PARLAMENTO EUROPEO 2009 - 2014

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

11.12.2013

DOCUMENTO DE TRABAJO 1

sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

Ponente: Claude Moraes

1. Vigilancia masiva de ciudadanos de la UE

Las últimas informaciones han revelado la existencia de sistemas de vigilancia masiva de ciudadanos en los Estados Unidos y en determinados Estados miembros de la UE. Estas actividades, impulsadas por un interés cada vez mayor en la seguridad, sobre todo tras los atentados del 11 de septiembre, fueron posibles gracias al crecimiento del uso de Internet, los avances en tecnología de la comunicación y un débil control de los servicios de inteligencia.

En tan solo los últimos 10 o 20 años, las vidas de los ciudadanos han cambiado completamente debido al uso de Internet, el correo electrónico, la comunicación a través de las redes sociales, las compras en línea, las llamadas de voz sobre IP, las tecnologías de la información y el almacenamiento de datos en la nube. Si bien estos son avances extremadamente positivos, sobre todo en términos de conveniencia y coste, conllevan una cantidad cada vez mayor de datos almacenados en medios electrónicos, muchos de los cuales incluyen información personal y datos privados. Al mismo tiempo, los avances en tecnología han aumentado la capacidad de las agencias de inteligencia para participar en intercepciones y análisis de estos datos a gran escala.

Estos avances tecnológicos parecen haber contribuido, junto con otros factores, a un cambio fundamental en el trabajo y las prácticas de las agencias de inteligencia, que se aleja del concepto tradicional de vigilancia específica como una medida necesaria y proporcional contra el terrorismo y se encamina hacia sistemas de vigilancia masiva. Si bien los servicios de inteligencia realizan una función indispensable a la hora de proteger a la sociedad democrática de amenazas interiores y exteriores, estas tienen que operar de conformidad con el Estado de Derecho; de lo contrario perderán legitimidad y desgastarán los cimientos de la misma sociedad democrática a la que intentan proteger. Este proceso de vigilancia masiva cada vez mayor no se ha sometido a debate público ni a una toma de decisiones democrática sino que las decisiones se han tomado, en gran parte, en pequeños círculos y a puerta cerrada. Parece que los marcos jurídicos, que se establecieron cuando la tecnología no era tan avanzada como ahora, se utilizan para justificar sistemas de vigilancia masiva incluso cuando esta no era la intención de su interpretación jurídica inicial. Debido a que los mecanismos de control de muchos Estados no han ido a la par con el aumento de las capacidades de las agencias de inteligencia, estos sistemas de vigilancia masiva se han seguido desarrollando.

Este debate público ha de tener lugar ahora. Tenemos que debatir la finalidad y el alcance de la vigilancia y qué lugar ocupa en una sociedad democrática. Tenemos que debatir medidas aceptables para combatir la delincuencia y el terrorismo así como dónde hay que dibujar la línea para preservar el derecho a la vida íntima y la protección de los datos personales en un mundo digitalizado. Tenemos que debatir cómo se supone que nuestros servicios de inteligencia deben colaborar sin menoscabar el Estado de Derecho. Tenemos que debatir cómo se efectúan los negocios transatlánticos y cómo el flujo de datos entre los países y continentes se mantiene seguro y se respetan las legislaciones aplicables.

Disponer de información adecuada es una condición vital para este debate. La investigación de la Comisión LIBE tenía por objeto recopilar y evaluar esta información. Este documento de trabajo es un elemento de este proceso que presenta una visión general de las actividades de vigilancia y debate las repercusiones de estas en los derechos fundamentales de los ciudadanos europeos.

2. Programas de vigilancia

En los últimos meses se ha revelado la existencia de numerosos programas diferentes. Se pueden distinguir varios tipos de supuestas cuestiones de vigilancia que repercuten en los derechos fundamentales de los ciudadanos europeos: la vigilancia masiva de ciudadanos europeos por parte de la Agencia de Seguridad Nacional (NSA), la cooperación de las autoridades de los Estados miembros de la UE en los programas de vigilancia dirigidos por la NSA, los programas de vigilancia dirigidos por los propios Estados miembros de la UE, así como los programas de vigilancia de terceros países. A continuación se presentan algunos programas de la NSA y de los Estados miembros de la UE.

Vigilancia masiva de ciudadanos europeos por parte de la NSA

Varios programas de la NSA[1] se centran en las actividades en línea. El **programa PRISM** proporciona presuntamente a la NSA acceso directo a los servidores centrales de nueve empresas de Internet líderes en los Estados Unidos permitiéndoles recopilar material de sus clientes, que incluye el historial de búsquedas, el contenido de los correos electrónicos, las transferencias de archivos y la mensajería instantánea a tiempo real.[2] El Gobierno de los Estados Unidos confirmó la existencia del programa PRISM. Sin embargo, han declarado que no se trataba de un programa de recopilación encubierta o de extracción de datos.[3]

Según los informes, el **programa Xkeyscore** permite a los analistas de la NSA buscar, sin previa autorización, en las amplias bases de datos que contienen correos electrónicos, conversaciones en línea e historiales de navegación de millones de personas así como sus metadatos[4]. Se describió como el sistema de búsqueda más amplio de la NSA que puede supervisar «casi todo lo que un usuario típico hace en Internet». En respuesta a esto, la NSA confirmó la existencia del programa como parte del sistema de recopilación legal de la NSA de señales de inteligencia extranjera diciendo que estaba limitado al personal que requería el acceso para tareas asignadas[5].

BULLRUN es, supuestamente, un programa de descifrado puesto en marcha por la NSA en un intento de descifrar las tecnologías de encriptación comúnmente utilizadas que permitirían a la NSA burlar la encriptación en línea empleada por millones de personas en sus transacciones en línea y correos electrónicos.[6] No se ha recibido respuesta de parte de la NSA en relación con el presunto programa Bullrun. Los informes de The Guardian, The New York

[1] Para una visión general de la situación jurídica de los EE. UU. véase el informe de las conclusiones del grupo de trabajo UE-EE. UU. ad hoc sobre protección de datos de los copresidentes http://register.consilium.europa.eu/pdf/en/13/st16/st16987.en13.pdf

[2] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1

[3] http://online.wsj.com/public/resources/documents/prismfactsheet0608.pdf

[4] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[5] http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml

[6] http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Times y ProPublica afirman todos que los oficiales de inteligencia pidieron que no se publicara la historia por motivos de seguridad nacional.

De conformidad con el artículo 702 de la Ley de vigilancia a la inteligencia extranjera (FISA), se puede requerir a un proveedor de servicios que «proporcione al Gobierno inmediatamente toda la información, medios o asistencia necesarios para completar la recopilación» de información de inteligencia extranjera. No se ha recibido aclaración alguna sobre si esta disposición podría obligar a divulgar claves criptográficas.[1]

Boundless Informant es una potente herramienta de extracción de datos utilizada por la NSA para registrar y analizar la información electrónica mundial. Detalla e incluso localiza por país la enorme cantidad de información, principalmente metadatos, que recopila de las redes informáticas y de telefonía. Según los informes, «la herramienta permite a los usuarios seleccionar un país en el mapa, ver el volumen de metadatos y seleccionar los detalles de las recopilaciones de ese país»[2]. En marzo de 2013, se recopilaron 97 000 millones de datos de inteligencia de redes informáticas de todo el mundo.

MUSCULAR, según informó The Washington Post el 31 de octubre[3], es un programa conjunto dirigido por la NSA y el Cuartel General de Comunicaciones del Gobierno (GCHQ) para interceptar, de enlaces privados, el tráfico de datos que fluye entre los servidores de Yahoo, Google, Microsoft Hotmail y Windows Live Messenger, entre otros. El punto de acceso, DS-200B, se encuentra fuera de los Estados Unidos, lo que hace que el programa esté fuera de la jurisdicción del Tribunal de Vigilancia de Inteligencia Extranjera (FISC) y depende de un proveedor de telecomunicaciones anónimo para proporcionar un acceso secreto a un cable o conmutador por el que pasa el tráfico de comunicaciones. Los documentos de la NSA sobre la actividad se refieren directamente a operaciones de «acceso masivo», de «acceso en bloque» y de «gran volumen» en las redes de Yahoo, Google y Microsoft. Se informó de que numerosos analistas que trabajan en el programa se habían quejado de que MUSCULAR produce demasiados datos, muchos de ellos poco valiosos en términos de inteligencia.

En octubre de 2013, los informes de prensa de Francia, España e Italia afirmaron que la NSA estaba interceptando enormes volúmenes de **llamadas telefónicas**. Por ejemplo, se afirmó que la NSA había recopilado 70,3 millones de registros telefónicos en Francia desde el 10 de diciembre de 2012 al 8 de enero de 2013. Como respuesta, el General Keith Alexander, jefe de la NSA, declaró que los datos eran recopilados conjuntamente por la NSA y las agencias de inteligencia de cada Estado miembro como medida de defensa y con el fin de apoyar operaciones militares[4].

---

[1] Los programas de vigilancia de los Estados Unidos y sus repercusiones sobre los derechos fundamentales de los ciudadanos de la UE
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf
[2] http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining
[3] http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
[4] http://www.washingtonpost.com/world/national-security/top-intelligence-officials-called-to-testify-on-nsa-surveillance-programs/2013/10/29/e9e9c250-40b7-11e3-a751-f032898f2dbc_story.html

Actividades de vigilancia de los Estados miembros de la UE

Según los informes de prensa, la agencia de inteligencia del Reino Unido, el **GCHQ**, tendría supuestamente acceso a las comunicaciones recopiladas por el programa PRISM, permitiéndole eludir el marco jurídico nacional sobre el acceso al material personal de una empresa de Internet establecida fuera del Reino Unido. Los informes también han señalado la participación conjunta del GCHQ con la NSA en el programa MUSCULAR. El Comité de Seguridad e Inteligencia del Parlamento del Reino Unido confirmó que el GCHQ había utilizado material de vigilancia obtenido del programa PRISM de los EE. UU. pero no consideró que este había eludido el Derecho británico al hacerlo.

El GCHQ ha sido acusado de participar en una actividad preliminar de vigilancia conocida como el **programa Tempora** que le permitiría acceder a grandes cables de fibra óptica que llevan cantidades enormes de comunicaciones privadas de los usuarios de Internet y de compartirlos con la NSA. Debido al volumen total de datos recabados, se dice que el contenido de la información se eliminaba pasados 3 días y los metadatos se guardaban normalmente durante 30 días[1].

El GCHQ ha sido acusado de dirigir un programa de descifrado similar a BULLRUN, conocido como **Edgehill**. Este programa tendría por objeto descifrar el tráfico encriptado que utilizan las empresas para proporcionar acceso remoto a sus sistemas y para «seguir trabajando en el conocimiento» de importantes proveedores de comunicación.

Los informes acerca de las actividades del **Instituto de Radio Defensa Sueco (FRA)**, han afirmado que este está recopilando y recibiendo datos de cables de fibra óptica que atraviesan las fronteras suecas desde los países nórdicos, los Estados bálticos y Rusia, y reenviando los datos a los Estados Unidos[2]. También habrían pinchado y supervisado presuntamente de forma sistemática los cables de teléfono e Internet noruegos que atraviesan Suecia, así como los datos de teléfonos móviles y llamadas de otros países nórdicos donde la señal se transmite a través de conexiones GSM suecas.

En **Francia** se ha acusado a la **Dirección General de Seguridad Exterior (DGSE)** de interceptar y recabar metadatos de los correos electrónicos, mensajes de texto y facturas de teléfono mediante un superordenador capaz de recopilar, tratar y almacenar datos. Los datos se interceptan y recopilan mediante estaciones de satélite y pinchando los cables submarinos de fibra óptica. Además, se ha afirmado que otros seis servicios de inteligencia, incluidos los servicios de aduanas y el servicio contra el blanqueo de capitales, tienen acceso a esta base de datos[3].

En **Alemania**, los informes de prensa han afirmado que el **Servicio de información federal (*Bundesnachrichtendienst*, BND)** ha creado oficinas en el DE-CIX (Intercambio de Internet

[1] http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[2] Fuente: M. Klamberg, (2010), «FRA and the European Convention on Human Rights», Nordic Yearbook of Law and Information Technology, Bergen 2010, pp. 96-134
Fuente: Declaración de Duncan Campbell durante la investigación de la Comisión LIBE del Parlamento Europeo sobre la vigilancia electrónica a gran escala de ciudadanos de la UE, primera vista, 5 de septiembre de 2013.
[3] Fuente: J. Follorou y F. Johannes (2013), «Révélations sur le Big Brother français» Le Monde, 4 de julio de 2013.

comercial alemán) para desviar el tráfico entrante, copiar los datos y analizarlos posteriormente en la sede del BND[1]. Los informes también indican que hay una estrecha cooperación entre los servicios de inteligencia alemanes y sus homólogos estadounidenses con informes de millones de metadatos recopilados por el BND y transferidos a la NSA a través de sitios de recopilación de datos en territorio alemán[2].

3. Repercusión sobre los derechos fundamentales en la Unión Europea

Los avances en tecnología han permitido que los Estados sepan más que nunca en la historia sobre los ciudadanos. Si bien antiguamente se requerían esfuerzos considerables y proximidad física para espiar a una persona, la tecnología actual permite esta acción con un alcance y profundidad imposibles hasta el momento.

Los sistemas de vigilancia masiva e indiscriminada repercuten significativamente sobre los derechos fundamentales de los ciudadanos. Aunque existen marcos jurídicos, sigue habiendo dudas con respecto a si los diferentes programas respetan su espíritu y a si su creación se concibe en los marcos jurídicos correspondientes, incluido el Derecho internacional y europeo, sobre todo con respecto a la pregunta de si estos programas se pueden considerar proporcionales, necesarios y apropiados en sociedades democráticas.

Los sistemas de vigilancia masiva descritos anteriormente repercuten principalmente sobre la intimidad de los ciudadanos. Puesto que los servicios de inteligencia pueden recopilar datos relacionados con el contenido de las comunicaciones, así como metadatos, y supervisar las actividades electrónicas de los ciudadanos, en particular su utilización de teléfonos inteligentes y tabletas, pueden saber, de hecho, casi todo sobre una persona. Pueden saber dónde está con programas de localización avanzados[3], con quién habla y durante cuánto tiempo, qué hace, qué compra, qué lee e incluso muy probablemente qué está pensando.

Por tanto, la vigilancia también afecta a otros derechos fundamentales como la libertad de expresión, de opinión, de credo, de asociación, la protección de datos, el derecho a un juicio justo, a acceder a un recurso judicial efectivo, etc. Tal como se destacó durante la investigación, preocupa particularmente la repercusión sobre la libertad de prensa, en especial el efecto amedrentador generado contra los periodistas que facilitan la información necesaria para mantener un debate fundado, mediante técnicas utilizadas bien para intimidar o para ralentizar la elaboración de informes.

Si bien los servicios de inteligencia son esenciales a la hora de proteger frente amenazas internas y externas, tienen que operar siempre conforme al Estado de Derecho. Incluso la existencia de una amenaza para la seguridad nacional no es un motivo suficiente para que un servicio de inteligencia infrinja la ley. Las actividades ilegales por parte de los servicios de inteligencia no solo menoscaban la propia sociedad democrática a la que pretenden proteger,

[1] http://www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html
[2] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html
[3] Los documentos de Snowden revelan que la NSA recopila 5 000 millones de registros telefónicos al día http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden

sino que también minan la legitimidad, la confianza democrática y el apoyo que estos necesitan.

Una cuestión clave que se ha debatido durante la investigación es si los programas de vigilancia infringen la ley, en particular el Derecho internacional y el Convenio Europeo de Derechos Humanos. Aunque obviamente solo los tribunales pueden responder a esta pregunta de forma definitiva, se ha declarado con firmeza que efectivamente nos encontramos en una situación en la que se han violado los derechos humanos y el Estado de Derecho.

3.1 La protección de la esfera privada por el Derecho internacional

En lo que respecta al Derecho internacional, se presentaron testimonios durante la investigación que concluyen que los Estados Unidos han incumplido su obligación de prohibir la injerencia arbitraria o ilegal en la vida privada de alguien o su correspondencia con arreglo al artículo 17 del Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos (PIDCP), ya que no cumplen los límites permisibles[1].

A este respecto, la investigación espera la evaluación del Comité de Derechos Humanos con respecto al cumplimiento del artículo 17 del PIDCP por parte de los Estados Unidos y pide que este Pacto se actualice para abordar los problemas de transparencia y proporcionalidad que han planteado las prácticas de vigilancia masiva, ya sea mediante una Observación general que introduzca una evaluación rigurosa de las limitaciones permisibles al derecho a la intimidad (incluida la protección de datos) o un nuevo protocolo adicional o que modifique el Pacto actual.

Todos los Estados miembros de la UE del PIDCP también están incluidos por lo que respecta a sus propias actividades de vigilancia independientemente de si su objetivo son sus propios ciudadanos o los de otros Estados miembros. En cuanto a la colaboración de las autoridades de los Estados miembros en los programas de vigilancia dirigidos por la NSA, el Comité de Derechos Humanos declara en su Observación general que «los propios Estados Partes tienen el deber de abstenerse de injerencias incompatibles con el artículo 17 del Pacto», por tanto, tal colaboración también es ilegal de conformidad con el PIDCP.

3.2 La protección de la esfera privada por el Convenio Europeo de Derechos Humanos (CEDH)

El Tribunal Europeo de Derechos Humanos (TEDH) ha resuelto de forma coherente que las agencias de seguridad nacional y de inteligencia están obligadas a respetar los derechos y libertades contemplados en el CEDH. No solo esto, sino que los Estados miembros tienen la

[1] Véase el testimonio del profesor Martin Scheinin (IUE), antiguo ponente especial de las Naciones Unidas sobre los derechos humanos y lucha contra el terrorismo y de Douwe Korff, profesor de Derecho Internacional en la Universidad Metropolitana de Londres (Reino Unido), en la Comisión LIBE sobre la vigilancia electrónica a gran escala de ciudadanos de la UE el 14/10/2013

obligación positiva de proteger a sus ciudadanos de la vigilancia ejercida por terceras partes, ya sean Estados o entidades privadas[1].

Considerando el alcance de la recopilación masiva de datos personales efectuada a través de los programas de vigilancia, existen serias preocupaciones con respecto a si estas actividades respetan el derecho de los ciudadanos de la UE a la vida privada y a la intimidad y en sus comunicaciones conforme al CEDH[2]. Aunque el derecho a la intimidad no es absoluto, esto no implica una suspensión automática por motivos de seguridad nacional. Según el TEDH, la mera existencia de legislación que permita que un sistema controle de forma secreta las comunicaciones supone una amenaza de vigilancia para todos aquellos a los que se aplique la legislación y, por tanto, puede interferir con el ejercicio de los derechos de las personas en virtud del artículo 8, independientemente de las medidas que se hayan tomado realmente en su contra[3].

Cualquier obstaculización de este derecho por medio de prácticas de vigilancia debería ser prescrita por la ley, limitada, necesaria y proporcional, y someterse a una evaluación continua. Teniendo en cuenta que las tecnologías de telecomunicaciones han evolucionado rápidamente para permitir la recopilación masiva indiscriminada de datos, es imprescindible que los Estados miembros de la UE adopten marcos legislativos precisos que garanticen un control jurídico eficaz a fin de salvaguardar la información privada[4].

Más concretamente, cualquier vigilancia ha de ser «conforme al Derecho». El TEDH ha interpretado este elemento como la accesibilidad de las disposiciones pertinentes y previsibilidad de sus consecuencias. Las normas jurídicas correspondientes definirán siempre las categorías de delitos o las personas que probablemente sean objeto de medidas de vigilancia[5]. Además, tiene que haber límites estrictos con respecto a la duración de toda vigilancia ordenada[6]. Asimismo, la injerencia estará al servicio de un «objetivo legítimo en una sociedad democrática» al tiempo que será «necesaria» y «proporcional» con respecto a ese objetivo. «Necesaria» implica que corresponde a «una necesidad social apremiante»[7] mientras que el término «proporcional» se definirá en referencia al objetivo legítimo que se persigue. En el mismo sentido, hay que establecer las garantías apropiadas para evitar todo abuso de poder[8]. Por consiguiente, la mera utilidad o conveniencia no es justificación suficiente. El TEDH también ha observado en varios casos que, por ejemplo, las normas

[1] Van Hannover contra Alemania, sentencia de 24 de junio de 2004, (2005) 40 TEDH 1; X & Y contra los Países Bajos, sentencia de 26 de marzo de 1985, (1985) 8 TEDH 235; véase también el Manual de Derechos Humanos del Consejo de Europa n.º 7 sobre las obligaciones positivas conforme al Convenio Europeo de Derechos Humanos, por Jean-Francois Akandji-Kombe, disponible en: http://www.coehelp.org/file.php/54/resources/Handbooks/pos_obl_eng.pdf.
[2] Artículo 8 del CEDH.
[3] Weber y Saravia, apartado 78.
[4] Uzun contra Alemania (2012) 54 TEDH 121, sección [61], en Weber contra Alemania (2008) 46 TEDH SE5 sección [93].
[5] Kennedy contra el Reino Unido, sentencia de 18 de mayo de 2010, diligencia n.º 26839/05.
[6] Weber y Saravia contra Alemania, Liberty y otros contra el Reino Unido.
[7] Leander contra Suecia, sentencia de 26 de marzo de 1987, § 48, serie A n.º 116.
[8] TEDH, Kruslin contra Francia, sentencia de 24 de abril de 1990, serie A n.º 176-A y TEDH Huvig contra Francia, sentencia de 24 de abril de 1990, serie A n.º 176-B.

deberían prever que la duración de la interceptación[1] y del almacenamiento de la información[2] sea limitada o, al menos, que se establezcan salvaguardias adecuadas a fin de controlar la discreción de las autoridades que la aprueban en este sentido[3].

3.3 Protección de los datos personales

El marco europeo de protección de datos se encuentra en una lista de principios fundamentales que incluye que: los datos se tratarán de forma leal y lícita; los datos de carácter personal se recogerán con un fin específico y legítimo; los datos de carácter personal serán adecuados, pertinentes y proporcionados al fin o fines para los que se procesen y se deben tomar medidas apropiadas contra el tratamiento no autorizado de datos personales.

Las presuntas prácticas de vigilancia masiva sin justificación específica descritas anteriormente contravienen estos principios fundamentales. La UE y sus Estados miembros tienen la obligación de proteger los datos personales de sus ciudadanos y garantizar que toda transferencia internacional de datos respete estos principios fundamentales.

3.4 El derecho a un recurso efectivo

Un recurso efectivo es un derecho fundamental de conformidad con la Carta y el Convenio Europeo de Derechos Humanos concedido a todas las personas con independencia de su nacionalidad y que también se aplica a los casos en los que se ha violado el derecho a la protección de los datos. El Tribunal de Justicia europeo también ha establecido como principio básico que se debe disponer de recursos en todos los casos en los que se haya infringido el Derecho europeo. Todas estas salvaguardias europeas contrastan directamente con el marco jurídico de los Estados Unidos que recíprocamente niega a los ciudadanos europeos que no residen en los Estados Unidos el derecho a un recurso efectivo.

Si los ciudadanos europeos son objeto de vigilancia por cualquier razón legítima, han de tener derecho a recusar la información de las autoridades de inteligencia. En vista de la transferencia internacional masiva de datos de ciudadanos europeos a las autoridades estadounidenses, la falta de un mecanismo de recurso apropiado para los ciudadanos europeos es un problema extremadamente preocupante. Los Estados Unidos, como paso hacia la reciprocidad, tienen que estudiar los mecanismos más adecuados para extender por lo menos la protección jurídica garantizada a las personas que residen en los EE. UU. a los ciudadanos europeos que están fuera de los EE. UU., con el fin de proporcionar un mecanismo de recurso jurídico efectivo a los ciudadanos europeos cuyos datos han sido guardados o consultados por las autoridades estadounidenses.

3.5 La protección contra la discriminación de ciudadanos europeos

[1] TEDH, Kruslin contra Francia, sentencia de 24 de abril de 1990, serie A n.º 176-A y TEDH Huvig contra Francia, sentencia de 24 de abril de 1990, serie A n.º 176-B.
[2] TEDH, Rotaru contra Rumania, sentencia de 4 de mayo de 2000, diligencia n.º 28431/95, TEDH Amann contra Suiza, sentencia de 16 de febrero de 2000, diligencia n.º 27798/95.
[3] TEDH, Kennedy contra el Reino Unido, sentencia de 18 de mayo de 2010, diligencia n.º 26839/05.

La reciprocidad es una característica esencial de las relaciones internacionales y algo de lo que ha carecido fundamentalmente la relación entre la UE y los Estados Unidos. Mientras que la protección jurídica de los Estados Unidos con respecto a los datos de las comunicaciones se aplica solo a los ciudadanos estadounidenses y residentes, en la UE se protegen como derechos fundamentales los datos personales y la confidencialidad de las comunicaciones de todo el mundo con independencia de su nacionalidad.

Según el marco jurídico de los Estados Unidos, las disposiciones de la primera y cuarta enmienda no protegen a los ciudadanos europeos y parece que los requisitos de pertinencia son muy bajos en el caso de las actividades de vigilancia estadounidenses dirigidas a ciudadanos europeos. Por ejemplo, en virtud del artículo 702 de la Ley FISA, no parece que se requiera una causa probable para convertir a ciudadanos extranjeros en objetivos ya que los principios de selección y minimización no se aplican en el caso de personas no estadounidenses.

Los ciudadanos europeos no tienen derecho a ser informados ni pueden recusar las actividades de vigilancia efectuadas por las autoridades estadounidenses de forma alguna pese al principio de no discriminación y de igualdad ante la ley, contemplado en el artículo 26 del PIDCP.

3.6 Programas de vigilancia y su compatibilidad con la presunción de inocencia

La práctica de vigilancia masiva indiscriminada y la recopilación de datos en bloque de ciudadanos europeos puede como mínimo poner en riesgo el cumplimiento del principio fundamental de la justicia —sobre todo en procedimientos penales— de «presunción de inocencia», que de nuevo incluye a todas las personas con independencia de su nacionalidad[1].

El papel de la vigilancia masiva conlleva un cambio en el Derecho penal desde su función de sancionar actos específicos sobre la base de la responsabilidad personal hasta la de reducir riesgos e identificar posibles infractores, lo que puede llevar a que todos los ciudadanos bajo vigilancia constante sean considerados sospechosos.

3.7 Libertad de expresión: repercusiones para el periodismo y los denunciantes

Existe un consenso con respecto a la necesidad de transparencia y de un debate fundado sobre el alcance de las actividades de vigilancia masiva y su repercusión sobre la intimidad. Un debate así solo es posible si se respeta la libertad de los medios de comunicación. Cuando los mecanismos de supervisión no impiden o rectifican la vigilancia masiva, el papel de los medios de comunicación y de los denunciantes a la hora de revelar las posibles ilegalidades o abusos de poder, sobre todo cuando estas infringen los derechos fundamentales de los ciudadanos, es especialmente importante.

[1] La presunción de inocencia se considera un principio fundamental del Derecho penal y se reconoce tanto en el CEDH como en la Carta de Derechos Fundamentales de la Unión Europea.

Durante la investigación, la Comisión LIBE ha escuchado varias declaraciones de periodistas, denunciantes y de la sociedad civil sobre la necesidad de que se proteja enérgicamente la libertad de información y de los medios de comunicación con respecto a un tema delicado como las actividades de inteligencia. Además, el editor de The Guardian, Alan Rusbridger, declaró que las reacciones de los Estados Unidos y del Reino Unido ante las revelaciones de Edward Snowden han tenido un efecto amedrentador sobre el periodismo e instó al Parlamento Europeo a que hiciese más por proteger a los medios de comunicación.

La libertad de expresión y de información, incluida la libertad de los medios de comunicación, están protegidas tanto por la Carta de Derechos Fundamentales de la UE (artículo 11) como por el CEDH (artículo 10). Estas libertades están avaladas por los últimos informes del Parlamento Europeo[1], la jurisprudencia del TEDH, la Asamblea Parlamentaria del Consejo de Europa y varios textos de las Naciones Unidas que requieren que los Estados miembros protejan la libertad de expresión y que solo se permitan injerencias con arreglo a condiciones restrictivas similares a las aplicadas en materia de intimidad, incluido en el ámbito de la vigilancia. Los periodistas también han de estar protegidos de las tácticas de intimidación para garantizar la libertad de prensa.

A lo largo de la investigación se hizo evidente que los denunciantes desempeñan un papel crucial en la revelación de violaciones graves de los derechos fundamentales y como resultado son extremadamente vulnerables a las represalias. El TEDH ha defendido los derechos de los denunciantes en las mismas condiciones que las que regulan la protección de la libertad de expresión, con fallos en contra de las injerencias del Estado o su empleador[2]. El Tribunal también ha confirmado la importancia del papel que desempeñan los denunciantes y la necesidad de protegerles de los despidos y del efecto amedrentador asociado[3].

El derecho de los denunciantes a la libertad de expresión también ha sido avalado por otras iniciativas recientes del Consejo de Europa[4], la Asamblea Parlamentaria[5], el Parlamento Europeo[6] y la sociedad civil, incluida la organización Transparency International[7] que aboga por una mayor protección de los denunciantes. Aunque la Comisión Europea ha adoptado disposiciones sectoriales relativas a la denuncia de irregularidades, es evidente que se podría concebir un planteamiento más completo a nivel europeo.

---

[1] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0203+0+DOC+XML+V0//EN

[2] Véase por ejemplo, Heinisch contra Alemania, diligencia n.º 28274/08, TEDH (2001)

[3] Guja contra Moldavia, diligencia n.º 14277/04, sentencia de 12 de febrero de 2008.

[4] http://www.coe.int/t/DGHL/STANDARDSETTING/CDcj/Whistleblowers/CDCJ%20(2012)9E_Final.pdf

[5] http://assembly.coe.int/main.asp?link=/documents/adoptedtext/ta10/eres1729.htm

[6] Resolución del Parlamento Europeo, de 23 de octubre de 2013, sobre la delincuencia organizada, la corrupción y el blanqueo de dinero: recomendaciones sobre las acciones o iniciativas que han de llevarse a cabo (informe definitivo) (2013/2107(INI))

[7] Transparency International, «Whistleblowing in Europe, Legal protections for whistleblowers in the EU», 2013 http://www.transparency.org/whatwedo/pub/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu