VIGILANCIA MASIVA
Conflicto entre seguridad nacional, derecho a la protección de datos personales y vida privada

MASS SURVEILLANCE
Conflict between national security, right to data protection and private life

VIGILÂNCIA MASIVA
Conflito entre segurança nacional, direito a proteção de dados pessoais e vida privada

*Pablo Espinosa**

Recibido: 15/05/2020
Aprobado: 20/06/2020

Resumen

La revolución tecnológica ha generado profundos cambios sociales y ha convertido a los datos en materia prima de herramientas para incontables fines. Los programas de vigilancia masiva permiten la captura indiscriminada de enormes cantidades de datos, razón por la cual, su uso con fines de investigación y prevención criminal es cada vez mayor en todo el mundo. Estas actividades constituyen una injerencia en la vida privada y en los derechos de las personas. En este artículo, se analizan las garantías para que dicha intromisión sea legítima y justificada, así como la ponderación entre vida privada, protección de datos y seguridad nacional.

Palabras clave: Derecho a la vida privada; Programas vigilancia masiva; Big Brother; Big data; Defensa Nacional

Summary

Technological revolution has brought deep social changes and has turned data into a tool with countless uses. Mass surveillance programs allow the indiscriminate capture of enormous amounts of data. Therefore, the use of this data for criminal investigation and prevention purposes has globally expanded. These activities are a violation of people's private life and rights. This article analyzes the guarantees for such interference to be legitimate and justified as well as the balance among private life, data protection and national security.

Key words: Right to privacy; Mass surveillance programs; Big Brother; Big data; Homeland Defense

Resumo

A revolução tecnológica gerou profundas mudanças sociais convertendo os dados em matéria prima como ferramentas para incontáveis fins. Os programas de vigilância massivas permitem a captura indiscriminada de enormes quantidades de dados, razão porque, seu uso com fins de pesquisa e prevenção criminal é cada vez maior em todo o mundo. Estas atividades constituem uma ingerência na vida privada e nos direitos das pessoas. Nesse artigo, se analisam as garantias para que esta intromissão seja legítima e justificada; assim como a ponderação entre a vida privada, proteção de dados e segurança nacional.

Palavras chave: Direito à vida privada; Programas vigilância massiva; Big Brother; Big data; Defesa Nacional

* Máster en Justicia Criminal por la Universidad Carlos III de Madrid. LL.M. Máster en Derecho con Especialización en Litigación Oral por California Western School of Law. Experto en Derecho y Compliance TIC, por la Universidad Camilo José Cela. Doctorando Investigador en el Programa de Derecho Penal y Nuevas Tecnologías, de la Universidad Carlos III de Madrid. Correo electrónico: pabloespinosap@outlook.com

INTRODUCCIÓN

Desde fines de los años 90 del siglo XX hasta el día de hoy, vivimos en una sociedad inmersa en una revolución digital de las tecnologías de la información y las comunicaciones (TIC), con las que se crea una base para el libre flujo de información, ideas y conocimientos en todo el planeta. En esta sociedad, conocida como Sociedad de la Información, la información pasa a convertirse en el factor decisivo de la organización económica, como consecuencia de la nueva tecnología digital, y genera cambios profundos en todos los ámbitos de la vida: culturales, políticos y sociales; sobre todo, aquellos determinados por la transformación de las condiciones en las interacciones entre los miembros la sociedad.

No es novedad que el vivir en la época de las nuevas tecnologías, en los años dorados del internet y la conectividad, nos ha llevado a estar abocados a vivir rodeados de información. Hoy en día facilitamos nuestra información casi en todo momento, entregamos datos cuando mantenemos una conversación con alguien mediante teléfono o mediante alguna aplicación de mensajería, lo hacemos al compartir publicaciones en las redes sociales; también cuando queremos adquirir algún producto o servicio en línea, y, en esos casos, no dudamos en facilitar nuestros datos bancarios y nuestros datos de domicilio, para que el bien deseado llegue a nuestras manos.

Pero este punto no es lo realmente relevante, pues el transferir nuestros datos es una acción que no podemos más que realizar, sin lo cual nos mantendríamos en una especie de aislamiento informacional. La cuestión es: ¿cuál es el tratamiento que se hace con esos datos? y ¿para qué fines las empresas privadas requieren esta información de nosotros? A partir de estas preguntas entra en juego el concepto de vigilancia masiva, en base al cual nos damos cuenta de que los datos que aportamos sirven para algo más que para simples fines comerciales.

En este contexto nacen los sistemas masivos de datos (*Big Data*), sistemas capaces de recoger, almacenar y tratar grandes cantidades de datos procedentes del entorno de las personas. El poder sobre la información que confieren estos nuevos sistemas ha sido el causante de que grandes empresas privadas, así como instituciones públicas, entre las que se encuentran las agencias de inteligencia de los Estados, los hayan situado en el centro de su inversión. Como consecuencia, se han creado centros de datos, en los que, según el tipo de entidad que los dirija, el uso de los datos obtenidos y analizados se puede destinar, entre otros, a fines u objetivos culturales, administrativos, o, como nos interesa aquí, para la investigación y la defensa estatal.

Y es que en un contexto social donde está presente la amenaza del terrorismo y la criminalidad, tanto nacional como internacional, en la práctica, la totalidad de los países del mundo y las agencias de inteligencia de los grandes Estados han aprovechado las ventajas que ofrecen estos sistemas de tratamiento masivo de datos para desarrollar los llamados "programas de vigilancia masiva" (PVM en adelante), sobre los que hablaremos más adelante y cuyo propósito inicial es la defensa de la seguridad nacional. No obstante, dado el secretismo y la escasa información que existe sobre ellos, así como la insuficiente regulación establecida a nivel nacional, estos programas entrañan numerosos riesgos para los derechos más elementales de los ciudadanos.

Por vigilancia masiva debemos entender aquella red de vigilancia que se ejerce sobre una importante parte de la población. Puede ser llevada a cabo por Estados, empresas privadas u organizaciones no gubernamentales, aunque el Estado suele ser el principal responsable. Las empresas, en ocasiones, desarrollan la vigilancia en nombre del Estado, aunque también pueden hacerlo por iniciativa propia. De acuerdo a las leyes de cada nación y sus sistemas judiciales, la legalidad, alcance y el tipo de vigilancia masiva varía. Puesto que existen muchos tipos de vigilancia, desde la que se da a conversaciones telefónicas, pasando por las imágenes que pueden ser captadas por un circuito cerrado o la utilización de los datos que hemos facilitado a una empresa, hasta las muy novedosas

aplicaciones de rastreo que incluso se pretenden normalizar por la actual pandemia ocasionada por la Covid-19. La utilización de esta información puede suponer un choque contra el derecho a la privacidad, intimidad, derecho a la protección de datos y al secreto de las comunicaciones.

Las preguntas más importantes son: ¿cómo afecta esta práctica a nuestra vida? y ¿estamos realmente sufriendo una violación del derecho a la vida privada al facilitar información? Hemos empezado a ser realmente conscientes, tanto la sociedad como los órganos jurisdiccionales, de la posible vulneración de nuestros derechos y de que estábamos siendo más vigilados de lo que pensábamos. A partir de las filtraciones de Edward Snowden, los tribunales han empezado a pronunciarse, aunque no siempre en el sentido que se podría intuir o en aquel que valoraba más el derecho a la intimidad que las posibles acciones terroristas. También se han llegado a desarrollar normativas completas (tratados, acuerdos y protocolos) en relación a la transmisión de informaciones entre países, o de empresas a gobiernos; como es el caso de los distintos acuerdos en relación al tratamiento de los nombres de pasajeros[1] y del Reglamento General de Protección de Datos (en adelante RGPD), que es una manera de dotar de ciertas garantías y de acabar por introducir la legitimidad de ciertas formas de vigilancia masiva.

VIGILANCIA MASIVA

1- Origen de la vigilancia masiva

El uso de tecnología para recopilar información no es reciente. La agencia de inteligencia de Reino Unido, en la II Guerra Mundial, se valió de Alan Turing y su equipo de capacidad innovadora informática para descifrar los códigos encriptados de los alemanes (Oppenheimer 2013). De modo que el uso de la tecnología como medio de vigilancia y espionaje, se podría rastrear desde su creación y uso en objetivos militares.

Los inicios de la vigilancia a gran escala se pueden remontar a los años 40, con la suscripción del Acuerdo entre Estados Unidos y Reino Unido, llamado UKUSA, que se firmó entre estos dos países en 1946. Esta alianza entre agencias de seguridad e inteligencia estadounidenses y británicas, se amplió en los años siguientes incorporando otros países, en especial Australia, Canadá y Nueva Zelanda, países con los cuales se formó lo que se denominó el *Five eyes*, grupo que duró más de 70 años en la confidencialidad y que llevó a cabo vigilancia de índole militar y diplomática en el marco de la guerra fría. Cada uno de sus Estados integrantes realizaba actividades de interceptación, colección, análisis y descifrado en su respectiva jurisdicción geográfica y luego la compartía con los demás. También se estableció en el acuerdo un centro de operaciones donde se reunirían los operativos de las agencias de inteligencia (González Porras 2015).

La Agencia Nacional de Seguridad estadounidense (en adelante NSA, por sus siglas en inglés) fue creada en 1952 por el presidente Harry Truman, teniendo como precedente la *Black Chamber*, que operó de 1919 a 1929. En 1960, el *Federal Bureau of Investigation* (FBI, por sus siglas en inglés), bajo el mandato de J. Edgar Hooveer, se dedicó a la recolección de información privada de dirigentes sindicales, políticos y activistas, por medio de escuchas telefónicas. A raíz del escándalo conocido como *Watergate,* se condujo una investigación por parte del Senado de los Estados Unidos, en la cual se llegó a la conclusión de que las agencias de inteligencia habían vulnerado los derechos constitucionales de los ciudadanos norteamericanos. Pero recién en 1978, después que se revelara esta conclusión, se creó la Ley de Vigilancia Extranjera, por la que se organizó un tribunal para administrar solicitudes de vigilancia, especialmente de vigilancia interna hacia extranjeros.

1 Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

2. Vigilancia masiva en la actualidad

Después del trágico atentado terrorista del 11 de septiembre de 2001, el Consejo de Seguridad de la ONU señaló que estos ataques son una amenaza para la paz y seguridad globales y adoptó la Resolución 1373 (2001), que motivaba a los Estados a tomar parte de la lucha contra el terrorismo con medidas para la prevención de comisión de actos terroristas, y les daba libertad para realizar operaciones subrepticias, que han originado vulneraciones a garantías fundamentales (Serra Cristóbal 2015).

Muchos Estados aprobaron leyes con la finalidad de legitimar estas intervenciones, como Reino Unido, que aprobó la ley antiterrorista en 2001, y Estados Unidos, que aprobó la Ley Patriota, que trajo muchas dudas sobre la constitucionalidad del uso excesivo de medidas adoptadas para la prevención de ataques. Muchos otros países crearon programas antiterroristas y permitieron el uso de espacios aéreos para el traslado y entrega de terroristas capturados a Estados Unidos.

Uno de los escándalos más recientes que atrajo la atención de la prensa y de la sociedad en general hacia la vigilancia masiva, fue la revelación de información por Edward Snowden. Este ex agente de la NSA hizo revelaciones al diario *The Guardian*, que publicó la primera de las denuncias sobre la recolección de información de usuarios de la compañía americana de telefonía celular Verizon por parte de la NSA (Greenwald 2013).

Estas noticias fueron polémicas y tuvieron relevancia de carácter global. Snowden empezó a ser perseguido por el gobierno estadounidense y se emitió una orden de extradición en su contra. Él fundamentó sus denuncias en documentos que extrajo de la NSA de manera clandestina, y se convirtió en fugitivo internacional. El gobierno de los Estados Unidos justificó su accionar por considerarlo necesario para proteger la vida de los ciudadanos, y con sustento en la *Protect America Act* (PAA) (González Porras 2015). Se puede decir que estas revelaciones abrieron los ojos de la sociedad en lo relativo al poder de la vigilancia masiva en internet y por medio de la tecnología en general, ya que se iniciaron litigios internacionales y demandas contra el gobierno estadounidense y el gobierno británico.

3. Principales programas de vigilancia masiva

Una de las principales características de estos programas es su confidencialidad estricta, lo que dificulta que se tenga información sobre el alcance real de estos programas. Así, lo poco que se conoce hasta el momento es la información que se ha logrado filtrar.

La información filtrada por Edward Snowden en sus entrevistas a los periódicos *The Guardian* y *The Washington Post*, mostraba el programa que utiliza la NSA desde el 2007 para esta vigilancia. Este programa de la NSA, llamado en clave PRISM, fue legalizado en los Estados Unidos a través de la Ley de Servicios de Inteligencia Extranjera (*Foreign Intelligence Service Act*, FISA), y es capaz, según las diapositivas de la NSA filtradas, de acceder e interceptar información de los *Data Centers* de empresas tan conocidas como Google, Microsoft, Facebook, Skype o Apple. Concretamente, es capaz de interceptar correos electrónicos, videos, fotos, chats (de video y voz), transferencias de archivos, notificaciones de actividad (cuando se ha conectado o desconectado una persona) y detalles de las redes sociales de los usuarios (Gonzáles Monje 2017). Y existen indicios claros de que el *Government Communications Headquarters* (GCHQ, por su siglas en inglés) de Reino Unido, tuvo acceso a este programa desde el año 2010.

Menos conocido, pero igual de intrusivo, es el PVM, conocido como XKeyScore (Mejías Alonso 2018), también de la NSA, que es mucho más complejo que el PRISM. El PVM es capaz no solo de interceptar y recolectar datos como lo hace el PRISM, sino también de almacenar información proveniente de otros sistemas y programas, con usos varios como: espionaje de diplomáticos y líderes políticos extranjeros; interceptación de datos de satélites y datos procedentes de servicios de telecomunicaciones, como Vodafone. Este programa permite, además de acceder al contenido de los correos electrónicos, leer el contenido íntegro de todos los mensajes y chats de Facebook. Para lograrlo,

el agente solo necesita introducir el nombre del usuario objetivo y un intervalo de fechas.

Por otro lado, el GCHQ británico controla el PVM TEMPORA, una versión mejorada del XkeyScore, capaz de nutrirse de toda la información que pasa a través de fibra óptica en diferentes países y en todo el tráfico telefónico. Tiene las mismas funcionalidades (grabaciones de llamadas, contenido de correos electrónicos, chats de Facebook, historial de acceso a páginas web de cualquier usuario) que los anteriores programas, pero a mayor nivel. Este programa no discrimina objetivos, es decir que almacena información de usuarios sin ningún fundamento de sospecha previo, y se ejecuta sin la necesidad de que se imponga alguna orden o permiso gubernamental (Gonzáles Porras 2015). La ley que autoriza la utilización de estos programas en Reino Unido es la *Regulation of Investigatory Powers Act 2000*.

No se puede dejar de mencionar a ECHELON. Este PVM es considerado por algunos expertos como la mayor red de espionaje de la historia de PVM. Cuerda Arnau describe su funcionamiento:

> "En sus numerosas estaciones de interceptación captura las conversaciones y, después, cada estación selecciona dicha información pasada por el tamiz de lo que podría denominarse «diccionarios de palabras clave» (sospechosas o peligrosas) diseñados por los Estados en función de los concretos intereses que cada uno pueda tener en ese particular momento. Posteriormente, la referida información o bien se transcribe y registra o bien se elimina, que es, al parecer, lo que sucede con la mayoría ante las dificultades para hacer frente a su almacenamiento y procesamiento" (Cuerda Arnau 2013,109).

4. Vulneración a los derechos fundamentales

Al respecto de este sistema, el Parlamento Europeo ya realizó un informe redactado por una Comisión temporal[2] que fue creada para investigarlo. El informe señaló que sólo se permitirían intervenciones de espionaje en los casos en que estuviere en peligro la seguridad nacional, y siempre y cuando esta injerencia a la privacidad se halle prevista en el derecho interno del país, sea accesible su conocimiento a todas las personas y se indique claramente en qué circunstancias se realizaría. Estas operaciones deben ser equilibradas, razón por lo que la cual se debe establecer una simetría con los derechos en juego, de acuerdo a la jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante TEDH). Estas medidas no sólo deben ser necesarias, sino también estar legitimadas y ser compatibles con los derechos fundamentales, de modo que deben observarse con medios de control estatales previamente designados (González Monje 2017).

Una vez revisada esta información parcial sobre el alcance de estos programas, parece lógico que el "Informe Moraes", de la Unión Europea (en adelante UE), haya determinado que estos programas son una vulneración sistemática de los derechos fundamentales de todos los ciudadanos, y que no es posible garantizar, ni a las instituciones públicas de la UE, ni a sus ciudadanos, que su seguridad o intimidad informática puedan ser protegidas de los ataques de intrusos bien equipados. Además, pone en entredicho que los fines de estas operaciones de vigilancia masiva respondan únicamente al fin de la lucha contra el terrorismo y la defensa de la seguridad nacional, y les llega a atribuir otros fines como el "espionaje político y económico", o la elaboración de perfiles de ciudadanos, a quienes trata como potenciales sospechosos[3]. En consecuencia, este informe concluye con la petición a las autoridades de los Estados Unidos y a los Estados miembros de la UE, que decidan la prohibición inmediata de las actividades de vigilancia masiva generalizada.

La amplia gama de programas documentada por diferentes Estados, y con diferentes propósitos, que abarcan desde espionaje de actividad en línea en tiempo real hasta descifrado de claves de transacciones bancarias,

2 *Informe Moraes* de 21-II-2014. En: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7- 2014-0139+0+DOC+XML+V0//ES

3 En este sentido, este informe señala en su conclusión 12ª, que estos programas "constituyen un paso más hacia el establecimiento de un estado preventivo de pleno derecho".

es muy preocupante, ya que nos muestra la dimensión a la que han llegado los Estados partícipes en el uso de estos programas. Esta vigilancia debe ser vista como una injerencia altamente intrusiva a la privacidad, que revela la tendencia al aumento de redes y programas de vigilancia masiva, incluso más allá de las fronteras de los países, en gran parte debido a los acuerdos que realizan los Estados, en los que se benefician mutuamente por la información recolectada unos de otros.

Se cree que es imposible que cualquier agencia pueda ser capaz de leer y analizar toda la información, correos electrónicos, metadatos y llamadas que colectan con su actividad a lo largo del mundo. Pero, sin duda provocan en la sociedad una sensación de vigilancia extrema, que causa que las personas se sientan todo el tiempo controladas, para así asegurar la reducción en el cometimiento de delitos y actos terroristas. Aunque este proceder puede ser muy efectivo para aumentar el cumplimiento de la ley o prevenir actos terroristas, es una vulneración grave a las garantías fundamentales de una sociedad democrática.

5. Derecho a la protección de datos personales y vigilancia masiva

El primer gran desafío en cuanto a tratamiento de datos personales, por su dimensión y primicia, ocurrió en 1935. Cuando el presidente norteamericano Franklin D. Roosevelt aprobó la Ley de Seguridad Social (en inglés, *Social Security Act*), con el objetivo de alcanzar los beneficios propios del Estado del bienestar, mediante el tratamiento de datos. Mediante esta ley se procuraba la actualización de los datos personales que concernían a la clase trabajadora, por ejemplo, en materia de pensiones.

El TEDH ha manifestado que la protección de los datos personales está dentro del ámbito de aplicación del artículo 8 de la Convención Europea de Derechos Humanos (en adelante, CEDH). En el Caso S. y Marper contra Reino Unido, señala que el simple acto de memorizar datos de la vida privada de una persona es una injerencia al artículo 8 del convenio, se utilice o no esta información en un futuro. También resalta que, para determinar si la información de carácter personal conservada por las autoridades hace que entre en juego algún aspecto de la vida privada, el Tribunal tendrá debidamente en cuenta el contexto particular en el que ha sido recogida y conservada la información, el carácter de los datos consignados, la manera en la que son utilizados y tratados, así como los resultados que pueden extraerse de ellos[4].

El Tribunal indica que información como huellas dactilares y ADN son datos personales, ya que se refieren a personas identificables. También considera como injerencia la conservación de datos relativos a la vida personal de un individuo por parte de una autoridad, así sea con motivos de seguridad nacional. De la misma forma, se entienden como datos personales: la compilación o análisis de datos médicos, llamadas telefónicas, localización por GPS, movimientos de tren y avión en bases de datos policiales, y antecedentes de un individuo (Salamanca Aguado 2014).

El derecho a la protección de datos personales está reconocido también en la Constitución ecuatoriana, en el artículo 66 numeral 19, en el que se reconoce y garantiza a las personas este derecho. Sin embargo, hasta el día de hoy no se ha logrado trasponer este mandato constitucional en legislación sobre este ámbito, siendo hasta el momento el intento más prometedor el Proyecto de Ley Orgánica de Protección de Datos Personales, presentado el 19 de septiembre de 2019. Este proyecto de ley lleva una clara y acertada inspiración en el RGPD europeo, que hasta ahora es la más vanguardista legislación a nivel mundial en protección de datos personales.

La gran concreción a nivel normativo y práctico del derecho de protección de datos personales, se materializa en el Reglamento General de Protección de Datos 679/ 2016 de la Unión Europea. Éste tiene como finalidad establecer un nivel coherente de protección de los datos de las personas físicas en toda la UE, así como proporcionar seguridad jurídica y transparencia a los operadores económicos. Se atribuye la titularidad del derecho únicamente a las personas físicas, independientemente de su nacionalidad o lugar de residencia.

4 Sentencia TEDH de 4-XII-2008, S. y Marper c. UK. Sentencia de 4-XII-2008, apartados (en adelante, *apdo*.) 67-69.

Se define como dato personal en el RGPD, art. 4.1:

> "toda información sobre una persona física identificada o identificable; se considerará persona identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular un identificador, como por ej. un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

De esta manera, la información recolectada por los PVM está plenamente considerada como datos personales. Una aportación muy valiosa que hace el RGPD es la concreción de los principios relativos al tratamiento de datos, los cuales son transversales a todo manejo de datos personales. Los datos deberán ser tratados de manera lícita, leal y transparente en relación con el interesado (principio de licitud, lealtad y transparencia); serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (principio de limitación de la finalidad); deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (principio de minimización de datos). También deberán ser exactos y actualizados (principio de exactitud); mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (principio de limitación del plazo de conservación); tratados de tal manera que se garantice una seguridad adecuada de los datos personales (principio de integridad y confidencialidad); y el responsable y encargado del tratamiento serán responsables del tratamiento y capaces de demostrarlo (principio de responsabilidad proactiva)[5].

Estos principios deberán ser mandatorios en todo tipo de tratamiento de datos, como confirma la Directiva (UE) 2016/680, de protección de las personas en cuanto al tratamiento de sus datos personales por las autoridades policiales y de justicia penal, y a la libre circulación de estos datos. Esta es la normativa legal que se aplicaría en los PVM, que señala los principios concretados por el RGPD, como obligatorios en el tratamiento de datos con fines de investigación criminal.

El *Big Data* es uno de los métodos mediante los cuales los PMV recopilan información y la analizan. Lamentablemente, el RGPD, más que proporcionar soluciones específicas para abordar los problemas planteados por el nuevo paradigma de gestión de la información, sólo es un punto de partida para una reflexión más amplia (Mantelero 2017). El marco regulador de la Unión Europea, a partir de las primeras leyes sobre protección de datos, se basa en el presupuesto según el cual las personas son capaces de conocer los métodos y los fines del tratamiento y de entenderlos en términos de posibles consecuencias. Sin embargo, en el contexto del *Big data*, la complejidad del tratamiento agrava los límites ya conocidos a la autodeterminación real de la persona. Así mismo, existen dificultades en la aplicación de los principios de minimización y de finalidad del tratamiento.

Los programas de vigilancia masiva claramente realizarían un tratamiento de datos personales. Por este motivo, y a primera vista, se pensaba que el RGPD sería un freno al uso de estos programas. Pero no ha sido así, ya que el reglamento, dentro de su ámbito de aplicación material, excluye el tratamiento por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[6].

Así las cosas, nuevamente se ve limitada la protección a derechos como el derecho a la intimidad o a la protección de datos personales, sobre la ponderación con otros como la seguridad nacional; por lo tanto, es pertinente revisar el choque, justificación y legitimación a nivel internacional de esta limitación.

5 Para más información sobre el Reglamento Europeo General de Protección de Datos, ver: Rebollo Delgado L. y M. Serrano Pérez. 2019. *Manual de Protección de Datos*. Madrid: Dykinson.

6 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27-IV-2016 relativo a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos, artículo 2.2.

EL DERECHO A LA VIDA PRIVADA FRENTE A LA DEFENSA DE LA SEGURIDAD NACIONAL

1. Derecho a la vida privada

El derecho a la vida privada se halla regulado en el artículo 12 de la Declaración Universal de Derechos Humanos, el cual establece que: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Este derecho está reconocido también en instrumentos internacionales regionales que Ecuador ha adoptado, como la Declaración Americana de los Derechos y Deberes del hombre de 1948 y la Convención Americana sobre Derechos Humanos de 1969, donde se señala el derecho de las personas a la protección de una vida privada sin injerencias arbitrarias o abusivas.

La Constitución del Ecuador reconoce y protege el derecho a la intimidad en la vida personal y familiar, así como el derecho a la inviolabilidad y al secreto de la correspondencia física o virtual, en su artículo 66 numerales 20 y 21 respectivamente. En el mismo sentido protector de este derecho, la legislación ecuatoriana tipifica la violación a la intimidad en el art. 178 del Código Orgánico Integral Penal (en adelante COIP), dentro de los delitos contra el derecho a la intimidad personal y familiar. En este precepto se sanciona toda conducta que implique el acceso, difusión o divulgación no consentida de información privada, y se castiga de manera amplia conductas que afecten a la intimidad y privacidad.

En el art. 476 del COIP, dentro de las actuaciones especiales de investigación, se enmarca la interceptación de las comunicaciones o datos informáticos. Hay que señalar que esta diligencia solamente podrá efectuarse previa solicitud de la Fiscalía, después de otorgada la orden judicial, cuando existan indicios relevantes a los fines de la investigación. Su alcance serán las comunicaciones del investigado o procesado y de aquellos con los cuales éste se comunique. Para solicitar la interceptación por parte de un fiscal, debe existir una investigación previa o una instrucción fiscal. Aquí se empiezan a notar las diferencias entre esta diligencia de investigación y los PVM, ya que estos efectúan interceptaciones generales sin previos indicios o investigaciones específicas, no dentro de una instrucción fiscal, sino buscando indicios de delitos que muchas veces aún no se han cometido, como ataques terroristas. Además, su alcance no está limitado a ciertas personas investigadas identificadas, sino que se da una interceptación de telecomunicaciones de carácter amplio, masivo y general.

De igual manera, en los requisitos señalados en el art. 476, se señala el plazo de duración de la interceptación, así como la necesaria autorización judicial correspondiente para la ampliación de esta medida; diferenciándose del secretismo y la falta de especificación temporal de utilización de los PVM.

Por su parte, el CEDH regula en su artículo 8 el derecho al respeto de la vida privada y familiar. Y manifiesta que:

> "no podrá haber injerencia de la autoridad en el ejercicio de este derecho sino en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás" (CEDH, artículo 8, apartado 2).

El TEDH ha interpretado que los términos "vida privada" y "correspondencia" abarcan las comunicaciones por teléfono[7], fax o correo electrónico. Incluye también aquí toda la información derivada del

7 STEDH de 29-VI-2006, Weber y Saravia c. Alemania. Apdo. 77.

seguimiento del uso personal de internet, el almacenamiento en un registro secreto y la comunicación de datos relativos a la vida privada de un individuo (Salamanca Aguado 2014).

Por otro lado, en el apartado 2° vemos que, en cuanto no nos encontremos ante un derecho absoluto, se permiten injerencias o limitaciones sobre este derecho, que aquí se regulan mediante una serie de requisitos con los que cualquier injerencia sobre este derecho quedaría justificada. Estos requisitos son: la previsión por la ley de la injerencia; que dicha injerencia responda a un fin legítimo (por ejemplo, la seguridad nacional); y, por último, que sea necesaria en una sociedad democrática para conseguir tal fin.

2. Gravedad de la injerencia de los PVM sobre el derecho a la vida privada

En cuanto a la gravedad de la injerencia, la podemos medir según dos criterios:

1. La calidad del ámbito material afectado por la intromisión. Donde el cuerpo, el domicilio y las comunicaciones personales conforman una intimidad de calidad máxima. Mientras los datos o información privada del sujeto que más relación guardan con el exterior constituyen una intimidad de calidad mínima.

2. El medio por el cual se accede al conocimiento de los datos o informaciones. Mas, al haber una amplia variedad de medios, la gravedad de la injerencia dependerá del carácter ocasional o permanente de la vigilancia, y de que ella se dirija contra persona determinada o contra un grupo; o que sea visible o se desarrolle subrepticiamente, de suerte que pasa inadvertida para el interesado.

En base a estos dos criterios, podemos determinar que los PVM producen una injerencia en el derecho a la intimidad de los ciudadanos con un grado de lesividad máximo, toda vez que, con estos programas, se puede acceder a datos estrechamente vinculados con el libre desenvolvimiento de la personalidad.

Respecto al argumento de que mucha de la información recopilada por los PVM nunca llegará a ser examinada, debemos traer a colación la Sentencia del Tribunal Europeo de Derechos Humanos (en adelante, STEDH) de 29 de junio de 2006, Weber y Saravia c. Alemania, en cuyo apartado 78º, el tribunal señala que la mera existencia de una legislación que permita un sistema para el monitoreo secreto de las comunicaciones conlleva una amenaza de vigilancia para todos aquellos a quienes se les pueda aplicar tal medida. Esta amenaza necesariamente afecta a la libertad de comunicación entre los usuarios y, por lo tanto, equivale a una injerencia en el ejercicio de los derechos recogidos en el art. 8 de la CEDH. Este fenómeno se encuentra ligado al "efecto panóptico", por el cual un poder es capaz de imponer conductas al conjunto de la población a partir de la idea de que estamos siendo vigilados, de acuerdo con la teoría del panóptico de Michel Foucault[8].

Otro argumento esgrimido por los Estados a la hora de atenuar el grado de injerencia de estos programas de vigilancia en la intimidad de los ciudadanos, es que algunos programas de vigilancia únicamente almacenan metadatos, sobre la información recolectada, y no su contenido propiamente dicho. Al respecto, la European Digital Rights, argumentó ante el TEDH, en el caso Big Brother Watch vs. United Kingdom, que, en la actualidad, los metadatos pueden proporcionar una imagen más detallada e íntima sobre la persona investigada, así como sobre las personas con las que se relaciona, que el propio contenido de la información. En suma, esta agrupación internacional concluye que no se debe otorgar un grado diferente de protección a los datos personales, basados en la distinción irrelevante entre el contenido y los metadatos[9]. Por tanto, los metadatos aportan información más rápida, precisa, fácil de analizar y mucho más operativa sobre cada individuo y su entorno social, especialmente para vigilancias prospectivas y sin destinatario específico (De

8 Para más información sobre el tema, ver en web: https://psicologiaymente.com/social/teoria-panoptico-michel-foucault
9 Apdo. 301º de la STEDH, de 13-IX-2018, Big Brother Watch vs. The United Kingdom.

Prada 2016). Se recalca así el grado máximo de injerencia de los PVM sobre los derechos de las personas.

3. Defensa de la seguridad nacional

No existe un consenso a nivel internacional sobre lo que constituye y abarca el concepto de Seguridad Nacional; debido a factores como la delimitación del término "seguridad", que es extensamente amplio, o la idea de amenaza, que genera la necesidad de seguridad y está en constante evolución. Este concepto respondía, en un principio, a amenazas en términos militares, pero que, con el paso del tiempo, han dado lugar a nuevas formas de amenazas no militarizadas, como pueden ser el ciberterrorismo o los problemas medioambientales. La Seguridad Nacional es una materia de competencia nacional, por lo que la UE no tiene competencia regulatoria alguna sobre ella, sino únicamente en la seguridad interna de la UE[10].

Parece claro que, entre los fines de la Seguridad Nacional, se encuentra la lucha contra el terrorismo, la criminalidad y delincuencia organizada. No obstante, debemos reiterar que uno de los principales aspectos controvertidos y criticados de los PVM es el uso de estos con propósitos distintos a los amparados por la Seguridad Nacional, ya sean fines políticos, económicos, de espionaje de autoridades, o, incluso, un fin delictual, como puede ser la extorsión a personas de interés (grandes empresarios, autoridades).

A la luz del precedente análisis, vemos que la defensa de la seguridad nacional responde a un interés general, el bienestar común de toda una sociedad, un derecho colectivo. Parece pues razonable que éste prevalezca frente a una serie de requisitos asociados al derecho a la intimidad, toda vez que éste responde a un interés individual. Como se desprende del apartado segundo del art. 8 de la CEDH, al señalar a la seguridad nacional como uno de los fines legítimos que justifica la injerencia en este derecho. Pero, en el caso de los PVM, donde su utilización aparentemente produce una violación del derecho a la intimidad de forma sistemática y masiva, no se puede hablar de un interés individual en conflicto con un interés general, sino de un conflicto entre dos intereses generales o colectivos.

No obstante, y pese a dicho enfrentamiento entre estos dos intereses, vemos que la seguridad y la intimidad o privacidad, no son conceptos antagónicos. Desde los Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos, en su cláusula 22º, se dispone que "la violación sistemática de los derechos humanos socaba la seguridad nacional y puede poner peligro la paz y la seguridad internacional". Vemos, por tanto, que la seguridad y el derecho fundamental a la intimidad y privacidad, se encuentran relacionados y son dependientes.

Llegados a este punto, dar una respuesta clara y genérica para este dilema es complicado. Por tal motivo, analizaremos cada uno de los requisitos que deben cumplir los Estados en la aplicación y utilización de los PVM, para que cualquier injerencia de estos sobre el derecho a la vida privada y familiar de los ciudadanos sea lo menos lesiva y pueda justificarse de acuerdo con lo estipulado en la CEDH. En este sentido, nos será de mucha ayuda la reciente STEDH de 13 de septiembre de 2018, Big Brother Watch vs. The United Kingdom, en la que nos apoyaremos más adelante para dar una respuesta a la compatibilización de ambos derechos.

4. Compatibilidad de los programas de vigilancia masiva con el CEDH

En el actual marco constitucional ecuatoriano se resuelve el conflicto entre derechos a partir de la ponderación de derechos, es decir: sopesar los principios que han entrado en colisión en el caso concreto para determinar cuál de ellos tiene un peso mayor en las circunstancias específicas y, por tanto, cuál de ellos determina la solución para el caso concreto. El núcleo de la ponderación consiste en una relación que se denomina ley de la ponderación y que se puede formular así: "Cuando mayor sea el grado de no satisfacción o restricción de uno de los principios, tanto mayor deberá ser el grado de la importancia de

10 Extraído del postulado de la seguridad nacional y la inteligencia del Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU. Informe Moraes", p. 52.

la satisfacción del otro"[11]. Existe una tendencia de la Corte Constitucional ecuatoriana, en sus sentencias, a aplicar el principio de proporcionalidad como criterio para examinar la constitucionalidad de las intervenciones en los derechos fundamentales, y la ponderación como método para la solución de conflictos entre derechos, valores o principios.

Esta se diferencia del TEDH, en que el tribunal europeo concentra, *prima facie,* su valoración en revisar si se ha vulnerado o no algún derecho protegido por el convenio. Sin embargo, el TEDH ha dejado claro en su jurisprudencia que no todos los derechos son absolutos. Por este motivo, utiliza también la ponderación y especialmente la proporcionalidad para verificar si la injerencia en un derecho es apegada a los requisitos señalados por el convenio. Las pruebas de necesidad y proporcionalidad son aplicadas por el TEDH dentro del requisito para legitimar una injerencia, que analizaremos posteriormente, conocido como "medida necesaria en una sociedad democrática".

Como hemos analizado, los PVM son un instrumento de control de la población en general, con un alto grado de injerencia en el derecho a la intimidad de todos los ciudadanos, y, por lo tanto, afectan a un interés colectivo. No obstante, parece razonable que, en situaciones donde la seguridad del Estado se encuentra comprometida, cuando existe peligro para la nación, su territorio o la independencia política, se puedan emplear estos programas como fórmula de defensa y prevención contra todas las amenazas que hemos señalado.

En todo caso, cualquier tipo de excepción que permita la disminución de garantías fundamentales en un Estado, como, en este caso, el acopio de información que consta en el apartado segundo del art. 8 de la CEDH, debe ser informada, de acuerdo de una serie de principios y conforme a la legalidad, a fin de evitar siempre cualquier limitación arbitraria, imprevisible o irrazonable.

De acuerdo con estas premisas, la visión del TEDH sobre los PVM se aleja de la afirmación de que cualquier sistema de interceptación masiva constituye una violación de la CEDH. Esta visión queda reflejada en la STEDH Big Brother Watch vs. United Kingdom, que establece, conforme al apartado segundo del art. 8 de la CEDH, los principios y requisitos a los que se deben someter estos programas, para salvaguardar y respetar los derechos fundamentales garantizados por el convenio. Para que la injerencia ocasionada por los PVM en el derecho a la intimidad del art. 8 de la CEDH quede justificada, deben concurrir los requisitos que se detallan en el siguiente apartado.

REQUISITOS PARA JUSTIFICAR LA INJERENCIA

1. Finalidad u objetivo legítimo

La seguridad nacional es uno de los objetivos legítimos recogidos en el apartado segundo del art. 8 de la CEDH. Al respecto, el tribunal europeo entiende que las autoridades nacionales disfrutan de un amplio margen a la hora de lograr tal objetivo. Señala que los PVM entran dentro de ese margen de apreciación y que constituyen un mecanismo adecuado en la consecución de este objetivo, porque en la actualidad las amenazas que atentan contra la seguridad de los Estados, como el terrorismo, el narcotráfico, la trata de seres humanos o ciertos delitos informáticos, se encuentran agravadas por el desarrollo tecnológico. Esta situación facilita la comisión delictiva dada la amplia variedad de canales y medios de comunicación (alto grado de imprevisibilidad), y, en consecuencia, dificulta su prevención y detención[12].

Esta prerrogativa dada a los Estados a la hora de poder elegir el mecanismo con el cual garantizar este objetivo legítimo, se ve contrarrestado por un mayor

11 Sentencia N°. 002-009-SAN-CC (Caso 0055-089-AN) del 2-IV-2009.
12 En este sentido, ver el apdo. 106 de su STEDH de 29-VI-2006, Weber y Saravia c. Alemania.

número de requisitos que hagan lo suficientemente previsibles estos regímenes de interceptación, de tal forma que se minimice el riesgo de abusos de poder por parte de los Estados.

2. Previsión legal

La previsión legal va a ser fundamental a la hora de que los Estados utilicen los PVM. La utilización de estos programas de interceptación masiva deberá estar regulada en el ordenamiento jurídico del país en una norma con fuerza de ley. Además, dicha ley deberá ser accesible y previsible para las personas interesadas en cuanto a sus efectos.

En cuanto a la previsibilidad, su grado de exigencia en el contexto de los PVM, dada su naturaleza subrepticia, no puede ser el mismo que en otros campos. En este sentido, el TEDH reitera, en esta sentencia, lo dispuesto en el apartado 93 de la STEDH Weber y Saravia c. Alemania; allí señala que la previsibilidad no significa que una persona pueda prever cuándo es probable que las autoridades intercepten sus comunicaciones, para adaptar su comportamiento en consecuencia, sino que para evitar la arbitrariedad y el abuso del Estado, lo esencial es que la legislación nacional sea lo suficientemente clara para dar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en que las autoridades están facultadas para recurrir a tales medidas. A la luz de esta jurisprudencia, el Tribunal reseña los seis requisitos mínimos que debe haber en la ley para la interceptación de comunicaciones en procesos penales, que son también de aplicación para estos programas, para así poder evitar abusos de poder.

En un análisis de la reiterada jurisprudencia sobre la intervención de las comunicaciones individuales, el TEDH ha establecido garantías mínimas que deben estar definidas en la ley, como son: la naturaleza de las infracciones que puedan dar lugar a una orden de interceptación, la especificación de las categorías de personas susceptibles de sufrir vigilancia telefónica judicial, los límites a la duración de la ejecución de la medida, el procedimiento que deberá seguirse para el uso y conservación de los datos obtenidos, las precauciones necesarias para comunicar los datos a otras organizaciones y las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de la información.

Adicionalmente, para los PVM también se tendrán en cuenta los acuerdos para supervisar la aplicación de las medidas de vigilancia secreta, los mecanismos de notificación y los recursos previstos a tal efecto[13].

3. Medida necesaria en una sociedad democrática para lograr el fin legítimo

Por último, la utilización de los PVM, además de responder a un fin legítimo y estar prevista en una ley con las características anteriormente descritas, debe constituir una medida necesaria en una sociedad democrática para lograr tal fin, en este caso la seguridad nacional.

Por tanto, con miras a determinar si se cumple este requisito, se deberá hacer un test de necesidad y otro de proporcionalidad (Salamanca Aguado 2014). Es decir que se deberá establecer que los medios sean necesarios para lograr el fin, y que, de entre las medidas disponibles para dicho fin, la elegida sea la menos perjudicial para el derecho a la intimidad.

En la STEDH Big Brother Watch vs. The United Kingdom, el tribunal, tras analizar una gran cantidad de material e informes, concluyó que la intercepción masiva de información, que incluye los PVM, es necesaria y proporcional en una sociedad democrática, en base a los argumentos que se expondrán a continuación[14].

Dadas las circunstancias sociales actuales, la sociedad se ve gravemente amenazada por terroristas y grupos criminales que cuentan con medios cada vez más sofisticados para llevar a cabo sus fines ilícitos y que escapan al control de los medios de detección tradicionales. Además, como ya se dijo, la utilización

13 Apdo. 308 de la STEDH Big Brother Watch v. The United Kingdom.
14 Información extraída del apdo. 384º de la STEDH Big Brother Watch vs. UK.

de internet proporciona acceso a una amplia variedad de canales de comunicación, de manera que se hace impredecible la ruta de comunicación empleada para preparar los actos delictivos.

No existe otra alternativa o alternativas que logren equipararse al poder y efectividad de intercepción del que se dispone por medio de los PVM, para lograr la preservación de la seguridad nacional.

Aunque se reconocen los riesgos para los derechos individuales de los ciudadanos que entraña la intercepción masiva, se ha reconocido la utilidad de estos programas para las operaciones de seguridad. Dado que permite a los Estados adoptar un enfoque proactivo frente al problema, así como detectar focos de peligro hasta ahora desconocidos.

En cuanto al régimen de intercambio de información entre las agencias de inteligencia, el TEDH entiende que, dada la particular complejidad inherente a las redes terroristas globales, es proporcional y legítimo el intercambio de información entre las agencias. Este permite prevenir la perpetración de actos violentos que ponen en peligro la vida de miles de ciudadanos inocentes. Pero esto es así siempre que lo prevea el legislador nacional y que se cumpla con las garantías en caso de abuso por parte de las autoridades, de forma que este modo de actuar sea plenamente compatible con el art. 8 de la CEDH.

CONCLUSIONES

- La utilización de los programas de vigilancia masiva por las agencias de inteligencia, sumada a la colaboración de las grandes empresas relacionadas con internet (Facebook, Google, Microsoft) y una mala praxis en el uso de las redes por los ciudadanos, nos han llevado a una situación en la que las autoridades pueden tener acceso a prácticamente cualquier información, inclusive datos personales sensibles. Este problema conduce, si no se adoptan las medidas y garantías necesarias, a una vulneración sistemática y masiva de un derecho tan importante para el sostenimiento del Estado de Derecho, como el derecho a la intimidad y a la vida privada de los ciudadanos.

- Ha quedado claro que tal grado de injerencia estaría justificado en aras de garantizar la defensa de la seguridad nacional. Este es, sin duda, uno de los fines de los PVM, y ello adquiere más fuerza en el contexto social actual, en el que todas las naciones del mundo se encuentran bajo amenaza terrorista y bajo el yugo de grandes organizaciones criminales. En este sentido, el desarrollo tecnológico ha facilitado la comisión de estas actividades delictivas, de modo que es necesaria la implementación y utilización de los PVM para prevenirlas y combatirlas, toda vez que los mecanismos de investigación tradicionales han resultado ser ineficaces.

- Nos encontramos en una era completamente digital, en la que el derecho al respeto a la vida privada o a la protección de datos necesitan ser entendidos de una forma completamente distinta y mucho más amplia. Hay que tener en cuenta que las injerencias que se oponen a este derecho pueden venir de otros Estados, y ésta sería posiblemente la forma más grave en la que se puede presentar tal intervención. Aunque parezcan suficientes, es necesario dotar de más garantías a todos los procesos que puedan suponer un medio para la vigilancia masiva, y asegurar que la intromisión que se va a dar en los derechos de una persona siempre será la mínima necesaria y justificada.

- A la luz de la jurisprudencia del TEDH, resulta esencial para la utilización de estos medios, una legislación nacional previsible y clara para los ciudadanos, que les proporcione suficientes garantías en los casos en que haya abusos. Este es el requisito más controvertido, dada la ausencia de una regulación armonizada al respecto. Es necesario que los aparatos legislativos de cada Estado trabajen con especial empeño en este requisito.

- En conclusión, queda un largo camino por recorrer a la hora de compatibilizar el uso de los PVM para

la defensa de la seguridad nacional con una adecuada protección de los derechos fundamentales de los ciudadanos. No obstante, y en base a los argumentos del TEDH, podemos afirmar que los PVM sí pueden ser compatibles con los derechos fundamentales de los ciudadanos, siempre que se cumpla con las exigencias y requisitos analizados. La clave será concretar el equilibrio y la cooperación, tanto entre autoridades como entre Estados, para que se respeten los derechos a la vida privada y a la protección de los datos personales.

ANEXO: ABREVIATURAS

CEDH: Convención Europea de Derechos Humanos.

DM: Decisión Marco.

FD: Fundamento de Derecho.

GCHQ: Cuartel General de Comunicaciones del Reino Unido.

LIBE: Comisión de Libertades Civiles, Justicia y Asuntos de Interior.

NSA: Agencia de Seguridad Nacional estadounidense.

PVM: Programas de vigilancia masiva.

RGPD: Reglamento General de Protección de Datos.

RIPA: Regulation of Investigatory Powers Act 2000.

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos.

TEDH: Tribunal Europeo de Derechos Humanos.

UE: Unión Europea.

BIBLIOGRAFÍA

Cuerda Arnau, María. 2013. «Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes». En: González Cussac y Arnau Cuerda (Eds.). *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*. Valencia: Tirant lo Blanch.

De Prada, Eirene. 2016. «Vigilancia masiva y derecho a la privacidad». En: *Revista Jueces para la Democracia 87*: 19-27. Acceso el 5-IV-2020. http://www.juecesdemocracia.es/wp-content/uploads/2017/05/revista-87-noviembre-2016.pdf

González Monje, Alicia. 2017. «Amenazas A La Seguridad Y Privacidad: La Dificultad Del Equilibrio Perfecto». En: *Revista Europea de Derechos Fundamentales* 29: 267-94. Acceso 18-IV-2020. https://dialnet.unirioja.es/descarga/articulo/6144011.pdf.

González Porras, Andrés José. 2015. «Privacidad en internet: Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia Masiva». Tesis doctoral. Universidad de Castilla-La Mancha. https://ruidera.uclm.es/xmlui/handle/10578/10092

Greenwald, Gleen. 2013. «NSA collecting phone records of millions of Verizon customers daily». En: *The Guardian*, 5 de junio de 2013. Acceso 7-IV-2020. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Mantelero, Alessandro. 2017. «From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era». En: Taylor, L., Van der Sloot, B. y L. Floridi (Eds.). *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing.

Mejías Alonso, Eva. 2018. «La vigilancia y el control de la población a través de la gestión, la conversación y la explotación de datos masivos». Tesis de posgrado. Universidad Autónoma de Barcelona. https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_271333/Treball_de_recerca_3_.pdf

Oppenheimer, Walter. 2013. «Turing, condenado por gay, recibe el perdón real 60 años después de su muerte». En: *El País*, 24-XII-2013. Acceso 10-IV-2020. https://elpais.com/internacional/2013/12/24/actualidad/1387873660_129481.html

Salamanca Aguado, Esther. 2014. «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones». En: *Revista del Instituto Español de Estudios Estratégicos* 4: 6-32. Acceso 25-IV-2020. https://dialnet.unirioja.es/servlet/articulo?codigo=4900470

Serra Cristobal, Rosario. 2015. «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional». En: *Revista de Derecho Político* 92: enero-abril 2015,73-118. Acceso el 2-IV-2020. https://dialnet.unirioja.es/servlet/articulo?codigo=5050060