Tecnologías de vigilancia masiva y derecho a la intimidad: cuando la necesidad de seguridad amenaza derechos fundamentales

Mass surveillance technologies and the right to privacy: when the need for security threatens fundamental rights

Enmanuela Torres-Gómez [1]

1. Estudiante de Derecho y semillerista de investigación en Bioética, Derechos Humanos y Educación de la Facultad de Derecho, Universidad Militar Campus Nueva Granada, Zipaquirá, Colombia. Correo electrónico: u0602418@unimilitar.edu.co ORCID: https://orcid.org/0000-0001-7993-3249

Tipología: Artículo de reflexión
Para citar este artículo: Torres-Gómez, E. (2021). Tecnologías de vigilancia masiva y derecho a la intimidad: cuando la necesidad de seguridad amenaza derechos fundamentales. *Revista Saberes Jurídicos, 1*(2), 15-23.

Recibido en mayo 26 de 2021
Aceptado en octubre 26 de 2021
Publicado en línea en diciembre 12 de 2021

Palabras clave: derechos; gobierno; privacidad; regulación; vigilancia.

RESUMEN

El presente artículo pretende analizar el contexto actual bajo el cual se desarrollan los derechos humanos con la presencia de la tecnología de vigilancia masiva,con la que cuentan los países más desarrollados en el mundo. Como objetivo primordial se plasma el desarrollo de un estudio jurídico sobre cómo la vigilancia masiva tiene una afectación directa a los derechos fundamentales, como el de la intimidad y la privacidad. Por otra parte, se abordarán también los temas del uso de datos personales de forma masiva y la falta de protección a las personas frente al tratamiento de estos, las consecuencias ético-legales del uso de la vigilancia masiva, cómo esta viola derechos fundamentales y, por último, cómo los gobiernos la ejercen de forma indiscriminada.

Keywords: Rights; Government; Privacy; Regulation; Surveillance.

ABSTRACT

This article aims to analyse the current context under which human rights are being developed with the presence of mass surveillance by the most developed countries in the world. With the main objective of the development of a legal study of how mass surveillance has a direct impact on fundamental rights, such as privacy. On the other hand, the issues of the use of personal data in a massive way and the lack of protection of individuals against the treatment of personal data will also be addressed, the legal ethical consequences of the use of mass surveillance, as it violates fundamental rights and finally, as governments exercise it indiscriminately.

INTRODUCCIÓN

A través de la historia han ocurrido varios acontecimientos relacionados con el avance tecnológico en el que se ve actualmente incurso el mundo; principalmente por parte de los países más desarrollados se realiza vigilancia indiscriminada y arbitraria de los datos privados de las personas de todo el mundo (Snowden, 2019, p. 11). Sin embargo, a raíz de las revelaciones realizadas en el año 2013 por Edward Snowden, exintegrante de la CIA (Cristóbal, 2015, p. 6), sobre cómo las agencias de seguridad estatal utilizan la vigilancia masiva para almacenar y analizar de forma oculta un sinnúmero de comunicaciones privadas de todas las personas en el mundo (Snowden, 2019, p. 7), surgió un dilema jurídico y de disgusto por parte de la sociedad mundial respecto a cómo es violado indiscriminadamente el derecho a la privacidad por parte de estas agencias de seguridad.

Actualmente, la protección de nuestra vida privada no solo está regularmente en riesgo por la creación de redes sociales o por la información que inscribimos en páginas de Internet, sino que muchas veces, sin nosotros haber dado consentimiento de

ello, nuestra información personal circula libremente en el mercado tecnológico (Alonso, 2016, p. 11). No es un secreto que en el presente la sociedad moderna depende en demasiados aspectos de las destrezas ofrecidas por las nuevas tecnologías de la información y comunicación, por lo que los datos personales son el precio pagado por el acceso y el uso de dichas tecnologías (Alonso, 2016, p. 16). Nuestros gobiernos plantean un dilema falso en el cual nos hacen elegir entre seguridad o libertad; estos gobiernos monitorizan indiscriminadamente los correos electrónicos, las llamadas telefónicas y el tráfico de internet de personas en todo el mundo (Cristóbal, 2015, p. 7).

La vigilancia masiva, como aspecto saliente de las tecnologías digitales, se distingue por la inexistencia de una sospecha previa; es decir, hoy en día seguimos sin conocer el alcance de la vigilancia masiva en todas las redes de comunicación, tanto a nivel global como en cada uno de los países (Cristóbal, 2015, p. 18). Los gobiernos esperan que asumamos que cuando hacemos uso de nuestro teléfono celular —o, incluso, del correo electrónico—, todo lo que decimos les pertenece. Es entonces obligación de los Estados respetar dichos derechos, limitando la vigilancia masiva e implementando normas que prohíban la utilización de datos personales sin pruebas que lo justifiquen (Alonso, 2016, p. 25). El actuar del Estado y de las empresas que tienen en su poder el acceso a la información debe cumplir con unos estándares internacionales de derechos humanos (Díaz, 2009, p. 3) y ello supone la adopción de medidas concretas y precisas; cambios legales puntuales y expeditamente identificables, que corrijan las violaciones constantes al derecho a la intimidad.

Por ello, el presente artículo se enfocará en desarrollar una investigación cualitativa respecto a la vigilancia masiva y las normas que la regulan tanto a nivel nacional como internacional, abordando la siguiente problemática: ¿dados los cambios tecnológicos que vivimos constantemente en el mundo, existen normas suficientes que garanticen la protección del derecho a la intimidad en los casos en que se realiza vigilancia de datos privados de las personas sin su consentimiento?

DESARROLLO

Normas que protegen el derecho a la privacidad

Recientemente, las agencias de seguridad utilizan la vigilancia para inmiscuirse en lo más profundo de nuestra intimidad, haciendo seguimiento de la actividad personal que realizamos diariamente en Internet (Snowden, 2019, p. 156). Es así que surge la pregunta: si nuestro derecho a la privacidad está siendo vulnerado con dichas acciones, ¿cómo las normas nacionales e internacionales nos protegen ante estas situaciones? Por ello, es primordial tener conocimiento sobre las normas existentes que protegen nuestros derechos, que están siendo violados por estos acontecimientos, y de la misma forma demostrar la falta de regulación del uso de la vigilancia masiva por parte de los gobiernos de cada país y de las agencias de inteligencia del mundo, que afectan directamente el derecho a la privacidad e intimidad de las personas frente al tratamiento de sus datos personales.

La privacidad regulada a nivel nacional

En Colombia existen una serie de derechos fundamentales que se encuentran contemplados en la Constitución Política; la vulneración de estos implica ciertas consecuencias. Uno de estos significativos derechos es aquel que se refiere a la intimidad personal y que la Constitución Política de Colombia, en su artículo 15, estipula de la siguiente forma:

Todas las personas tienen derecho a la intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar (Díaz, 2009, p. 30). De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (Ley 1581, 2012). En la recolección, el tratamiento y la circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la

ley (Art. 15, Constitución Política de Colombia, 1991).

Es decir que la privacidad es un derecho fundamental que es reconocido constitucionalmente a cada una de las personas que conforman la sociedad colombiana y que además incluye en sí misma la protección de datos personales y el derecho al buen nombre, que a su vez se deben entender como límites del derecho a la intimidad (Sentencia C-640, 2010). De igual forma, la Corte Constitucional también se ha pronunciado sobre la necesidad de amparar este derecho, determinando que la intimidad es un derecho absoluto en los siguientes términos:

> Proteger la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad [...]. La intimidad alude al derecho obvio de todo individuo a rehusar que cualquiera, Estado o particulares, tengan acceso a la esfera interna de la persona (Sentencia nro. T-176, 1996).

Además, como medio de protección al derecho de intimidad en Colombia se expide la Ley 1581 de 2012, que implementa el Régimen General de Protección de Datos Personales en virtud del artículo 15 de la Constitución Política de Colombia. Esta ley constituye reglamentos específicos en el marco general de la protección total de los datos personales en Colombia respecto a las autorizaciones por parte del titular de la información para el tratamiento de sus datos personales, las políticas del tratamiento de estos datos y la rendición de cuentas respecto de la utilización de datos personales (Ley 1581, 2012).

La privacidad regulada a nivel internacional

Por otro lado, la comunidad internacional ha hecho esfuerzos por darle la debida protección al derecho a la intimidad y privacidad personal, en especial con el auge de las nuevas tecnologías, que permiten la realización de vigilancia masiva en el mundo y a raíz de la cual se ha perdido la confianza sobre los medios tecnológicos y de comunicación (Cristóbal, 2015, p. 9). El derecho internacional de los derechos humanos salvaguarda los derechos a la intimidad y a la libertad de expresión, pronunciando su preocupación por la seguridad en el uso de las nuevas tecnologías y encontrándose en proceso de aumento de normas internacionales para la protección integral de la intimidad y de los datos personales.

Es primordial que los Estados cumplan la obligación legal de proteger y hacer valer los derechos de privacidad e intimidad personal con el que cuentan sus ciudadanos. Por ejemplo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos protege a las personas frente a las "injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia" (ICCPR, 1966, p. 17). El derecho internacional permite a los gobiernos, con ciertas restricciones, llevar acciones que interfieren con esos derechos, pero esto solo en determinadas circunstancias: la vigilancia legítima de las comunicaciones es una de ellas (DUDH, 1948, p. 19). Aun así, es importante aclarar que cualquier impertinencia en el uso de datos personales que no sea acorde con las obligaciones de los Estados es una violación de derechos humanos (Díaz, 2009).

De igual forma, el derecho al respeto de la vida privada o la intimidad son considerados como derechos humanos fundamentales, establecidos por diversos instrumentos internacionales como la Declaración Universal de los Derechos Humanos aprobada por la Asamblea General de las Naciones Unidas en 1948 (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículos 17 y 19), la Convención Americana sobre Derechos Humanos de 1969 (artículos 11 y 13), y la Convención sobre los Derechos del Niño de 1989 (artículo 16), instrumentos todos estos firmados y ratificados por nuestro país.

Legalidad de la vigilancia masiva

La jurisdicción nacional autoriza en ciertos casos la vigilancia de las comunicaciones; sin embargo, existen programas de vigilancia que son totalmente ilegítimos y que, a pesar de su apariencia de legalidad, no van acorde a los lineamientos establecidos por el derecho internacional, incluso si estos son conformes a la legislación nacional (Snowden, 2019, p. 186), pues los Estados deben

cumplir con ciertas obligaciones en materia de derechos humanos en virtud de sus ordenamientos jurídicos internos y del derecho internacional.

Los derechos que resultan más afectados por la vigilancia masiva indiscriminada son la intimidad y la libertad de expresión, derechos incluidos en la Declaración Universal de Derechos Humanos, protegidos por la Constitución Política Colombiana y garantizados por el derecho internacional. En solo ciertos casos, la vigilancia masiva resulta ser legal y legítima; cuando:

- Es autorizada por la legislación; es decir, que se efectúa acorde a las leyes y normas claras de acceso público, como la Ley 1581 de 2012, que implementa el Régimen de Protección de Datos Personales en Colombia.

- Es emitida y autorizada por una orden de una autoridad independiente, como un juez, en los casos de investigaciones penales.

- Es utilizada para conseguir un fin legítimo, en casos de investigaciones penales o en pro de la seguridad nacional.

- Es para obtener un fin legítimo y está dirigida a una persona, un grupo de individuos definido o un lugar concreto, que es directamente pertinente para el logro de dicho fin.

- Su ejercicio es necesario para lograr una finalidad legítima como la investigación y prevención de un delito.

- Es proporcionada a la finalidad legítima para la que se lleva a cabo y se equilibra de acuerdo con cómo afecte los derechos humanos, siempre que no sobrepase estos límites y se use para fines no legítimos. Es decir, debe hacerse uso de los medios de vigilancia menos intrusivos.

Aun así, la Amnistía Internacional considera que la vigilancia masiva indiscriminada de ninguna forma permite construir una injerencia necesaria y proporcionada en los derechos humanos (Amnistía Internacional, 2013, p. 3). Esta vigilancia solo es permitida a los gobiernos cuando la realizan bajo los anteriores casos; de esta forma se realiza de manera selectiva (Cristóbal, 2015, p. 18). No obstante, la NSA, que es la Agencia de Seguridad Nacional estadunidense, y la jefatura de comunicaciones del Gobierno británico, realizan vigilancia masiva de las comunicaciones sobre varios países del mundo de manera ilegítima y desproporcionada (Snowden, 2019, p. 159), pues no han demostrado pruebas convincentes de la existencia de una necesidad o fin legítimo y, además, están autorizados por leyes imprecisas de difícil interpretación.

¿Cómo tienen acceso a los datos personales?

En realidad, la vigilancia masiva es posible gracias al uso diario que le damos a la tecnología que tenemos a nuestro alcance. Con estas acciones se está anulando la privacidad, ya que, por medio de las redes sociales, las redes telefónicas, los proveedores de internet de empresas, establecimientos, hogares, etc., e incluso cables de fibra óptica, se permite el ingreso a los datos personales de cualquier ciudadano, los cuales son guardados en grandes centros de almacenamiento o bases de datos (Cristóbal, 2015, p. 10).

Es decir que por el simple hecho de conectarnos a internet los gobiernos y las agencias de vigilancia masiva constituidas en el mundo ya tienen acceso a nuestros datos. Además, existen programas desarrollados a nivel nacional e internacional, donde simplemente las personas somos un número de teléfono, un correo electrónico, un ordenador o una dirección IP en donde todos nuestros datos están siendo recolectados (Snowden, 2019, p. 186).

Los ciudadanos, en general, entregan su información personal (teléfonos, número de cédula, fotos, correo electrónico, etc.) a diferentes entidades (bancos, universidades, centros comerciales, lugares de trabajo etc.) y, en caso de que esta información personal sea expuesta, se recurre a la Ley General de Protección de Datos Personales que establece lo siguiente: “Nadie puede acceder a los datos de ninguna persona sin estar previamente autorizado y que esta autorización haya sido emitida por la persona de la que se requiere información” (Ley 1581, 2012). En esta ley se establecen ciertos requisitos mínimos que todas las empresas están en obligación de cumplir para el tratamiento de datos personales; incumplir dicha ley acarrearía ciertas sanciones.

Un uso inadecuado de la información personal de cualquier persona que se encuentre registrada en una base de datos de cualquier entidad la expone constantemente a que se le generen riesgos a su reputación, en el ámbito financiero o en su buen nombre, pues cuando la información circula en la web no puede ser controlada con facilidad (Díaz, 2009, p. 6). Es por ello que la Superintendencia de Industria y Comercio implementó una sanción con una multa de hasta de cien millones de pesos ($100.000.000) para todas aquellas entidades que violen este derecho —según sea el caso depende el monto de la sanción—; además, la correspondiente indemnización por perjuicios causados a la persona que estuvo perjudicada (Ley 1581, 2012).

Afectación del derecho a la privacidad a causa de las nuevas tecnologías

Como anteriormente se hizo mención, la privacidad es un derecho reconocido internacionalmente con una protección especial y es comprobado constitucionalmente en Colombia como un derecho fundamental con el que cuentan todos los ciudadanos (Art. 15, Constitución Política de Colombia, 1991). Además, la privacidad trae consigo otros dos derechos conexos como el de Protección de Datos Personales (Habeas Data) y el Buen Nombre, los cuales tienen una función determinada que consiste en actuar como límites del derecho a la intimidad (Ley 1581, 2012).

A raíz de la aparición de nuevas tecnologías y principalmente del internet, el derecho a la intimidad ha tenido que ir evolucionando, pues su protección internacional debe ser acorde con los cambios tecnológicos, de tal forma que su concepción inicial de restringir el acceso de terceros a una parte de la vida de las personas trasciende, dando protección al titular de los datos para permitirle ejercer control sobre su propia información (Alonso, 2016, p. 27). Surge, entonces, una dicotomía del derecho a la intimidad como absoluto y fundamental, y el derecho a la información como limitante del habeas data para tener seguridad y protección nacional, pero de ninguna forma debe existir subordinación de alguno de estos, pues ambos son derechos autónomos y el derecho a la información debe ser limitado más no absoluto (Díaz, 2009, p. 7).

A pesar de lo anterior, el derecho a la información no puede ser suprimido puesto que es necesario para el desarrollo de las actividades administrativas, por lo cual es menester que el Estado colombiano regule muy bien su funcionamiento y que este sea acorde con lo establecido en la Constitución, en la ley y el margen de protección implementado internacionalmente respecto del derecho a la privacidad (Sentencia C-640, 2010). Es decir que el seguimiento que es realizado a gran escala de manera indiscriminada por el Estado y otras agencias de vigilancia masiva de las comunicaciones de las personas no puede seguir realizándose sin una sospecha razonable de que estas se encuentren implicadas en una actividad delictiva o que sea a causa de un fin legítimo (Cristóbal, 2015, p. 25).

Acceso a la información como derecho

El acceso a la información es un derecho fundamental, reconocido internacionalmente por la Convención Americana de Derechos Humanos en su artículo 13, el cual se conecta integralmente con el derecho de libertad de expresión, y por la Declaración Universal de los Derechos Humanos de 1948, en su artículo 19, el cual manifiesta que:

> Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. (DUDH, 1948).

A nivel nacional, el acceso a la información es reconocido por la Ley 1712 de 2014 de Transparencia y del Derecho de Acceso a la Información Pública Nacional; esta es utilizada como herramienta normativa que se encarga de regular todo lo relacionado con el derecho fundamental de acceso a la información pública en Colombia. El ejercicio de este derecho se basa en que los ciudadanos han depositado en el Estado cierta información, concediéndole atribuciones a este, razón por la cual toda información que el Estado posee le pertenece a toda la sociedad por derecho,

como también el hecho de conocer qué hacen con la información depositada por los ciudadanos en sus entidades (Díaz, 2009, p. 5).

Es por ello que la Corte Constitucional determina que a través del derecho de petición los ciudadanos pueden hacer valer su derecho de acceso a la información precisando que:

> La Constitución consagra expresamente el derecho fundamental de acceso a información pública (C.P. Art. 74) y el derecho fundamental de petición (C.P. Art. 23) como herramientas esenciales para hacer efectivos los principios de transparencia y publicidad de los actos del Estado y, en consecuencia, se convierten en una salvaguarda fundamental de las personas contra la arbitrariedad estatal y en condiciones de posibilidad de los derechos políticos. Por tales razones, los límites a tales derechos se encuentran sometidos a exigentes condiciones constitucionales y el juicio de constitucionalidad de cualquier norma que los restrinja debe ser en extremo riguroso (Sentencia T 487, 2017).

Redes sociales

Por otra parte, el internet ha resultado ser una gran herramienta de información mundial, ya que ha trascendido las fronteras y además ha cuestionado las concepciones de la soberanía de los Estados (Cristóbal, 2015, p. 25). En el siglo XXI, las redes sociales han surgido como una respuesta al entorno social de comunicarse y de establecer vínculos personales, sea a nivel profesional o sentimental, y en algunas ocasiones en dichas redes se proyecta una imagen virtual que no corresponde a la realidad o cotidianidad de las personas (Carrillo, 2012, p. 6).

Por ello, es importante tener en cuenta que como actualmente el concepto de "intimidad" se ha venido transformando, esto también ha sido debido a la facilidad que tienen las redes sociales para difundir la información que anteriormente era considerada privada y que ahora los usuarios de internet consideran de posible publicación (Carrillo, 2012, p. 8). Con ello, se asiste a otra forma de desfiguración de la intimidad reconocida constitucionalmente como derecho fundamental y se permean los límites entre lo privado y lo público.

Es una realidad que el internet es actualmente una herramienta esencial para los ciudadanos en función de su actividad social en la sociedad, pero a pesar de que el internet brinda a las personas una posibilidad de realizar sus comunicaciones a nivel nacional y más allá de las fronteras nacionales, o de acceder a información sobre el mundo en general, no necesariamente justifica sacrificar la privacidad y las expresiones de intimidad para crear un poder de vigilancia masiva de gran magnitud por parte de las agencias de inteligencia e, incluso, de nuestros propios gobiernos (Snowden, 2019, p. 5).

Vigilancia masiva ejercida por los gobiernos

Los gobiernos nacionales asumen que en el momento en que los ciudadanos hacen uso de las nuevas tecnologías, utilizando sus teléfonos, abriendo sus redes sociales, sus correos electrónicos o, simplemente, ingresando a internet, todo lo que consignen o busquen en este medio ya les pertenece (Carrillo, 2012, p. 22). En Colombia, siendo un Estado Social de Derecho, donde las leyes equilibran los conceptos del derecho a la intimidad y el derecho al acceso de información y uso de la vigilancia por parte de la nación (Sentencia T 487, 2017), las personas deberían ser consideradas inocentes hasta que se demuestra lo contrario, de conformidad con lo establecido en la ley, y además gozar efectivamente del derecho a que se respete su vida privada. Por tanto, antes de violar estos derechos fundamentales, como lo son la libertad, privacidad e intimidad, los gobiernos deben tener indicios de que se está cometiendo un delito o comprobar que existe un fin legítimo por el cual se hará uso de la vigilancia o interceptación de comunicaciones (Cristóbal, 2015, p. 37).

Normalmente, por parte de los gobiernos se lleva a cabo la vigilancia de manera selectiva en cuanto al seguimiento de las comunicaciones, de las acciones o de los movimientos de una persona, pero esto solo puede ser realizado si se comprueba que este seguimiento se dirige a una persona o a un grupo determinado por motivos legítimos concretos (Ley 1581, 2012). Es decir que, para ello, las autoridades

tendrían que obtener el permiso de un juez o de una autoridad nacional competente. Si el seguimiento es realizado a gran escala o de forma indiscriminada, y se procede a vigilar las comunicaciones de las personas sin que exista una sospecha razonable de que estas estén implicadas en una actividad delictiva, entonces se parte de la presunción de que todo el mundo es potencialmente culpable, en vez de partir de la presunción de inocencia hasta que se demuestre lo contrario (Snowden, 2019, p. 10).

El mayor ejercicio de vigilancia masiva a nivel mundial lo realiza la Alianza de los Cinco Ojos, que está integrada por los gobiernos de Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda, en donde se encuentran las agencias de seguridad estadounidense NSA y la británica GCHQ, las cuales tienen algunos de los centros de datos más grandes de todo el mundo (Alonso, 2016, p. 37). Estas agencias actúan bajo la excusa de necesitar más métodos de espionaje para atrapar a los "terroristas" (Cristóbal, 2015, p. 19), en donde los gobiernos monitorizan de forma indiscriminada todos los correos electrónicos, las llamadas telefónicas y el tráfico de internet de personas de todo el mundo. Esto lo hacen a través de ciertos programas que permiten acceder a los datos de las principales empresas de internet y de telefonía a gran escala, sin tener en cuenta la normatividad internacional y nacional de protección contra la violación indiscriminada del derecho a la intimidad.

Por otra parte, Colombia es un país que sobresale dentro de los países latinoamericanos debido al despliegue de PUMA, una infraestructura implementada para la vigilancia masiva dentro del país que está a cargo de la Dirección de Inteligencia Policial, identificada con las siglas DIPOL (Alonso, 2016, p. 36). Esta es principalmente utilizada para la interceptación y el espionaje de políticos, jueces, periodistas o activistas de derechos humanos, y su poder le permite realizar la vigilancia masiva de datos de telefonía móvil 3G y de líneas principales de internet, así como el monitoreo de comunicaciones de voz y de datos en todo Colombia.

Falta de protección al derecho a la intimidad

En la sentencia C-640 de 2010 la Corte Constitucional reiteró que el derecho a la intimidad es inalienable, imprescriptible y solo susceptible de limitación por razones legítimas y siendo estas debidamente justificadas constitucionalmente; "por esta razón, la privacidad como ese espacio personal y ontológico, sólo puede ser objeto de limitaciones o de interferencias en guarda de un verdadero interés general que responda a los presupuestos establecidos por el artículo 1.o de la Constitución" (Sentencia C-640, 2010). Sin embargo, a pesar de la protección existente del derecho a la intimidad por normas de derechos humanos a nivel internacional, o a nivel nacional por parte de la Constitución y las leyes de protección de datos, estas no resultan ser suficientes, pues son violadas por los propios gobiernos que las imponen y por agencias de vigilancia masiva a nivel mundial.

Además, algunas de las leyes nacionales existentes para la conservación de datos, en vez de protegerlos, en ciertos casos se vuelven invasivas, pues obligan a los proveedores de servicios de comunicaciones a generar bases de datos respecto a quiénes se comunican con ellos por medio telefónico o por internet (Cristóbal, 2015, p. 23), aumentando considerablemente el ejercicio de vigilancia por parte del Estado y, de este modo, el alcance de las violaciones de los derechos humanos. Dicha violación del derecho a la intimidad también puede presentarse porque las agencias de vigilancia masiva a nivel mundial se aprovechan de las bases de datos de comunicaciones nacionales por ser estas vulnerables al robo de datos o a la revelación accidental de los mismos (Alonso, 2016, p. 17).

Es menester la intervención por parte de las organizaciones internacionales encargadas de la protección de los derechos humanos a nivel mundial para hacer frente a esta violación indiscriminada del derecho a la intimidad de las personas, y que no es respetado ni siquiera por nuestros propios gobiernos. Es por ello que se requiere de una norma internacional que frene todo tipo de recolección de datos de forma ilegítima, por parte de gobiernos y agencias de vigilancia mundial, y que, además, se implemente una inspección detallada de las actividades referentes al acceso de información y recolección de datos de estos mismos, asegurándose que se realicen conforme a un fin legítimo y respetando el derecho a la intimidad como absoluto y fundamental de cada ser humano en la sociedad.

CONCLUSIÓN

En la actualidad, seguimos sin conocer el alcance que tiene la vigilancia masiva en las redes de comunicación, tanto a nivel global como a nivel nacional, en cada uno de los gobiernos. Es por ello que en una sociedad que internacionalmente respeta la intimidad, la privacidad y la libertad, y en un Estado Social de Derecho que constitucional y legalmente protege estos derechos, no pueden buscarse pruebas aleatoriamente en las comunicaciones privadas de las personas sin antes comprobar la existencia de un fin legítimo o la protección a otros bienes jurídicos de igual o mayor amparo, como por ejemplo la seguridad nacional. Todo esto debe realizarse acorde al principio de necesidad y proporcionalidad, y en caso de que no existiese ningún fin legítimo se estaría frente a una clara violación del derecho a la intimidad personal: no olvidemos que es considerado un derecho fundamental y absoluto de las personas.

La vigilancia masiva a nivel nacional y global sigue sin cumplir con los estándares de derechos fundamentales y los que establecen los principios de necesidad y de proporcionalidad, ni va tampoco acorde con las normas internacionales de derechos humanos que prohíben dicha actividad y que son de carácter imperativo, al ser exigidas a todos los países. Es decir que, a pesar de la existencia de estas normas internacionales, y de su fuerza vinculante en cada Estado, no se está cumpliendo con un nivel de protección alto de derechos ni tampoco se han puesto restricciones suficientes sobre la utilización y recolección de datos personales a gran escala a los gobiernos nacionales y a las agencias globales de vigilancia masiva a nivel nacional e internacional.

En vista de que el crecimiento de la informática u otros avances tecnológicos facilitan la recaudación, la codificación, el almacenamiento y la circulación de datos referentes a aspectos diversos de la vida personal de los ciudadanos, es necesario que exista una regulación clara sobre el tema y que, a diferencia de la actual protección internacional del derecho a la intimidad, esta proteja de manera efectiva dicha información de carácter privado e impida la violación indiscriminada por parte de los gobiernos y las agencias de vigilancia del derecho a la intimidad, como actualmente se ha venido presentando, y que, de igual forma, se facilite el acceso a dicha información personal bajo ciertas condiciones establecidas normativamente.

REFERENCIAS BIBLIOGRÁFICAS

Alonso, E. M. (2016). La Vigilancia y el control de la población a través de la gestión, la conservación y la explotación de datos masivos. Escola Superior d´Arxivística i Gestió de Documents. UAB, 148 [En línea]. https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_271333/Treball_de_recerca_3_.pdf?fbclid=IwAR1fVGcREU9gJ3w1gItKmxYR74JgvfT9LFCaNo5LwMpzhMlh-x4hOBmhlmU

Amnistía Internacional. (2013). Vigilancia masiva. Amnistía Internacional España. https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/?fbclid=IwAR2vgw7EEjEhAYEBqC53dd7ytyb-s1ojT5JZ0GnK5x5-WlsXxSCoexlt6zg

Asamblea General de la ONU. (1966). ICCPR. Naciones Unidas. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Carrillo, M. R. (2012). El impacto de Internet y las redes sociales en el derecho a la libertad de expresión. *Revista de Filosofía Jurídica, Social y Política, 19*(3), 331-349. Tomado de https://www.corteidh.or.cr/tablas/r32923.pdf

Congreso de la República de Colombia. (2012). Ley 1581 Protección de Datos Personales [En línea]. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República de Colombia. (2012). Ley 1581 Protección de Datos Personales [en línea]. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Constitución Política De Colombia. (1991). Art. 15: Derecho Privacidad [En línea]. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Cristóbal, R. S. (2015). La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional. UNED, *Revista de Derecho Político (92)*, 73-118. https://doi.org/10.5944/rdp.92.2015.14422

Naciones Unidas (1966): Pacto Internacional de Derechos Civiles y Políticos. Resolución 2200 A (XXI), de 16 de diciembre de 1966, de la Asamblea General. [En línea]. https://www.refworld.org.es/docid/5c92b8584.html

Declaración Universal de los Derechos Humanos. (1948). Comisión de Derechos Humanos Naciones Unidas. [En línea] https://www.un.org/es/universal-declaration-human-rights/

Declaración Universal de los Derechos Humanos. (1948). Artículo 19. Comisión de Derechos Humanos Naciones Unidas. https://www.un.org/es/universal-declaration-human-rights/

Díaz, F. C. (2009). Derecho a la Intimidad y Habeas Data. Derecho y Realidad, 10. ///C:/Users/ASUS%20X407UA%20I3/Downloads/5010-Texto%20del%20art%C3%ADculo-11064-1-10-20160707.pdf

Sentencia C-640. (2010). Corte Constitucional Colombia [En Línea]. https://www.corteconstitucional.gov.co/relatoria/2010/C-640-10.htm

Sentencia T-487. (2017). Corte Constitucional Colombia [En línea] https://www.corteconstitucional.gov.co/relatoria/2017/T-487-17.htm

Snowden, E. (2019). Vigilancia Permanente. Planeta. en: https://kavilando.org/images/stories/documentos/Sin-ttulo.pdf