] Véase la Estrategia de Seguridad Nacional aprobada por el Gobierno español en 2013, que supuso una revisión y actualización de la del año 2011.

(que implica que el daño aún no se ha producido), dificultan enormemente esta tarea judicial de control.

Sobre todo, ese control por los tribunales es escaso porque la práctica totalidad de actuaciones de los servicios de inteligencia son secretos y, como consecuencia, los ciudadanos no somos conocedores de la existencia de las mismas y quien corresponda no puede denunciarlas. Muchas veces ni siquiera podemos saber *a priori* qué es lo que nos interesa saber como ciudadanos y, por lo tanto, tampoco podemos demandar en términos absolutos un conocimiento genérico de algo que desconocemos. De lo que no se sabe, no se puede opinar, por lo tanto, esa información quedará fuera del debate público. Como mucho, queda el acceso de la Comisión parlamentaria del órgano que nos representa, que puede llevar a cabo una deficitaria labor de control, y que, en todo caso, se realiza en sesiones que se rigen también por el principio del secreto[48].

Por otro lado, lo que no se sabe, difícilmente es denunciable ante los tribunales, pudiendo escapar de la revisión judicial más allá del control previo al que es sometido el CNI cuando sus actuaciones afecten al secreto de las comunicaciones o a la inviolabilidad domiciliaria[49]. Pero en esos casos, la preceptiva autorización del Magistrado del TS designado al efecto solo se prevé para interceptaciones temporalmente breves de las comunicaciones (siendo prorrogables) y con identificación de la persona o personas afectadas por las medidas. Pero no parece estar pensada esta intervención judicial para interceptaciones de comunicaciones con carácter masivo o prospectivo.

En este escenario de desinformación y falta de control que la seguridad del Estado a veces impone, lo que se guarda es la confianza de que se perciba una cierta «transparencia», en el sentido de que se genere la convicción de que la clasificación de determinadas materias como secretas se adopta respetando el marco del Estado de Derecho. Para ello, cuantos más parámetros o directrices incluya la ley en la potestad gubernamental de clasificación de la información, —tarea aún pendiente—, más garantías tendremos los ciudadanos de que la decisión del Gobierno de impedir el acceso del público a la misma responde a un interés público mayor y no se usa en provecho propio. Y más fácil será ejercer un control jurisdiccional sobre tales decisiones.

---

[48] Art. 11 Ley 11/2002, reguladora del Centro Nacional de Inteligencia.

[49] Ley Orgánica 2/2002, reguladora del control judicial previo del Centro Nacional de Inteligencia.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

3. CUANDO LO SECRETO SE HACE PÚBLICO. EL DEBATE SOBRE LAS MEDIDAS ADOPTADAS FRENTE AL RIESGO DEL TERRORISMO INTERNACIONAL

Pero, cuando la información que recaban los servicios de inteligencia no necesita seguir manteniéndose como reservada, porque su conocimiento ya no puede poner en peligro la seguridad nacional, o, simplemente, cuando ese secreto es desvelado por quien no debía hacerlo[50], lo que antes estaba fuera del alcance del público pasa a ser de general conocimiento. Es cuando la sociedad recobra los elementos necesarios para seguir ejerciendo su derecho a participar: su derecho a exigir explicaciones, a entender el porqué de una actuación, de los medios utilizados y sus consecuencias, a fiscalizar si la acción estatal constituía la única alternativa, si fue proporcionada y si se respetaron las reglas del Derecho.

En este sentido, recordemos las palabras que se recogen en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno:

> «La transparencia, el acceso a la información pública y las normas de buen gobierno deben ser los ejes fundamentales de toda acción política. Sólo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podremos hablar del inicio de un proceso en el que *los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos*».

Es en ese momento de control por la ciudadanía cuando las instituciones reafirman su legitimidad o se deslegitiman[51]. No sólo queremos saber si no espían o no, queremos que los poderes públicos nos informen, que rindan cuentas.

Y es que, desde que saltara a la luz la información sobre el espionaje masivo de datos, en el debate público ha surgido la cuestión de cómo se están gestionando los riesgos o amenazas en nuestros días, y si las técnicas y medidas de lucha contra esos riesgos son proporcionales a los mismos.

Se trata de una cuestión que interesa a la ciudadanía. Esperamos que nuestros gobernantes adopten los medios para conseguir un equilibrio entre la garantía de la seguridad y, al tiempo, la salvaguarda de unos estándares básicos

---

[50] Sobre la dificultad de mantener en secreto muchas de las actividades y sus resultados llevadas a cabo por los servicios de inteligencia puede verse: Fenster, Mark (2014): «The implausibility of Secrecy», *Hastings Law Journal*, n.º 65, págs. 309-369.

[51] En este sentido, la Convención del Consejo de Europa sobre el acceso a los documentos públicos, de 18 de abril de 2009, indica en sus considerandos que la transparencia de las autoridades públicas «fomenta la integridad, la eficacia, la eficiencia y la responsabilidad de autoridades públicas, ayudando así a que se afirme su legitimidad».

de respeto de nuestros derechos. Pero la realidad parece devolvernos otra cara. Justamente la lucha contra la amenaza del terrorismo, que precisamente tiene como destino principal «proteger las libertades de los ciudadanos», ha conllevado el establecimiento de medidas extraordinarias que se alejan mucho de los estándares mínimos nacionales e internacionales de protección de los derechos humanos.

Para analizar cuándo cabe tal limitación de las libertades para protegernos de ese presunto peligro para la seguridad nacional podrían ser útiles las reflexiones de Rawls sobre la llamada «regla del peligro claro y presente». Esta teoría se aplica a los posibles límites a la libertad de expresión, pero, por analogía, cabría aplicarla a la limitación de otros derechos ante un «peligro claro y presente»[52]. Esta teoría fue utilizada por el Tribunal Supremo norteamericano diciendo que «en cada caso, (los tribunales) deben preguntarse si la gravedad del mal reducida por su improbabilidad, justifica tal invasión de (la libre expresión) como la necesaria para evitar el peligro»[53]. Según esta doctrina, la regla no exige que el mal sea inminente, pero sí puede bastar con que sea grande y suficientemente probable. Para Rawls, lo que se necesita es especificar con mayor precisión el tipo de situación que puede justificar la restricción de la libertad. Y para él es necesario que se trate de una situación de emergencia en el que se plantea una amenaza presente o previsible de grave perjuicio. Solo puede limitarse el contenido de un derecho si ello es necesario para evitar una pérdida mayor y más significativa, bien directa o indirecta, de esas libertades[54].

Habrá que partir de nuevo de la idea de que la limitación de derechos debe ser la excepción. Por lo tanto, solo cuando exista una probabilidad razonablemente constatable de que se produzca un daño en la seguridad de los ciudadanos (posibles ataques terroristas), cabrá adoptar medidas que limiten o perjudiquen los derechos de los ciudadanos: el derecho a la intimidad principalmente, pero también la limitación de otras libertades, como el derecho a ser informado o la libertad de expresión.

La regla del peligro inminente nos conduce, inevitablemente de nuevo a la justificación a través de la ponderación de intereses. ¿Tiene justificación que para la persecución de posibles terroristas se almacenen y procesen de forma masiva datos de millones de ciudadanos? ¿tiene sentido que ello se haga sin que exista ningún indicio racional de que los espiados puedan tener la más mínima relación con actos terroristas? ¿el riesgo del terrorismo es tan fuerte que justifica ese tipo

[52] Rawls, John (ed. 1996): *Sobre las libertades*, Barcelona, Paidós, págs. 97 y ss.

[53] Caso *Dennis v. United States*, 341 U. S. 494 en 510, cit. 183 F. 2, en 212.

[54] Rawls, John (ed. 1996): *Sobre las libertades, op. cit, pág. 102-105.*

de intromisiones en la privacidad de los ciudadanos? A nadie escapa que el tipo de controles prospectivos de los que nos ha estado informando la prensa difícilmente pasarían ese test de proporcionalidad. Los riesgos potenciales de ataques terroristas que, con carácter genérico, amenazan de forma global a cualquier Estado no justifican suficientemente el recurso a la «vigilancia total», al escrutinio de los datos de millones de ciudadanos, ni a una invasión infundada de su derecho a la privacidad.

Es cierto que el Estado tiene como funciones principales garantizar la igualdad, la justicia y *la seguridad*, para asegurar a su vez el disfrute de *la libertad* por parte de los ciudadanos[55]. Y que para ello ha de actuar estratégicamente, ha de advertir los posibles riesgos que se ciernen sobre el Estado, analizar las posibles medidas a adoptar y proceder en consecuencia. Pero, debe hacerlo sin menoscabar innecesariamente los derechos y libertades fundamentales de los ciudadanos y hacerlo dentro del marco del Estado de Derecho. Se trata de una cuestión de planteamiento, de entender que los derechos de los ciudadanos son un componente esencial de la propia seguridad que se pretende. En esto son perfectamente pertinentes hoy las palabras que hace años emitiera Revenga: «Quizá hay pocos problemas tan necesitados de desarrollo normativo, jurisprudencial y dogmático como el que plantea elaborar un concepto de seguridad nacional compatible con el Estado democrático. Un concepto capaz de superar una contraposición subliminal entre seguridad y libertad; uno que se decida a asumir, con todas las consecuencias, que el respeto a los derechos cae de lleno en el núcleo duro de la seguridad del Estado democrático»[56].

Ciertamente, los ciudadanos necesitamos confiar en que las actuaciones que llevan a cabo nuestros poderes se rigen por principios como la necesidad, justificación y proporcionalidad, y sobre todo, por el respeto a nuestros derechos y libertades.

---

[55] A este respecto, decía Humboldt que «sin seguridad, el hombre no puede formar ni percibir los frutos de las mismas, pues sin seguridad no existe libertad. Pero la seguridad es, al mismo tiempo, algo que el hombre no puede procurarse por sí mismo; así lo demuestran las razones tocadas de pasada… y la experiencia de nuestros Estados (…) El mantenimiento de la seguridad, tanto frente al enemigo exterior como frente a las disensiones interiores, debe constituir el fin del Estado y el objeto de su actividad». Humboldt, Wilhem von (1988), «El fin último del Estado», en *Los límites a la acción de Estado*, Madrid, Tecnos, 1988, pág. 50-51.

[56] Revenga Sánchez, Miguel (1998): «Razonamiento judicial…», *op. cit.,* pág. 67.

4. LA IMPORTANCIA DE UNA OPINIÓN PÚBLICA INFORMADA. EL PAPEL DE LA PRENSA

Destacábamos ya al inicio de este trabajo la importancia que tiene para un Estado democrático el acceso a la información. Y acabamos de poner de manifiesto el interés que muestra la ciudadanía, las agrupaciones, las ONGs, u otras organizaciones u asociaciones en saber y en ejercer su particular crítica sobre los medios utilizados por el Estado para prevenir posibles riesgos para la seguridad nacional.

Ciertamente, el flujo informativo y la participación ciudadana contribuyen a construir la opinión pública sobre aquellas cuestiones que interesan a todos. Maximizar la circulación de información debiera ser la prioridad en un Estado democrático, porque ello contribuye a que esa opinión pública sea plural, formada y libre. Para favorecer que ello sea así se precisa de unos poderes públicos que no limiten el acceso a la información a aquéllos que pudieran contribuir a difundirla y propiciar ese debate público, particularmente cuando no haya razón para hacerlo porque son cuestiones que, aún pudiendo haber sido secretas, ya son de general conocimiento.

> En este sentido resulta ilustrativo el caso *Youth Initiativa for Human Rights c. Serbia*, que resolvió el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) en su sentencia de 25 de junio de 2013. Una ONG, conocedora de que su Gobierno estaba llevando a cabo controles electrónicos de los ciudadanos se dirigió a la Agencia de inteligencia solicitando información sobre cuánta gente había estado vigilada de este modo durante el año 2005. Dicha información le fue denegada y recurrieron al *Information Commisioner* (órgano interno encargado de asegurar la correcta aplicación de la Ley de información serbia) que les reconoció tal derecho, pero entonces la Agencia de inteligencia comunicó que ya no disponía de los datos que le solicitaban. La Corte de Estrasburgo emitió una loable (aunque posiblemente inesperada) sentencia reconociendo que la negativa de los Servicios secretos a facilitar la información requerida vulneraba el derecho a recibir información y a difundirla posteriormente (Art. 10 del Convenio), pues era obvio que el interés de la ONG en dicha información residía en la voluntad de difundirla y contribuir con ello al debate público.

Indudablemente, en ese proceso de información de la opinión pública, los medios de comunicación juegan un rol fundamental. La libertad de prensa constituye una libertad instrumental del propio derecho de los ciudadanos a ser informados. Son esos medios los que actúan como correa de trasmisión de hechos noticiables y a través de ellos alcanzamos a saber en la mayor parte de las ocasiones lo que de otra manera escaparía a nuestros ojos. La satisfacción del interés

informativo de los ciudadanos en cuestiones de seguridad pende casi por entero de la actividad de la fuentes de información: de los resultado alcanzados por los medios de comunicación tras sus pesquisas y de lo poco que quiera contar el gobierno.

Los medios de comunicación, por cumplir con una función social de gran valor en el seno de una sociedad democrática, deben ser amparados y protegidos por el Derecho de la forma especial que exige el interés colectivo que implica su misión. Pero, en materias relacionadas con la seguridad del Estado, no parece que la facilitación de información a dichos medios para que éstos puedan trasmitirla tenga mucha cabida, incluso puede suceder todo lo contrario.

Decimos esto porque con los programas de espionaje masivo de datos la misma libertad de prensa y, por ende, la formación de una opinión pública libre también puede quedar dañada del modo que ahora explicaremos. Si lo que los programas de espionaje tratan de detectar es precisamente las comunicaciones que se mantienen con presuntos terroristas o países que han dado cobijo al terrorismo internacional (ej. Al-Qaeda), ese control va a terminar recayendo inevitablemente sobre las llamadas/correos de periodistas que cubren la información acerca de los países islámicos, o sobre el terrorismo, o tal vez sobre las primaveras árabes o acerca de cualesquiera otras cuestiones conexas. Precisamente la vigilancia prospectiva conduce (consciente o inconscientemente) al escrutinio de los servicios de inteligencia sobre muchas de las comunicaciones que estos periodistas mantienen en esos ámbitos temáticos y sobre sus fuentes de información. Los profesionales que trabajan para esos medios de comunicación pueden acabar siendo deliberadamente espiados. Sin duda, ello supone una intromisión en el ejercicio de la libertad informativa, genera miedos en aquéllos que se saben posiblemente vigilados y con ello se ponen trabas a un flujo informativo que debiera ser libre.

En Europa se han dado casos de vigilancia electrónica y de comunicaciones de carácter prospectivo por parte de los servicios secretos sobre periodistas que trabajaban en materias que son competencia de los servicios de inteligencia. En un inicio, el TEDH no reconoció que tales vigilancias fueran contrarias al Convenio Europeo de Derechos Humanos por existir suficiente cobertura legal para tal tipo de actuaciones y por responder a un interés legítimo.

> Así sucedió en el asunto *Weber y Saravia c. Alemania*, de 26 de junio de 2006, donde una periodista alemana que investigaba cuestiones que estaban sujetas a la supervisión del Servicio Federal de Inteligencia, y que viajaba para ello a diferentes países de Europa, Sudamérica, y América Central, consideró que podía ser interceptada deliberadamente en sus comunicaciones en cualquiera de

> estos lugares tras la introducción por el Gobierno de un sistema de control prospectivo (*strategic monitoring*). Con este sistema, siguiendo determinadas palabras clave, se rastreaban las comunicaciones y los datos personales de cualquier ciudadano, estuvieran en Alemania o en el extranjero, todo ello con el fin de obtener información para prevenir ataques terroristas u otros riesgos. Para la demandante esos controles coartaban su labor periodística, pues al trabajar ella sobre ese tipo de materias (terrorismo, drogas, tráfico de armas….) podía ser espiada y ya no podía estar segura de que su información y fuentes periodísticas pudiesen seguir siendo confidenciales, lo cual era crucial para la libertad de prensa en un Estado democrático. La Corte, tras analizar la regulación legal de esos controles estratégicos, consideró que ésta era lo suficientemente garantista como para asegurar el no abuso de este instrumento por las autoridades y entendió que esa posible intromisión en las comunicaciones o el posible peligro para la libertad de prensa estaban suficientemente justificados por la salvaguarda de un interés legítimo, la seguridad nacional.

Afortunadamente, no tardaron en llegar decisiones del Tribunal de Estrasburgo donde se consideró este tipo de vigilancia contraria al derecho a la vida privada y al derecho a recibir y difundir información (art. 8 y 10 del Convenio). En el caso *Telegraaf Media Nederland Landelijke Media y otros c. Netherlands* (22 de noviembre de 2011) unos periodistas habían difundido información relativa a actividades de la propia agencia de inteligencia y fueron sometidos a vigilancia con el fin de averiguar sus fuentes de información. El Tribunal no discutió que, efectivamente, detrás de la actuación de vigilancia operada por los servicios de inteligencia estaba el interés de salvaguardar la seguridad nacional, pero aplicó el test de «la necesidad en una sociedad democrática». Este test obliga a determinar si la «injerencia» se justificaba en una «necesidad social imperiosa», si era proporcionada al fin legítimo perseguido y si los motivos alegados por las autoridades nacionales para justificarla eran pertinentes y suficientes. El Tribunal consideró que la legislación en los Países Bajos no había superado este test y no preveía la suficiente salvaguarda en relación con las facultades de vigilancia usados por el Estado en contra de los demandantes con el fin de descubrir sus fuentes periodísticas. Y terminó reiterando una vez más la importancia de la protección de estas fuentes para la prensa libre en cualquier sociedad[57].

[57] La aplicación de este test en otros supuestos de vigilancia puede verse en los asuntos: *Savovi c. Bulgaria*, de 27 de febrero de 2013, o *Ungváry and Irodalom KFT. c. Hungría*, de 3 de diciembre de 2013.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

Desde luego, como recuerda Quill[58], es difícil para los profesionales de la noticia indagar e informar sobre lo que se supone que no se puede saber. Aquí se ha señalado que en un Estado democrático los poderes públicos debieran colaborar y propiciar el flujo de información para promover una opinión pública lo más informada posible. Pero no nos engañemos, ¿cómo vamos a esperar esa colaboración si precisamente esos poderes públicos son los primeros interesados en seguir manteniendo el secreto sobre muchas de esas actividades? Como mucho, y a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos, lo que les queda a los profesionales de la información es el derecho a reclamar que no se impongan trabas artificiales a la libertad informativa y no se inmiscuyan en el proceso de búsqueda y trasmisión de la información, si no existe una necesidad social imperiosa para hacerlo.

5. QUEREMOS SABER EN QUÉ MEDIDA NUESTROS DERECHOS PUEDEN QUEDAR AFECTADOS POR EL ESPIONAJE MASIVO

5.1. La afección al derecho a la intimidad y al secreto de las comunicaciones

En los apartados anteriores nos hemos preguntado acerca del derecho a estar informados y a opinar sobre ciertas medidas preventivas que se han adoptado ante la amenaza del terrorismo internacional, y acerca del papel que la prensa puede jugar en la formación de esa opinión ciudadana sobre dicha materia, que es de indudable interés público. Pero no podemos dejar de analizar una cuestión más, que es que en el espionaje masivo de datos no se trata simplemente de una cuestión de interés público, sino que hablamos de la recopilación de «mis» datos, de que me están controlando «a mí» sin la existencia de indicios de cualquier índole que lo justifique. El ciudadano siente que el halo de privacidad con el que actúa e interactúa en su vida privada —y que es lo que le hace sentirse en libertad— está en peligro. Es cuando la pretendida búsqueda de la seguridad nacional acaba erosionando la «seguridad» que uno tiene en que hay un espacio en el que puede actuar sin controles y que hay una información que corresponde a ese espacio privado y que no goza de mayor relevancia o de la que no se pueden derivar mayores consecuencias.

La realidad es que el conjunto de metadatos que los poderes públicos (o entes privados) pueden almacenar sobre los ciudadanos es incalculable y puede ir desde una información muy sensible (ej. datos sobre salud) hasta otros datos que

[58] Sobre ello véase, Quill, Lawrence (2014): *Secrets and Democracy. From Arcana Imperii to Wikileaks*, New York, Palgrave Macmillan, pág. 8.

aisladamente considerados pudieran parecer no tener gran valor, como por ejemplo quién es el titular de un determinado móvil. Pero, incluso los datos que pudieran no tener especial relevancia (considerados aisladamente), si los analizamos en su conjunto y son bien «tratados», pueden arrojar lo que se denomina una «información de calidad».

Cuando esto sucede cabe plantearse si se ha respetado el derecho a la autodeterminación informativa (como una manifestación de la propia libertad del individuo) y si del tratamiento de estos datos se puede producir una invasión en mi vida privada. Porque, con independencia de que se haya defendido y reconocido la existencia de un derecho autónomo a la autodeterminación informativa, la jurisprudencia y numerosos textos supranacionales han considerado el tratamiento de los datos de carácter personal como una cuestión en la que puede verse afectado el ámbito de la intimidad/privacidad[59] del individuo[60].

Si, además, se cruzan determinados datos de tráfico (identificación de llamadas, interlocutores en mensajes electrónicos…) y se tratan los mismos mediante determinados programas o técnicas informáticas que permiten conocer los interlocutores en una comunicación electrónica o incluso el contenido de la comunicación misma, podría quedar menoscabado el derecho a la inviolabilidad del secreto de las comunicaciones. Así, las modernas tecnologías permiten descifrar los números de identificación de los dispositivos móviles (IMSI y IMEI)[61] y, a partir de ahí, derivar un elenco considerable de datos relativos al titular del aparato móvil, localización de la llamada, interlocutores y otros aspectos más. Es indudable que, de un modo u otro, la recolección y almacenamiento de datos sobre comunicaciones, —que se produce por los servicios de inteligencia—, puede ir más allá de la mera recolección de datos (como el IMEI) para pasar a un procesamiento analítico y estratégico de la información de tráfico de un calado mayor. O incluso tratarse de un control prospectivo del contenido mismo de las comunicaciones[62].

---

[59] Sobre el ámbito de la privacidad o vida privada, como un concepto que tiene mayor capacidad que la intimidad puede verse, MARTÍNEZ MARTÍNEZ, Ricard (2005): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas, págs. 35-44.

[60] Un amplio desarrollo sobre esta cuestión puede verse en RUIZ MIGUEL, Carlos (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», *Revista de Derecho Comunitario*, n.º 14, págs. 7-43.

[61] IMSI, *International Mobile Suscribe Identity*, y IMEI, *International Mobile Identity Module*.

[62] En todo caso, la recopilación de datos que realizan los servicios de inteligencia procede no solo de fuentes propias (la inteligencia de señales, derivada de la interceptación de comunicaciones y emisiones electrónicas; la inteligencia de imágenes; y la inteligencia humana, la que recaban los agentes conocidos comúnmente como espías), sino también de fuentes abiertas, cuya información se recaba de fuentes públicas (internet, prensa…)

Sin ir más lejos, el 31 de julio de 2013, *The Guardian* publicaba información sobre un sistema utilizado por la NSA llamado *XKeyscore*. Esa tecnología, utilizando metadatos —quién, cuándo y dónde accede alguien a una cuenta o a quién envía un mensaje— extrae, filtra y clasifica la información que cualquier usuario ponga en correos electrónicos y conversaciones digitales, así como los historiales de los navegadores de internet[63]. Y el 28 de septiembre de 2013, el *The New York Times* reveló que, desde 2010, la NSA estaba utilizando el tipo de datos a los que nos estamos refiriendo para elaborar perfiles individuales y gráficos complejos donde se describen las interrelaciones entre distintos usuarios de redes sociales[64].

De igual modo, puede traerse a colación, entre otros ejemplos, uno de los mayores sistemas de espionaje e interceptación de comunicaciones electrónicas de la historia —el sistema de interceptación Echelon—, que es controlado por EE. UU., Canadá, Gran Bretaña, Australia y Nueva Zelanda, y que puede capturar comunicaciones por radio y satélite, teléfono, faxes y e-mails en casi todo el mundo y clasificarlas por palabras clave u otros criterios.

Similar inquietud generó en su día el sistema de escuchas telefónicas SITEL utilizadas por las fuerzas de seguridad del Estado y por los servicios del Centro Nacional de Inteligencia españoles. Es un avanzado sistema electrónico que permite interceptar y grabar en tiempo real cualquier conversación telefónica, correo electrónico o mensaje de móvil, además de almacenar en formato digital todos los datos de esas comunicaciones para su posterior análisis[65]. En todo caso, en principio, este sistema de vigilancia sólo puede ser utilizado con autorización judicial previa.

5.2. La necesidad de habilitación legal y de intervención judicial

Con independencia de que esté justificado o no que los servicios de inteligencia recaben tales datos o si tenemos derecho a saber que ello sucede, lo que sí tenemos derecho, como mínimo, es a que las actividades de vigilancia se realicen dentro del respeto a la legalidad vigente y a que el tratamiento de los datos goce de todas las garantías, —por supuesto, cuando afectan a la intimidad y más aún, si interfieren en el secreto de las comunicaciones—.

---

[63] Greenwald, Glenn: «XKeyscore: NSA tool collects 'nearly everything a user does on the internet' », *The Guardian*, 31 July 2013.

[64] Risen, James, y Poitras, Laura: «N. S. A. Gathers Data on Social Networks of U. S. Citizens», *The New York Times*, 28 September 2013.

[65] Una descripción técnica de este sistema pude encontrarse en la STS 250/2009, de 13 de marzo, F. J. 6.º

Por poner un sencillo (pero fundamental) ejemplo, recordemos que cuando se trata de recabar datos derivados de comunicaciones que puedan afectar al secreto de éstas (escuchas telefónicas o electrónicas), nuestra Constitución exige la autorización de un juez, sin distinguir entre interceptaciones individuales de comunicaciones o vigilancia masiva de comunicaciones (art. 18.3 CE). Y cuando dichos controles tienen que ser realizados por los servicios de inteligencia en el marco de sus funciones, la Ley Orgánica 2/2002, reguladora del control judicial previo del Centro Nacional de Inteligencia, indica que «el Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro».

Además, es necesario que exista una previsión legal que permita tal tipo de controles prospectivos, puesto que pueden verse menoscabados derechos fundamentales como el derecho a la intimidad y/o el secreto de las comunicaciones. En relación a esto, procede ahora recalar en el conocido caso de «las escuchas del CESID».

> El centro de escuchas integrado en el Departamento de Acción Operativo del Centro Superior de Información de la Defensa (CESID) había procedido desde el año 1982, con equipos que se fueron renovando y ampliando su capacidad de «barrido», al análisis del espectro radio-eléctrico. Se interceptaban y grababan aleatoriamente conversaciones que se mantenían utilizando el sistema de telefonía móvil automática por ciertos ciudadanos concretos, pero necesariamente quedaban también interceptadas numerosas conversaciones que, menos aún, tenían que ver con la seguridad nacional. Por lo tanto, la vigilancia prospectiva iba más allá de una mera recopilación de datos de tránsito (de comunicación) entrando de lleno en el contenido de las comunicaciones. Las grabaciones así obtenidas, tras su análisis, en unos casos se destruían y en otros, aunque la información careciera de interés desde el punto de vista operativo del CESID, se almacenaban y se conservaban. Los responsables fueron procesados y adujeron que las actividades de vigilancia no tenía otro objeto que proteger altos intereses públicos en permanente riesgo de agresión por potencias extranjeras, que se trataba de una mera acción de vigilancia defensiva y que, sólo de manera muy ocasional y aleatoria, incidía inevitablemente en el espacio de las ondas por las que discurren las conversaciones privadas mediante telefonía celular o móvil. La Audiencia Provincial de Madrid[66]

[66] Sentencia de 26 de mayo de 1999, de la Sección Decimoquinta de la Audiencia Provincial de Madrid.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

consideró esta conducta de delito continuado de interceptación ilegal de las comunicaciones, porque todo ello se realizó sin la existencia de una habilitación legal en aquel momento que autorizara dichas interceptaciones y grabaciones y sin ninguna clase de autorización ni control judicial previo. Además, no amparó la pretendida justificación de la vigilancia en la salvaguarda de un interés general, ni en el cumplimiento de un deber, como alegaban los acusados[67]. En todo caso, esta decisión fue anulada por el Tribunal Constitucional en STC 39/2004, de 22 de marzo, por falta de imparcialidad en el proceso. En una revisión posterior del caso, uno de los inculpados quedó absuelto, mientras otros fueron condenados[68].

En esto el TEDH ha realizado también un loable trabajo de protección de los derechos humanos en el marco de la lucha contra el terrorismo y, en concreto, en la protección de intimidad/privacidad cuando se llevan a cabo programas de vigilancia general o interceptaciones estratégicas, exigiendo no solo una habilitación legal, sino una previsión legal que sea precisa y respetuosa con los derechos fundamentales[69].

Un caso pertinente para el tema que nos ocupa es el que se resolvió por sentencia de 1 de julio de 2008, el asunto *Liberty y otros c. Reino Unido*. Se descubrió que los Servicios de Defensa británicos habían estado interceptando todas las telecomunicaciones entre las dos emisoras de British Telecom (Clwyd y Chester), conexión que soportaba la mayor parte del tráfico de comunicaciones con y desde Irlanda. Esas informaciones se almacenaban y se filtraban mediante palabras clave, perfiles, etc, antes de trasladarlas a los analistas de inteligencia. El Tribunal europeo entendió que esto suponía una injerencia en los derechos de la privacidad y secreto de las comunicaciones al no estar tales controles suficientemente

[67] Por otro lado, la Audiencia provincial de Álava condenó en 2003 a los exdirectores del CESID por las escuchas ilegales que se realizaron a la sede de la ilegalizada *Herri Batasuna* y, de nuevo en este caso, el magistrado no ha admitido la justificación de que las escuchas ser realizaron «en el intento de salvaguardar la seguridad nacional, colocando ésta por encima del derecho a la intimidad y del secreto de las conversaciones telefónicas». Pero la decisión fue anulada por el Tribunal Supremo el 15 de abril de 2004.

[68] El Tribunal de Estrasburgo, en julio de 2002, había reconocido a uno de los inculpados en este caso, Alberto Perote, número dos del CESID, la vulneración del derecho a un proceso imparcial. Aún así, fue condenado en una nueva revisión del caso en octubre de 2006, mientras que otro de los implicados, Emilio Alonso Manglano, en su día Director general del CESID, fue finalmente exculpado por la Audiencia de Madrid el 13 de abril del 2005.

[69] SSTEDH asunto *Klass y otros c. Alemania*, de 6 de septiembre de 1978; asunto *Malone c. Reino Unido*, de 2 de agosto de 1984; asunto *Huving c. Francia*, 24 de abril de 1990; *Koop c. Switzerland*, de 25 de marzo de 1998; Valenzuela Contreras c. España, de 30 de julio de 1998; *Padro Bugallo c. España*, de 18 de febrero de 2003; *Dulkarin Coban c. España*, de 26 de septiembre de 2006; *Weber y Saravia c. Alemania*, 26 de junio de 2006; Asunto *Kennedy c. Reino Unido*, de 18 de mayo de 2010 y otras más citadas en este trabajo.

> previstos por la ley. Extendió las garantías que deben acompañar a estos derechos cuando se trata de interceptaciones de comunicaciones a individuos concretos a las interceptaciones estratégicas o generales, como era el caso, exigiendo que la Ley fijara las garantías y límites al poder que deben establecerse en esa vigilancia prospectiva. Advertía el Tribunal que, «además, como la aplicación de las medidas de vigilancia secreta de las comunicaciones escapa tanto al control de los interesados como del público en general, la «Ley» pugnaría con la supremacía del derecho de que se trata si la facultad discrecional concedida a la Administración no tuviera límites» (Para. 94).

En síntesis, aunque el TEDH ha reconocido que tal tipo de vigilancia prospectiva es a veces necesaria, ha exigido una previsión legal que la regule que sea precisa y respetuosa con los derechos fundamentales, que exista proporcionalidad en el ejercicio de tales prácticas y una autoridad externa independiente que las supervise (STEDH asunto *Rotaru c. Rumania*, de 4 de mayo de 2000)[70]. Recordemos las palabras del Tribunal a este respecto:

> «La Corte, en primer lugar, reiterar su reconocimiento de que el uso de información confidencial es esencial en la lucha contra la violencia terrorista y la amenaza que el terrorismo organizado representa para la vida de los ciudadanos y para la sociedad democrática en su conjunto. Esto no significa, sin embargo, que las autoridades investigadoras tengan carta blanca…»[71]. Pues, «la grabación y otras formas de interceptación de conversaciones telefónicas constituyen una grave injerencia en la vida privada y la correspondencia y en consecuencia debe ser basada en una «ley» que sea particularmente precisa. Es indispensable contar con reglas claras y detalladas sobre el tema, sobre todo porque la tecnología disponible para ello se está haciendo cada vez en más sofisticada[72]».

5.3. El respeto de los principios que rigen el tratamiento de datos

Por otro lado, los ciudadanos deberíamos estar seguros de que se cumplen determinadas garantías en el tratamiento de los datos personales o de tráfico recabados por los servicios de inteligencia. Pese a que la LO 15/1999, de protec-

[70] Sobre esta decisión y otra jurisprudencia del Tribunal Europeo de Derechos Humanos en materia de vigilancia de comunicaciones y datos puede verse el valioso trabajo: Górriz Royo, Elena M. (2013): «Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas», en González Cussac, José Luis y Cuerda, Arnau, M. Luisa (Dir.), *Nuevas amenazas a la seguridad nacional*, Valencia, Tirant lo Blanch, págs. 243-283.

[71] *Murray c. the United Kingdom*, 28 de octubre de1994, para. 58.

[72] *Kopp C. Switzerland*, 25 de marzo de 1998, para. 72.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

ción de datos, no se aplica a los ficheros sometidos a la normativa sobre materias clasificadas o a los establecidos para la investigación del terrorismo (art. 2), los principios básicos que informan dicha Ley no dejan de tener pertinencia también en ese tipo de información recabada, almacenada y tratada por los servicios de inteligencia. Son principios que informan, entre otras cosas, cuándo se pueden recopilar datos, cuándo pueden cederse, o qué medidas de seguridad se adoptan para evitar el acceso de terceros. Estos principios son los de *consentimiento, necesidad/calidad, finalidad, información y seguridad*.

Los principios de *consentimiento* e *información*, al igual que quedan excepcionados por la Ley de Protección de datos para los ficheros de los cuerpos de seguridad del Estado, también quedan excepcionados por la Ley reguladora del Centro Nacional de Inteligencia por el carácter secreto de toda información de inteligencia que generen dichos servicios (art. 5). Por lo tanto, no podemos decir que exista un derecho a acceder a los ficheros producto de la vigilancia prospectiva para inteligencia, ni es necesario nuestro consentimiento para que se recaben esos datos y difícil es pedir información al respecto. Sobre estos aspectos ya hemos incidido en apartados anteriores. Cosa distinta es la necesidad de que se cumplan ciertos requisitos para poder recabar y tratar dicha información.

En cuanto al principio de *necesidad/calidad*, que exige que solo se puedan tratar datos cuando sean adecuados, pertinentes y no excesivos, habría que analizar en cada caso si estamos ante una actividad de recogida y tratamiento de datos que responda a un interés que justifique suficientemente la necesidad de llevarla a cabo. Es necesaria la justificación porque, como hemos indicado, de tal vigilancia y tratamiento de datos pueden derivarse posibles daños para los derechos de los ciudadanos, fundamentalmente para la salvaguarda de la privacidad/intimidad y el derecho a la autodeterminación informativa de los titulares de tales datos[73], y en ocasiones para el secreto de las comunicaciones. Así, el art.

[73] Así se desprende de la normativa nacional y europea. Recuérdese ahora la adoptada en el marco de la Unión Europea:

(1) La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, exige que los Estados miembros protejan los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de datos personales y, en particular, su derecho a la intimidad, para asegurar el libre flujo de datos personales en la Comunidad.

(2) La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, traduce los principios establecidos en la Directiva 95/46/CE a normas específicas para el sector de las comunicaciones electrónicas.

8.2 del Convenio Europeo de Derechos Humanos establece que no podrá haber injerencia de los poderes en el derecho a la vida privada, y en el secreto de la correspondencia y comunicaciones, en tanto en cuanto esta injerencia no esté prevista por la ley y constituya una medida que sea necesaria para el logro de alguno de los objetivos de interés general que enumera, entre los cuales se halla la seguridad nacional[74]. Por lo tanto, la recogida y tratamiento de datos personales y de comunicaciones debiera producirse sólo cuando sea realmente necesario para la salvaguarda de la seguridad. Y entendemos esa idea de «necesidad» en el sentido de relación directa entre el conocimiento de esa información y la defensa de la seguridad en algún aspecto concreto. Pero no solo basta con que exista una necesidad, sino que hemos de acudir, como ya lo hiciéramos en el punto 3 al principio de proporcionalidad, que es el límite de toda injerencia estatal en los derechos fundamentales. Es decir, que además de perseguir la salvaguarda de la seguridad nacional, sea estrictamente necesario tal control y que no existan medios alternativos menos invasivos para alcanzar la garantía de tal seguridad. Nos remitimos a lo que ya hemos indicado sobre el principio de proporcionalidad.

Respecto del principio de *seguridad*, y teniendo en cuenta que la tecnología avanza a pasos agigantados, hemos de pensar en las medidas que han de adoptarse para evitar que esos datos caigan en manos de terceros, no sólo porque podrían utilizarlos para dañar la intimidad de sus titulares, sino también para la comisión de delitos, para lucrarse con su uso o incluso para atentar contra la seguridad nacional o minorarla. Porque los datos con los que operan los servicios de inteligencia no sólo son sensibles para los titulares de los mismos, sino para la propia institución. Su conocimiento podría desvelar sus fuentes, modos de proceder o de encriptar, o simplemente desvelar cualquier aspecto de su forma de trabajar. Precisamente por ello se mantienen secretos.

La preocupación por la seguridad de las bases de datos sobre información clasificada ha estado presente en la UE desde hace años, en cuyo marco se han ido adoptando normas de seguridad para la protección de la información cla-

(3) Los artículos 5, 6 y 9 de la Directiva 2002/58/CE definen las normas aplicables al tratamiento, por los proveedores de red y de servicios, de los datos de tráfico y de localización generados por el uso de servicios de comunicaciones electrónicas. Estos datos deben borrarse o hacerse anónimos cuando ya no se necesiten para la transmisión, salvo los datos necesarios para la facturación o los pagos por interconexión. Previo consentimiento, determinados datos pueden también tratarse con fines comerciales y la prestación de servicios de valor añadido.

[74] Sobre la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre esta cuestión y la aplicación del art. 8.2 del Convenio Europeo de Derechos Humanos pueden verse las decisiones que se citan en el último punto de este trabajo en el texto y a pie de página.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

sificada[75]. Igualmente, conscientes de la evolución de la sociedad y las tecnologías de la información, se aprobó en España, por Orden Ministerial 76/2006, de 19 de mayo, la política de seguridad de la información del Ministerio de Defensa, mejorando con ello las escasas previsiones anteriores que existían en cuestión de seguridad de la información[76]. Y en 2010 con el Real Decreto 3/2010, de 8 de enero, se entró a regular el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, con el fin de genera confianza sobre los medios electrónicos en la relación entre el ciudadano y la Administración Pública. En todo caso, la tecnología mantiene un imparable progreso que exige, a su vez, de una respuesta en materia de seguridad de datos que siga idéntico ritmo.

Por último, lo mismo cabe decir respecto de otras reglas de juego propias del tratamiento de datos, como el derecho a que nuestros datos sean usado únicamente con la finalidad para la que fueron recabados (*Principio de finalidad*). ¿Tenemos garantía de que ellos es así? ¿Acaso esa masiva recopilación de datos no puede estar sirviendo al tiempo a otros intereses distintos al de la salvaguarda de la seguridad?

En relación a esto, cobra relevancia lo concerniente a la cesión de datos. Poco después de los ataques terroristas del 11 de septiembre de 2001, se hizo público que entre la UE y el Departamento del Tesoro de EE. UU. se había acordado un Programa de Seguimiento de la Financiación del Terrorismo (TFTP UE-EE. UU.), Programa que fue renovado en 2010 por un nuevo Acuerdo[77], y confirmado por la Comisión Europea en febrero de 2011 y diciembre de 2012. El TFTP permite a las autoridades estadounidenses controlar el acceso a las transferencias de datos bancarios con respecto a los sospechosos de terrorismo de la UE y viceversa. Desde entonces, el TFTP ha generado inteligencia significativa que ha sido de gran utilidad tanto para los EE. UU. como para la UE en la lucha contra el terrorismo, pero también ha abierto muchas preguntas acerca de la protección de los derechos fundamentales. De hecho, el Comité de Derechos Civiles del Parlamento Europeo ha estado estudiando la posibilidad de modificar el TFTP

[75] Decisión del Consejo 2001/264/EC, sobre las normas de seguridad del Consejo. Estas normas fueron modificadas en 2011, Decisión del Consejo 2011/292/UE, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE.

[76] Entre otras, las que se contemplaban en el Decreto 242/1969, de desarrollo de la Ley de Secretos oficiales; Orden Ministerial 12/1982, de 21 de octubre, del manual de seguridad industrial de las Fuerzas Armadas; Ley 15/1999, de protección de datos,…

[77] *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, signed in Brussels*, 28 de junio de 2010.

UE-EE. UU, al considerar que ya no protege suficientemente la intimidad de los ciudadanos de la UE[78]. También en el ámbito de la UE la Decisión Marco del Consejo 2006/960/JAI, estableció un sistema simplificado de intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, que tuvo su desarrollo en nuestro país a través de la Ley 31/2010, de 27 de julio. Ha de hacerse notar que en dicha norma se prevé la posibilidad de que las autoridades españolas se nieguen a trasmitir esa información de inteligencia, entre otros motivos, cuando «fuera claramente desproporcionado e irrelevante para el fin que persigue la solicitud» (de cesión de información) (art. 11.1.c).

5.4. De nuevo el test de proporcionalidad

Sobre muchos de los puntos que acabamos de enumerar se ha pronunciado recientemente el Tribunal de Justicia de la UE, en el asunto *Digital Rights Ireland y Seitlinger y otros* (2014)[79], contribuyendo a aportar luz a las cuestiones que nos planteábamos. La Corte de Luxemburgo ha mostrado de nuevo su sólido compromiso con la prevalencia de los derechos fundamentales al invalidar la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Esta Directiva permitía la conservación de los datos de tráfico y localización, y de identificación del abonado o usuario para fines de prevención y persecución de delitos graves como la delincuencia organizada y el terrorismo. Para el Tribunal, aunque dicha conservación de datos para su posible trasmisión a las autoridades nacionales responde a un objetivo de interés general, —la seguridad pública—, el legislador de la Unión sobrepasó los límites que exige el principio de proporcionalidad. El modo en que la Directiva regulaba la conservación de datos suponía una injerencia amplia y especialmente grave en los derechos fundamentales, siendo necesaria una regulación que garantice que dicha injerencia se limite

[78] Por las limitaciones de este trabajo no es posible profundizar sobre otros episodios de cesión de datos entre países de la UE y EE. UU. realizados también en el marco de la protección de la seguridad nacional. Piénsese en las dudas que suscitó el Acuerdo de cesión de datos de pasajeros que debían ser trasmitidos por las compañías aéreas cuyos vuelos tuvieran como destino final o de tránsito EE. UU.

[79] Sentencia Tribunal de Justicia de la Unión Europea, Gran Sala, de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12.

efectivamente a lo estrictamente necesario. La invalidez de la Directiva se ha justificado en que (1) ésta no definía la magnitud y gravedad de los delitos que justificarían esa injerencia en los derechos fundamentales. (2) La Directiva abarcaba de modo generalizado a todas las personas, medios de comunicación electrónica y datos, sin ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra delitos graves. Supondría una interferencia en los derechos fundamentales de la práctica totalidad de la población europea, incluyendo incluso a las personas sometidas a la obligación del secreto profesional. (3) Tampoco concretaba las condiciones materiales y procesales en las que las autoridades nacionales competentes podían tener acceso a los datos y su utilización posterior (por ejemplo, control previo por un órgano judicial). Igualmente, (4) el Tribunal ha considerado que los plazos temporales de conservación debieran establecerse conforme a las categorías de datos y posible utilidad con respecto al objetivo perseguido. Asimismo, (5) ha estimado que la Directiva no contenía garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y (6) contra cualquier otro acceso y utilización ilícitos de los datos, esto es, ha hecho hincapié en la cuestión de las medidas de seguridad para la protección de los datos. Por último (7), el Tribunal ha criticado que la Directiva no obligaba a que los datos se conservasen en el territorio de la UE. En definitiva, ha concluido que la Directiva no respeta el principio de proporcionalidad.

Junto a todo ello, y en relación a nuestro tema de análisis, resulta especialmente relevante la advertencia de que la retención de esos datos puede generar en sus titulares «la idea de que sus vidas privadas están sujetas a una constante vigilancia» (apartado 37).

La sentencia del Tribunal de Luxemburgo coincide con el perfil limitador adoptado anteriormente por algunos tribunales nacionales sobre el control de datos de los ciudadanos en el ámbito de la lucha antiterrorista.

> Así, el Tribunal Constitucional alemán, en su decisión de 23 de mayo de 2006[80], estableció límites a la policía en su capacidad sobre el tratamiento automatizado de datos relativos a supuestos simpatizantes del terrorismo internacional (células *durmientes*), al exigirles para ello que existiese un peligro concreto para la seguridad. Y en la sentencia de 27 de febrero de 2008[81], estableció que la normativa de un *Land* que permitía a los servicios de inteligencia del *Land* la facultad de acceder a los ordenadores y sistemas informáticos, cuando hubiera sospechas de que se estaban llevando a cabo a través de los mismos actividades

[80] BVerfG. 1 BvR 518/02, de 23 de mayo.
[81] BVerfG. 1 BvR 370/07, de 27 de febrero.

terroristas, vulneraba el derecho a la intimidad y a la autodeterminación informativa. Para el Alto tribunal es imprescindible que ello se realice con la intervención de un juez y solo en el caso de que exista un grave interés público como la tutela de la vida, integridad o libertad.

Por lo tanto, de nuevo volvemos a la exigencia de los requisitos que alegábamos desde un inicio: ante la imprecisión de las previsiones legales que autorizan a los servicios de inteligencia a llevar a cabo determinadas vigilancias prospectivas, la única medida de la que disponemos es la de la intervención judicial. A través del control judicial podrá ponderarse lo que ya indicamos: si la injerencia en los derechos fundamentales (derecho a la autodeterminación/ secreto de las comunicaciones) responde justificada y proporcionalmente a un interés mayor que ha de salvaguardarse.

6. REFLEXIONES FINALES

Posiblemente no seamos conscientes de la cantidad ingente de datos documentales, de imágenes, de grabaciones sonoras, de transacciones bancarias, de comunicaciones realizadas, de contratos suscritos, y de mil y un aspecto más, que se encuentran almacenados sobre los ciudadanos. En la mayor parte de las ocasiones o no sabemos de su existencia, o solo nos lo imaginamos, o no podemos conocerlo porque son datos tratados en el marco del secreto de Estado. Lo que es palpable es que existe un déficit de información sobre todo ello. Además, como indicaba Sansó-Rubert, parece que las actividades de los servicios de inteligencia «que puedan vulnerar los derechos y libertades, en la práctica, únicamente son controladas por el poder judicial, el político y la opinión pública cuando llegan a cierto nivel de penetración, sea esta cualitativa o cuantitativa. En los restantes casos, la impunidad de estas organizaciones de seguridad está casi garantizada»[82]. El carácter secreto de la información de inteligencia hace impenetrable a la opinión pública toda esa información. Sólo cuando se produce una desclasificación de la misma o cuando alguien indebidamente saca a la luz pública esos datos, —como ha sucedido en varias ocasiones, siendo la más sonada recientemente la del caso Snowden— es cuando la opinión pública empieza a exigir su derecho a ser informado y a ejercer el poder de control. Es cuando en democracia los ciudadanos se convierten en participantes activos del proceso de rendición de cuentas.

[82] Sansó-Rubert, Daniel (2006): «El papel de la información en la lucha contra la delincuencia organizada», *UNISCI Discussion Papers*, n.º 18, págs. 218-19.

Indudablemente, la convivencia entre la libertad informativa y el secreto es difícil. Díez-Picazo Giménez explicaba que «la democracia no puede sobrevivir sin opinión pública; y opinión pública es tanto opinión del público como opinión sobre asuntos públicos. Ello se traduce en una innegable necesidad de información y crítica, sin las cuales resulta imposible la exigencia de responsabilidad, política y jurídica, a quienes desempeñan funciones públicas»[83]. Pero, como decíamos, esa opinión pública no puede versar sobre todo, porque no todo se puede saber o no a todo se puede acceder. En ocasiones hay derechos, bienes o intereses mayores que proteger, que justifican la excepción a la regla general de la publicidad que adjetiva a un Estado democrático. Como se ha visto, el secreto respecto de las actuaciones encaminadas a la salvaguarda de la seguridad del Estado es buen ejemplo de ello.

Pero, la salvaguarda de la seguridad no puede convertirse siempre en una excusa para convertir en opacas ciertas actuaciones de los poderes públicos y eximir a las mismas del natural proceso de rendición de cuentas ante la sociedad y ante los tribunales.

Como advertía Innerarity[84], nuestras principales discusiones futuras van a girar en torno a la cuestión de cómo valoramos los riesgos y qué conductas recomendamos en consecuencia. Éste autor apuesta por practicar toda la normalidad que sea posible en la gestión de las amenazas[85]. Y por una gestión *democrática* de las actuales situaciones de riesgo. Porque en la gestión de esos riesgos hay otros actores que también quieren expresar su parecer: los movimientos sociales, la sociedad civil[86].

Desafortunadamente, es complicado para la ciudadanía medir conceptos como «valores en juego», «peligro», «amenaza», o «daños». Incluso para los expertos resulta muy difícil dar una respuesta objetiva, clara y consistente. No es sencillo conciliar los importantes intereses nacionales relativos a la seguridad, con los igualmente importantes intereses de una sociedad abierta e informada. Pero los ciudadanos queremos ser partícipes de ese debate.

Tal vez no tengamos derecho a conocer de la existencia de determinadas investigaciones y actuaciones que llevan a cabo los servicios de inteligencia,

---

[83] Díez Picazo, Luis María (1997): «Publicidad y secreto en la Constitución», *Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial, Madrid, pág. 3.

[84] Innerarity, Daniel (2011): «Introducción: La humanidad amenazada», *La humanidad amenazada: Gobernar los riesgos globales* (Daniel Innerarity y Javier Solana, coord.), Paidós, pág. 13.

[85] *Ibidem,* pág. 19.

[86] En el mismo sentido, Jáuregui, Gurutz (2011): «La emergencia de un nuevo orden jurídico-institucional: el Estado y la Constitución de la era de la globalización», en *La humanidad amenazada, op. cit., pág. 241.*

porque ello podría poner en riesgo la defensa y seguridad del Estado, pero no se nos puede excluir de un debate más amplio sobre una cuestión que afecta a todos. Los ciudadanos tienen derecho a recibir explicaciones sobre las actuaciones públicas que les conciernen cuando no está justificada su ocultación, a que exista una cierta trasparencia sobre los principios o reglas que se utilizan para clasificar una materia como secreta (ello podría llevarnos a hablar aquí del secreto «legítimo» y secreto «ilegítimo, como lo hiciera Fenster[87]), a realizar un escrutinio de las actividades llevadas a cabo por el Gobierno una vez se hacen públicas, a criticar los excesos en la respuesta estatal ante los posibles riesgos, a exigir una rendición de cuentas, y a un sinfín de cosas más. Porque, para hacer frente a la amenaza del terrorismo, como a cualesquiera otras, habrá que barajar principios como los de prevención, precaución y anticipación, pero también los de proporcionalidad, justificación, respeto al Estado de Derecho y responsabilidad frente a los ciudadanos y ante los tribunales.

La opinión pública tiene derecho a exigir todo ello porque la política de seguridad nacional ha de diseñarse e implementarse también bajo el enfoque de los derechos fundamentales. Pues, como advertía Torres del Moral (y coincidimos con él), no puede olvidarse que la seguridad no es un fin en sí misma, sino un instrumento o, si se quiere, un fin instrumental al servicio de la libertad, de la justicia y de la dignidad humana. Por ello se alude a la seguridad de los derechos, la seguridad de las libertades o la seguridad de las instituciones[88].

La seguridad nacional no puede justificar cualquier intromisión o limitación de las libertades. En un Estado de Derecho sólo se pueden aceptar injerencias en los derechos fundamentales por parte de los servicios de inteligencia cuando estos ejerzan sus atribuciones dentro de la legalidad. Pero, además, la ley no puede acomodar cualquier excepción empleando la seguridad como pretexto.

Cierto es que la política de inteligencia y defensa del Estado es responsabilidad del ejecutivo y la actuación en este ámbito se rige por reglas de discrecionalidad (de opción política), pero ello no quiere decir que pueda estar exento de control y menos cuando se actúa sin respeto a la legalidad o de forma desproporcionada. Que los márgenes de apreciación del ejecutivo sobre qué acciones convienen o pueden ser eficaces para la defensa de la seguridad nacional —o sobre qué puede hacerse público o debe mantenerse en secreto— puedan ser amplios, no significa que no tenga límites. Ese poder gubernamental debe ser delimitado, y no puede ser excesivo o descomedido, pues ha de respetar el principio de proporcionalidad. De ahí

[87] Fenster, Mark (2014): «The implausibility of Secrecy», *op. cit.,* pág. 360.

[88] Torres del Moral, Antonio (2010): «Terrorismo y principio democrático», *Revista de Derecho Político*, n.º 78, págs. 106-107.

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

que si se realiza un acopio masivo de datos de millones de ciudadanos, es preciso que sea por una causa legítima, cual es la seguridad del Estado, que dichos controles sean necesarios para prevenir los peligros que se ciernen sobre la seguridad nacional y que se justifique que no existen medios menos gravosos para la intimidad de los individuos. Y si resulta que un control preceptivo e indiscriminado de datos y comunicaciones es altamente necesario para dicha seguridad y está justificado que se mantenga bajo secreto, así tendrá que ser. Pero mientras tanto, la regla es que la limitación de los derechos fundamentales constituye una excepción. Existen parámetros que han sido elaborados por la jurisprudencia y la doctrina para medir la proporcionalidad entre la adopción de esas medidas para prevenir posibles daños a la seguridad nacional y los perjuicios que ello pueda causar a los derechos fundamentales (recuérdense ahora los términos a los que hemos aludido en este trabajo: «Peligro inminente», «necesidad social imperiosa», «idoneidad de las medidas», «intervención mínima»…).

La dificultad estriba en que mientras estas actuaciones permanecen bajo el manto del secreto, no cabe someterlas a ese test. Lo que no se sabe no se puede controlar. Ahora bien, cuando lo secreto sale a la luz pública, los mecanismos de control judicial pueden empezar a utilizarse. Y es también en ese momento cuando los ciudadanos directamente o a través de sus representantes pueden exigir explicaciones públicas sobre las medidas adoptadas. Precisamente, en un informe, de 23 de septiembre de 2014, del Relator especial de Naciones Unidas sobre terrorismo y derechos humanos[89] se realiza una dura crítica al espionaje masivo llevado a cabo por los servicios de inteligencia estadounidenses e ingleses, y de otros Estados. En el informe se denuncia que el modo indiscriminado en que esos controles se han realizado supone una interferencia sistemática de la intimidad de las comunicaciones. Pero, además, indica que «Los Estados han fallado en proveer detallada y razonada justificación pública de su necesidad, y casi ningún Estado ha adoptado derecho interno para autorizar su uso». Y añade: «Los Estados que han utilizado esa tecnología se reservan un monopolio sobre esa información que es una forma de censura, que impide un debate público informado».

Cuando la ciudadanía se siente coartada en sus derechos es cuando mayor necesidad tiene de exigir una justificación. Porque podemos entender la importancia de prevenir los riesgos que amenazan la seguridad nacional, pues sin seguridad no nos sentimos libres, pero si se coartan nuestras libertades, de nada nos sirve sentirnos seguros.

[89] UN General Assembly, Rapport of the Special Rapporteur on the Promotion and protection of human rights and fundamental freedoms while counter-terrorism, de 23 de septiembre de 2014, (A/69/37).

BIBLIOGRAFÍA

Álvarez Conde, Enrique (1997): «El temor del Príncipe o el temor al Príncipe. Secretos de Estado y Constitución», *Anuario Jurídico de La Rioja*, n.º 3, págs. 349-364.

Beck, Ulrich (2011): «Convivir con el riesgo global», en *La humanidad amenazada: Gobernar los riesgos globales (Daniel Innerarity y Javier Solana, coord.)*, Paidós, págs. 25 y ss.

Brown, Ian y Korff, Douwe (2009): «Terrorism and the proportionality of Internet Surveillance», *European Journal of Criminology*, vol. 6 (2), págs. 119-134.

Cole, David Cole; Fabbrini, Federico y Vedaschi, Arianna (eds.) (2013). *Secrecy, national security and the vindication of Constitutional Law*, Cheltenham, Edward Elgar Publishing Limited.

Cousido González, Pilar (1995): *Comentario a la Ley de Secretos Oficiales y su reglamento*, Barcelona, Bosch.

Cuerda Arnau, M. Luisa (2013): «Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes», en González Cussac, José Luis y Cuerda, Arnau, M. Luisa (Dir.), *Nuevas amenazas a la seguridad nacional*, Valencia, Tirant lo Blanch, págs. 103-143.

De Lucas, Javier (1990): «Democracia y transparencia. Sobre poder, secreto y publicidad», *Anuario de Filosofía del Derecho*, vol. VII, págs. 131-145.

De Vergottini, Giuseppe (2004): «La difícil convivencia entre libertad y seguridad. Respuestas de las democracias al terrorismo», *Revista de Derecho Político*, n.º 61, págs. 11-36.

Díez Picazo, Luis María (1997): «Publicidad y secreto en la Constitución», *Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial, Madrid.

Esteban Navarro, M. A. y Carvalho, A. V. (2012): «Inteligencia: concepto y práctica», en González Cussac, J. L. (Coord.): *Inteligencia*, Valencia, Tirant lo Blanch, págs. 17-71.

Feldman, David (2005): «Terrorism, human rights and their Constitutional implications», *European Constitutional Law Review*, Vol 1 (3), págs. 531-552.

Fenster, Mark (2014): «The implausibility of Secrecy», *Hastings Law Journal*, n.º 65, págs. 309-369.

Fiss, Owen M. (2013): «El mundo en el que vivimos», *El Cronista del Estado social*, n.º 37, págs. 20-31.

Flores Giménez, Fernando (2013): «Somos transparentes, son opacos», *Al Revés y al Derecho*, 2 de septiembre de 2013, versión digital: http://alrevesyalderecho.infolibre.es/?p=1582

Goldsmith, Jack (2012). «Power and Constraint: National Security Law After the 2012 Election», *Case Western Reserve Journal of International Law*, vol. 45.

González Cussac, Jose Luis; Larriba Hinojar, Beatriz y Fernández Hernández, Antonio (2012): «Servicios de inteligencia y Estado de Derecho», en González Cussac (Coord.): *Inteligencia*, Valencia, Tirant lo Blanch, págs. 281-311.

Górriz Royo, Elena M. (2013): «Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas», en González Cussac, José Luis y Cuerda, Arnau, M. Luisa (Dir.), *Nuevas amenazas a la seguridad nacional*, Valencia, Tirant lo Blanch, págs. 243-283.

Groppi, Tania (2013): «El papel de los tribunales en el control de las medidas contra el terrorismo internacional: ¿hacia un diálogo jurisprudencial», *Revista de Derecho Político*, n.º 86, págs. 309-356.

Gross, Emanuel (2004): «The struggle of a Democracy Against terrorismo —Protection of Human Rights: The Right to Privacy versus teh National Interest— The Proper Balance», *Cornell International Law Journal*, Vol. 37, págs. 27-93.

Guerrero Gutiérrez, Eduardo (2010): «Transparencia y seguridad nacional», *Cuadernos de Transparencia*, n.º 18, Instituto Federal de Acceso a la Información y Protección de datos, págs. 9-54. http://www.eldiario.es/turing/Espionaje-derechos-humanos_0_159934512.html

Humboldt, Wilhem von (1988), «El fin último del Estado», en *Los límites a la acción de Estado*, Madrid, Tecnos, 1988,

Innerarity, Daniel (2011): «Introducción: La humanidad amenazada», en *La humanidad amenazada: Gobernar los riesgos globales (Daniel Innerarity y Javier Solana, coord.)*, Paidós.

Jáuregui, Gurutz (2011): «La emergencia de un nuevo orden jurídico-institucional: el Estado y la Constitución de la era de la globalización», in *La humanidad amenazada, op. cit., pág. 241.*

Kempen, Piet Hein van (2013): «Four concepts of Security-A Human Rights Perspective», *Human Rights Law Review*, n.º 1, págs. 15-16.

Martínez Martínez, Ricard (2005): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas.

Open Society Justice Iniciative (2013): *Globalizing torture CIA Secret Detention and Extraordinary rendition*, New York, Open Society Foundations.

Quill, Lawrence (2014): *Secrets and Democracy. From Arcana Imperii to Wikileaks*, New York, Palgrave Macmillan.

Rallo Lombarte (2002): «Medios de comunicación y democracia. Apuntes para una reforma», en *Estudios de Derecho Constitucional homenaje a Joaquín García Morillo* (Coord. Luis López Guerra), Valencia, Tirant lo Blanch, págs. 223-250.

Rawls, John (ed. 1996): *Sobre las libertades*, Barcelona, Paidós.

Revenga Sánchez, Miguel (1995): *El imperio de la política. Seguridad nacional y secreto de Estado en el sistema constitucional norteamericano*, Barcelona, Ariel.

— (1998): «Razonamiento judicial, seguridad nacional y secreto de Estado», *Revista Española de Derecho Constitucional*, n.º 53, págs. 57-74.
— (2001): «Servicios de inteligencia y derecho a la intimidad», *Revista Española de Derecho Constitucional*, n.º 61, págs. 59-84.
— (2008): «Tipos de discurso judicial en la guerra contra el terrorismo a propósito de la sentencia del Tribunal Supremo de Estados Unidos en el caso *Boumediene c. Bush*», *Pensar, Fortaleza*, vol 13, n.º 2, págs. 175-188.
Roach, Kent (2013): «Managing secrecy and its migration in a post 9/11 world», en *Secrecy, national security*…, *op. cit.,* págs. 119-120.
— (2014): «The 9/11 effect in comparative perspective: some thoughts on terrorism la in Canada, Spain an the United States», en Miguel Revenga Sánchez (Director), *Terrorismo y Derecho bajo la estela del 11 de septiembre*, Valencia, Tirant lo Blanch, págs. 21-60.
Ruiz Miguel, Carlos (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», *Revista de Derecho Comunitario Europeo*, n.º 14, págs. 7-43.
Sánchez Ferro, Susana (2006): *El secreto de Estado*, Madrid, Centro de Estudios Políticos y Constitucionales.
— (2009): «Libertades informativas y poder ejecutivo: secretos oficiales», en Torres del Moral (Dir.), *Libertades informativas*, Madrid, Ed. Constitución y Leyes Colex, págs. 1017-1058.
Sansó-Rubert, Daniel (2004): «Seguridad vs. libertad: el papel de los servicios de inteligencia», *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, n.º 48, págs. 85-112.
— (2006): «El papel de la información en la lucha contra la delincuencia organizada», *UNISCI Discussion Papers*, n.º 18, págs. 207-227.
Scheinin, Martin (editor) (2013): *Terrorism and Human Rights*, Elgar Research Collection, Edward Elgar Ed.
Tejerina Rodríguez, Ofelia (2014): *Seguridad del Estado y privacidad*, Madrid, Editorial Reus.
Torres del Moral, Antonio (2009): «El instituto jurídico de la opinión pública libre», en Torres del Moral (Dir.), *Libertades informativas*, Madrid, Ed. Constitución y Leyes Colex, págs. 135-158.
— (2010): «Terrorismo y principio democrático», *Revista de Derecho Político*, n.º 78, págs. 95-160.
Troncoso Reigada, Antonio (2008): «Acceso a la información administrativa y protección de datos personales», en Troncoso (Dir.): *Transparencia administrativa y protección de datos*, Madrid, Thomson-Civitas, especialmente págs. 35 a 39.
— (2010): *La protección de datos personales: en busca del equilibrio*, Valencia, Tirant lo Blanch.

Tzu, Sun (2008), *El arte de la Guerra* (versión de Thomas Cleary), Madrid, EDAF S. L., 35.ª edición.

Vashakmadze, Mindia (2013). «Secrecy vs. Openness: counter-terrorism and the role of the German Federal Constitutional Court», en David Cole, Federico Fabbrini y Arianna Vedaschi (eds.), *Secrecy, national security and the vindication of Constitutional Law*, Cheltenham, Edwuard Elgar Publishing Limited, págs. 46-47.

Vedaschi, Arianna (2013): «*Arcana imperii* and *salus rei publicae*: state secrets privilege and the Italian legal framework», en *Secrecy, national security…*, *op. cit.,* págs. 95-111.

Fuentes provenientes de medios de comunicación

Ackerman Spencer y Ball, James (2014): «Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ», *The Guardian*, 28 de febrero de 2014.

Agencias: «El PP reclama al Gobierno que explique todo lo que sabe de los vuelos de la CIA», *El Mundo*, 1 de diciembre de 2008.

Del Pino, Daniel: «Londres también espía las comunicaciones españolas», *publico.es*, 4 de septiembre de 2013.

Europa Press, «El CNI colaboró con Reino Unido en operaciones encubiertas de vigilancia masiva en internet», *Público.es*, 17 de febrero de 2014.

Follorou, J. Y Johannès, F.: «Révélations sur le Big Brother français», *Le Monde*, 4 de julio de 2013.

Galdón Clavell, Gemma: «Espionaje y derechos humanos: los límites a la intromisión de la intimidad», *eldiario.es*, 4 de agosto de 2013. Versión electrónica: http://www.eldiario.es/turing/Espionaje-derechos-humanos_0_159934512.html

González, Miguel: «Aznar dio vía libre al paso por España de presos hacia Guantánamo y lo ocultó», *El País*, 1 de diciembre de 2008.

Greenwald, Glenn: «XKeyscore: NSA tool collects 'nearly everything a user does on the internet' », *The Guardian*, 31 July 2013.

Risen, James, y Poitras, Laura: «N. S. A. Gathers Data on Social Networks of U. S. Citizens», *The New York Times*, 28 September 2013.

S. A.: «De los 11 vuelos a Guantánamo con escala en España, 9 han sido bajo el mandato de Zapatero», *El confidencial*, 1 de diciembre de 2012.

Savage, Charlie (2014). «Obama to Call for End to N. S. A.'s Bulk Data Collection», *The New York Times*, 24 de marzo de 2014.

Title:

THE PUBLIC OPINION AND THE MASSIVE DATA SURVEILLANCE. A DIFFICULT BALANCE BETWEEN ACCESS TO INFORMATION AND NATIONAL SECURITY

Summary:

1. The threat of international terrorism and the measures to protect national security. 2. We want to know if we are under surveillance, but access to information has limits. The secret on national security. 3. When the secret becomes public. A public debate on the counterterrorism measures. 4. The importance of an informed public opinion. The rol of the press. 5. We want to know how our rights could be affected by the massive surveillance. 5.1. Impact on privacy and secret of communications. 5.2. Need of a legal prevision and a judicial warrant. 5.3. The respect for principles ruling data processing. 5.4. Again the test of proportionality. 6. Final considerations. Bibliography. Other sources.

Resumen:

La transparencia y el acceso a la información convierten a la sociedad en una participante activa del proceso de rendición de cuentas de los poderes públicos. Pero, esa libertad informativa tiene límites, como lo es el secreto que necesariamente impone, en la mayor parte de las ocasiones, la salvaguarda de la seguridad nacional. El secreto —y por lo tanto, la excepción a la regla general de la publicidad— tiene como misión impedir que se conozcan ciertas actividades de inteligencia, que recaban y tratan información con la finalidad de garantizar el éxito de determinadas acciones de los servicios de inteligencia-defensa o de prevenir riesgos. En este trabajo se aborda la difícil convivencia entre el derecho de acceso a la información y el secreto de Estado en un momento en que se ha hecho pública la existencia de un control masivo de datos de los ciudadanos por parte de los servicios de inteligencia nacionales y extranjeros. El objeto principal de análisis es ese tipo de controles/vigilancia de las comunicaciones y datos personales que se realizan con un carácter general, preventivo y/o prospectivo y que se diferencia de los más comunes controles de comunicaciones dirigidos a aportar pruebas en el marco de un proceso penal.

Abstract:

Transparency and access to information turn society into an active participant in the accountability process of public authorities. But

© UNED. *Revista de Derecho Político*
N.º 92, enero-abril 2015, págs. 73-118

that freedom of information has limits, as it is the secret that necessarily the safeguarding of national security imposes many times. The secret —and therefore, the exception to the general rule of publicity— is designed to prevent certain intelligence activities were known and to ensure their success. Between others, these activities consist in processing data of citizens to give enough information to the State to adopt strategic decisions. This essay focuses on the difficult coexistence between the right of access to information and the state secret in a moment when it has come to light the existence of a massive surveillance of citizens' data by national and foreigner intelligence services. The main object of analysis is such control/surveillance of communications and personal data carried out with a general, preventive and/or prospective aim. This type of surveillance differs from the more common controls of communications pointed to provide evidences under criminal proceedings.

Palabras clave:

acceso a la información, seguridad nacional, espionaje, terrorismo, secreto, opinión pública.

Key words:

access to information, national security, surveillance, terrorism, secrecy, public opinion.