UNIVERSIDAD DE PIURA

FACULTAD DE DERECHO

Constitucionalidad de la vigilancia masiva en el tratamiento de los datos personales en relación al derecho a la intimidad

Tesis para optar el Título de
Abogado

César Roberto Haro Benites
Yadira Cristal Moncada Hernández

Asesor(es):
Dr. Luis Fernando Castillo Córdova

Piura, setiembre de 2024

Aprobación

La tesis titulada “Constitucionalidad de la vigilancia masiva en el tratamiento de los datos personales en relación al derecho a la intimidad”, presentada por lo bachilleres César Roberto Haro Benites y Yadira Cristal Moncada Hernández en cumplimiento con los requisitos para obtener el Título de Abogado, fue aprobada por el Director de tesis Dr. Luis Fernando Castillo Córdova.

Director de tesis

UNIVERSIDAD DE PIURA

Declaración Jurada de Originalidad del Trabajo Final

Yo, César Roberto Haro Benites, egresado del **Programa Académico** de Derecho de la Facultad de Derecho de la Universidad de Piura, identificado(a) con DNI N° 70264792.

Declaro bajo juramento que:

1. Soy autor del trabajo final titulado:
   "Constitucionalidad de la vigilancia masiva en el tratamiento de los datos personales en relación al derecho a la intimidad"
   El mismo que presento bajo la modalidad de **Tesis**[1] para optar el Título profesional[2] de Abogado.

2. Que el trabajo se realizó en coautoría con los siguientes alumnos de la Universidad de Piura.
   - Yadira Cristal Moncada Hernández, identificado con DNI N° 71055188

3. La asesoría del trabajo estuvo a cargo de:
   - Dr. Luis Fernando Castillo Córdova, identificado con DNI N° 02822012

4. El texto de mi trabajo final respeta y no vulnera los derechos de terceros o de ser el caso derechos de los coautores, incluidos los derechos de propiedad intelectual, datos personales, entre otros. En tal sentido, el texto de mi trabajo final no ha sido plagiado total ni parcialmente, para la cual he respetado las normas internacionales de citas y referencias de las fuentes consultadas.

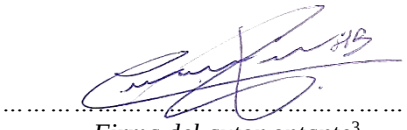
5. El texto del trabajo final que presento no ha sido publicado ni presentado antes en cualquier medio electrónico o físico.

6. La investigación, los resultados, datos, conclusiones y demás información presentada que atribuyo a mi autoría son veraces.

7. Declaro que mi trabajo final cumple con todas las normas de la Universidad de Piura.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad de Piura y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Fecha: *02/09/2024*.



……

Firma del autor optante[3]

[1] Indicar si es tesis, trabajo de investigación, trabajo académico o trabajo de suficiencia profesional.
[2] Grado de Bachiller, Título profesional, Grado de Maestro o Grado de Doctor.
[3] Idéntica al DNI; no se admite digital, salvo certificado.

UNIVERSIDAD DE PIURA

Declaración Jurada de Originalidad del Trabajo Final

Yo, Yadira Cristal Moncada Hernández, egresado del **Programa Académico** de Derecho de la Facultad de Derecho de la Universidad de Piura, identificado(a) con DNI N° 71055188.

Declaro bajo juramento que:

1. Soy autor del trabajo final titulado:
   "Constitucionalidad de la vigilancia masiva en el tratamiento de los datos personales en relación al derecho a la intimidad"
   El mismo que presento bajo la modalidad de **Tesis**[1] para optar el Título profesional[2] de Abogado.

2. Que el trabajo se realizó en coautoría con los siguientes alumnos de la Universidad de Piura.
   - César Roberto Haro Benites, identificado con DNI N° 70264792

3. La asesoría del trabajo estuvo a cargo de:
   - Dr. Luis Fernando Castillo Córdova, identificado con DNI N° 02822012

4. El texto de mi trabajo final respeta y no vulnera los derechos de terceros o de ser el caso derechos de los coautores, incluidos los derechos de propiedad intelectual, datos personales, entre otros. En tal sentido, el texto de mi trabajo final no ha sido plagiado total ni parcialmente, para la cual he respetado las normas internacionales de citas y referencias de las fuentes consultadas.

5. El texto del trabajo final que presento no ha sido publicado ni presentado antes en cualquier medio electrónico o físico.

6. La investigación, los resultados, datos, conclusiones y demás información presentada que atribuyo a mi autoría son veraces.

7. Declaro que mi trabajo final cumple con todas las normas de la Universidad de Piura.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad de Piura y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Fecha: *02/09/2024*.

……
Firma del autor optante[3]

[1] Indicar si es tesis, trabajo de investigación, trabajo académico o trabajo de suficiencia profesional.
[2] Grado de Bachiller, Título profesional, Grado de Maestro o Grado de Doctor.
[3] Idéntica al DNI; no se admite digital, salvo certificado.

Dedicatoria

A mis padres, César y Janet, por haberme brindado una educación y cuyo amor incondicional, sacrificio, apoyo y enseñanzas han sido la base de cada paso en mi camino universitario.

A mi hermana María Lucía, por su confianza, comprensión y cariño que son una fuente constante de fortaleza.

A mis abuelos, Roberto y Doris, por los valores que me han inculcado, así como también por su sabiduría que me inspiran a alcanzar mis metas.

A Floriselda, por su esfuerzo, ayuda y dedicación hacia mi persona han sido fundamentales para contribuir a este logro

César Roberto Haro Benites.

Dedico este trabajo a mis padres, Manuel y Consuelo, quienes, con su esfuerzo y sacrificio, me han dado la oportunidad de estudiar. Siendo esta investigación un reflejo del amor, la fe y el apoyo incondicional que me han brindado. Sin su presencia y apoyo constante, este logro no hubiera sido posible.

A mi hermana, Gloria, por su apoyo inquebrantable. Gracias por estar a mi lado durante esta etapa, preocupándote y dando más de lo que te correspondía. A mi hermano, Ryan, por ser mi red de seguridad y por animarme siempre.

Finalmente, dedico este trabajo a Sasy, aun cuando ya no esté conmigo, su presencia fue una pieza clave en mi etapa universitaria, llenando mis días de alegría y compañía.

Yadira Cristal Moncada Hernández

Agradecimientos

Queremos expresar nuestro más sincero agradecimiento a Dios y a la Virgen María por las bendiciones y la guía que han iluminado nuestro camino a lo largo de este proceso.

Nuestro agradecimiento se extiende a nuestros maestros académicos, cuyas enseñanzas y consejos han dejado una huella indeleble en nuestra formación profesional y personal. En particular, deseamos expresar un especial reconocimiento al Dr. Luis Fernando Castillo Córdova su apoyo incondicional, paciencia y dedicación han sido fundamentales para la realización de este trabajo. Su compromiso con nuestra formación ha sido una fuente constante de inspiración y motivación.

Agradecemos profundamente a todos quienes han contribuido, directa o indirectamente, al éxito de esta investigación.

Resumen

En la era digital, la tecnología ha mejorado la conectividad global y la comunicación instantánea, pero también ha planteado desafíos en términos de seguridad nacional y protección de derechos fundamentales. Una de las medidas adoptadas por los estados para enfrentar estos desafíos es la vigilancia masiva, que implica la recopilación y análisis extensivo de datos personales para garantizar la seguridad. Sin embargo, esta práctica suscita dudas sobre su constitucionalidad y las implicaciones éticas en relación con el derecho a la intimidad.

La investigación examina la relación entre vigilancia masiva, como mecanismo para garantizar la seguridad nacional, y el derecho a la intimidad; desde la perspectiva de la teoría armonizadora de los derechos, que propone buscar soluciones que permitan la coexistencia de ambos en lugar de sacrificar uno en favor del otro. Se requiere un análisis detallado de cada caso específico para aplicar este enfoque.

Se exploran los términos, marcos regulatorios y principios esenciales para comprender cómo esta práctica afecta los derechos individuales y el manejo de datos en la era digital, analizando la evolución del derecho a la intimidad y cómo se integra en el sistema normativo peruano, así podríamos analizar si la vigilancia masiva se ajusta a las normas constitucionales peruanas y sus implicaciones para la intimidad y otros derechos.

El objetivo principal de esta investigación es ofrecer una visión integral que permita una aplicación equilibrada de la vigilancia masiva para garantizar la protección de la seguridad nacional respetando los derechos fundamentales de los ciudadanos. La investigación busca desarrollar un marco que, a través de la teoría armonizadora, proporcione directrices para aplicar la vigilancia masiva de manera que respete los derechos humanos y promueva un equilibrio justo entre intimidad y seguridad.

Tabla de contenido

Lista de tablas

Lista de figuras

Introducción

En la era digital actual, la tecnología ha transformado significativamente diversos aspectos de la vida cotidiana, mejorando la conectividad global y facilitando la comunicación instantánea. Sin embargo, este avance también ha planteado desafíos importantes, especialmente en el ámbito de la seguridad nacional y la protección de los derechos fundamentales. En este contexto, los estados han adoptado diversas medidas tecnológicas para combatir la delincuencia y garantizar la seguridad de sus ciudadanos. Una de estas medidas es la vigilancia masiva, que implica la recopilación y análisis de datos personales con el fin de proteger la integridad y soberanía de un país.

La implementación de la vigilancia masiva, justificada en algunos casos por razones de seguridad, plantea serias interrogantes sobre su constitucionalidad y las implicancias éticas en el tratamiento de los datos personales. El derecho a la intimidad, reconocido como un derecho fundamental, se ve particularmente afectado por estas prácticas. Por lo tanto, es crucial examinar los desafíos legales y morales asociados a la vigilancia masiva, considerando cómo puede erosionar la esfera privada de los individuos y socavar los pilares de las sociedades democráticas.

Esta investigación se centra en analizar la interacción entre la vigilancia masiva y el derecho a la intimidad desde la perspectiva de la teoría armonizadora de los derechos. Esta teoría propone que, en lugar de eliminar uno de los derechos relevantes para resolver una controversia en favor del otro, se deben buscar soluciones que permitan la coexistencia de ambos derechos en la medida de lo posible a partir de que los derechos cuentan con un alcance constitucional razonable y, por tanto, limitado. Este enfoque requiere un cuidadoso análisis detallado de las circunstancias específicas de cada caso.

En el primer capítulo titulado “La vigilancia masiva y su implicancia en el tratamiento de datos personales”, se explican los conceptos fundamentales que serán cruciales para comprender el contenido que abordaremos a lo largo del texto. La vigilancia masiva, una práctica en la que se recopila y analiza grandes volúmenes de datos de manera indiscriminada, ha adquirido una relevancia creciente en la era digital. Por lo tanto, es esencial desglosar y entender términos clave, marcos regulatorios y los principios que rigen la protección de la información individual. Este capítulo establecerá las bases conceptuales necesarias para abordar cómo la vigilancia masiva afecta los derechos de los individuos y las prácticas de manejo de datos en nuestra sociedad contemporánea.

En el segundo capítulo titulado “Derecho a la intimidad como derecho fundamental”, se aborda el origen de la protección de este derecho, así como los elementos que configuran

su el contenido constitucionalmente protegido, a través de las metodologías sobre el contenido de los derechos (teoría conflictivista y teoría armonizadora). En un contexto donde la protección de datos personales y la intimidad se han convertido en temas de creciente relevancia, es fundamental comprender cómo el derecho a la intimidad se integra y protege dentro del sistema normativo peruano. Este capítulo examina las bases constitucionales y legales que sustentan este derecho, así como su evolución y la manera en que se aplica en la práctica. Además, se analizan cómo las normas peruanas se alinean con los estándares internacionales y los desafíos específicos que enfrenta el país en la protección de la intimidad en la era digital. A través de este enfoque, buscamos ofrecer una visión comprensiva de la importancia del derecho a la intimidad en el Perú y su impacto en la vida de los ciudadanos.

Para concluir, en el tercer y último capítulo titulado “La validez de la vigilancia masiva. Especial referencia a su constitucionalidad en el Perú”, se aborda diversas situaciones donde se ha manifestado la práctica indebida e indiscriminada de la vigilancia masiva, así como también un análisis detallado sobre la legitimidad de la misma desde una perspectiva constitucional y teórica. Este capítulo se enfoca en la teoría armonizadora como una herramienta clave para enfrentar los dilemas que plantea la vigilancia masiva, buscando equilibrar la necesidad de seguridad nacional con la protección de los derechos fundamentales de los ciudadanos.

Exploraremos cómo la vigilancia masiva se enfrenta a las normas constitucionales peruanas y qué implicaciones tiene para el derecho a la intimidad y otros derechos fundamentales en relación con este. A través de gráficos ilustrativos, se facilitará una comprensión más clara de la solución a la que se podría llegar para evitar interferencias desproporcionadas. Siendo el principal objetivo ofrecer una visión comprensiva que permita una aplicación adecuada de la vigilancia masiva, garantizando siempre el respeto a los derechos humanos y promoviendo la seguridad nacional sin que se comprometa las libertades individuales.

Capítulo 1

La vigilancia masiva y su implicancia en el tratamiento de datos personales

1.1 Vigilancia masiva. Aspectos conceptuales y marco general

El significado de la palabra vigilancia según la Real Academia Española de la Lengua (RAE) "es el cuidado y atención exacta en las cosas que están a cargo de cada uno"[1]. La vigilancia está destinada a observar conductas y acciones de personas, teniendo como foco central el registro de expectativas de comportamiento, es decir, el interés por registrar y dar cuenta de conductas y acciones que son previsibles que ocurran en un momento y lugar determinado. Además, la vigilancia se caracteriza por ser rutinaria, sistemática, dirigida a observar detalles de las personas, que tiene como objetivo el control, eficiencia y coordinación en la realización de los comportamientos. Que sea "masiva" significa que está en referencia a las masas humanas, a la multitud; que es muy dispersa y usualmente sus miembros no se conocen entre sí. Es un concepto que hace alusión a un grupo de personas heterogéneas, de todos los estratos sociales y grupos demográficos, pero que su conducta es homogénea en escoger un particular objeto de interés. Claramente este significado no basta, sino que es necesario profundizar en él especialmente desde un ámbito jurídico.

Es normal que un Estado realice vigilancia a grupos o individuos sospechosos de haber cometido algún delito. En democracias modernas este tipo de vigilancia se debe realizar a través de una orden judicial que determine que hay indicios de que alguien es sospechoso de haber cometido un crimen. Según la organización Privacy International (2015) la vigilancia masiva es "la sujeción de una población o componente significativo de un grupo al monitoreo indiscriminado. Implica una interferencia sistemática con el derecho de las personas a la privacidad"[2]. De esta manera, la vigilancia masiva puede ser entendida como el acopio y análisis indiscriminado de datos, lo que quiere decir que las personas, al hacer uso de la Internet, incluso al hacerlo dentro de los parámetros de la ley, estarán sujetos a esta recolección masiva. Es así que la vigilancia masiva implica una amenaza para nuestro derecho a la intimidad y para la democracia.

Al vivir en una sociedad donde la tecnología crece a pasos agigantados, no resulta raro pensar que estas actividades de vigilancia puedan llegar a ser excesivas, arbitrarias o indeseables, ya que con esta nueva tecnología se hace un seguimiento detallado sobre los

---

1 REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. Vigésimo primera edición. Madrid: Editorial Espasa Calpe. 1992. ISBN: 84-239-9416-3

2 BONIFAZ, R. *Vigilancia masiva y privacidad en Internet. La NSA según las Revelaciones de Snowden*. Universidad de Buenos Aires, Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería. 2017, p. 17. Disponible en: http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-0938_BonifazR

individuos. El desarrollo tecnológico ha potenciado la vigilancia masiva, lo que ha permitido que incluso sea realizada por cualquier persona y en contra de cualquier persona, la vida privada ya no queda aislada de la vida pública, por lo que se llega a conocer aspectos privados con mayor facilidad y exactitud, habiendo una intromisión en las esferas personales de las personas, lo que constituye una afectación grave al derecho a la intimidad.

Cualquier sistema que genere y recopile datos sobre individuos sin intentar limitar el conjunto de datos a personas definidas como objetivos de vigilancia es una forma de vigilancia masiva, entendiéndolo entonces como la red completa de búsqueda de información que se ejerce sobre una importante parte de la población. Su fundamento sería la seguridad nacional de un país, por lo que la injerencia en estos casos está justificada, tal como señala el artículo 8.2[3] del Convenio Europeo de Derechos Humanos.

Usualmente esta vigilancia es selectiva, pues solo se puede llevar a cabo ese seguimiento si está dirigido a una persona o a un grupo por motivos legítimos concretos. Para que las autoridades entren a esa esfera de la privacidad es necesario que tengan el permiso de un juez, y esto solo si se sospecha que la persona está implicada en actividades delictivas.

Si este seguimiento es a gran escala y de manera indiscriminada, es decir sin una sospecha razonable de que exista una actividad delictiva por parte del sujeto que altere el orden público, entonces la presunción de que todos son inocentes hasta que se pruebe su culpabilidad, no tendría vinculación alguna y debería reformularse a que todo el mundo es potencialmente culpable hasta que se demuestre que es inocente.

En junio de 2013 Edward Snowden filtró millones de documentos que revelaban cómo las agencias de seguridad estatales utilizaban la vigilancia masiva para recoger, almacenar y analizar en secreto millones de comunicaciones privadas de personas de todo el mundo[4]. Además, proporcionó información que sugiere que el Reino Unido y los Estados Unidos han puesto en marcha programas de vigilancia masiva en alianza con sus socios Canadá, Australia y Nueva Zelanda, a esta alianza se le denomina “Los Cinco Ojos”.

Estos países controlan de manera ilegal e indiscriminada los correos electrónicos, llamadas de teléfono y cualquier forma de comunicación en la que se requiere el uso de

---

[3] Artículo 8. Derecho al respeto a la vida privada y familiar:
[...] 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[4] Estas revelaciones pusieron en jaque a muchos gobiernos y abrió los ojos a la sociedad del poder que ostenta la vigilancia masiva realizada con herramientas tecnológicas, lo que llevó a que se inicien demandas y litigios internacionales.

Internet a personas en todo el mundo. Entonces, ¿dónde queda la intimidad de las personas? En una sociedad en la que no se respete la intimidad de las personas, no existe libertad de manera plena. Es por ello que en este trabajo analizaremos si está constitucionalmente permitido que los gobiernos se inmiscuyan en la esfera privada de las personas en aras de la búsqueda de la seguridad nacional y, de ser el caso, cuáles serían los límites razonables.

1.2 Datos masivos, seguridad nacional y rastro digital. Conflicto entre privacidad y seguridad

1.2.1 *Datos masivos*

Los datos masivos, o también conocidos como *big data* o datos a gran escala, si bien no existe un significado genérico es un "término que describe el procesamiento de *big data* usando algoritmos matemáticos para determinar correlaciones entre ellos, predecir tendencias y tomar decisiones"[5].

El Parlamento Europeo no hace tanta referencia a "datos masivos", sino a "macrodatos": "Recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones"[6].

Al hablar de *big data*, encontramos las siguientes características: velocidad, veracidad, volumen, valor y variedad. El volumen, una característica clave para este significado, se refiere a la gran cantidad de datos que se generan, procesan y almacenan a nivel macro internacional de magnitudes incomprensibles para la mente humana. La velocidad se relaciona con la rapidez que se generan y propagan los datos a través de la web. La variedad es entendida en dos campos distintos: el primero a razón de la variedad de las distintas fuentes de territorio que pueden tener origen los datos y lo segundo a que existen diferentes tipos de datos, ya sean estructurados, semiestructurados y no estructurados. La veracidad se refiere a la exactitud de los datos recolectados, donde se trata de eliminar la mala interpretación de estos y mejorar la calidad de ellos. Por último, el valor de los datos tiene que ver con la generación

---

5 MAYER-SCHÖNBERGEr V. y CUKIER. K. *Big Data. A Revolution That Will Transform How We Live, Work, and Think*. (A. Iriarte, Trad.) Madrid: Turner Publicaciones S.L. Primera edición. 2013. ISBN: 978-84-15427-81-0. Disponible en: http://catedradatos.com.ar/media/3.-Big-data.-La-revolucion-de-los-datos-masivos-Noema-Spanish-Edition-Viktor-Mayer-Schonberger-Kenneth-Cukier.pdf

6 FIGUEROA FRANCISCO, J.M. *Inteligencia artificial, big data y derecho sanitario: reflexiones a la luz de los derechos fundamentales* [trabajo fin de grado en derecho]. Universidad de Cantabria, Santander. Facultad de Derecho. Santander. 2022. p. 30 Disponible en: https://repositorio.unican.es/xmlui/bitstream/handle/10902/26234/FIGUEROAFRANCISCOJAVIERAMONTSERRAT.pf?sequence=1

de valor a partir de los datos iníciales, de manera que desde este punto se logre realizar un correcto procesamiento de datos al menor costo y obteniendo una información útil. Sin desmedro de lo anteriormente mencionado se destaca el valor potencial presente y futuro de los datos recolectados; además de la veracidad de estos, pues no pueden ser manipulados, analizados, procesados con mecanismos o procesos tradicionales.

Un ejemplo de órgano de captación de datos masivos es la Agencia de Seguridad Nacional de los Estados Unidos (en inglés: *National Security Agency*, o, por sus siglas, NSA). Esta Agencia es la encargada de recolectar toda la información de manera global, con fines de inteligencia, por medio de cables de fibra óptica, comunicaciones satelitales y telefonía celular. Las grandes empresas de Internet entregan los datos de sus usuarios a esta Agencia y si esto no es suficiente para obtener toda la información que la misma requiere, se recurre a los ataques informáticos para buscar la información restante.

Las comunicaciones recolectadas son procesadas en sistemas sofisticados. Los mismos permiten a los analistas de la Agencia de Seguridad Nacional de los Estados Unidos encontrar información a través de buscadores similares al navegador de *Google* e intervengan sobre las comunicaciones privadas de quiénes usan Internet. También recolecta datos y metadatos: los primeros son el contenido de las comunicaciones, mientras que los segundos describen ese contenido. Por ejemplo, en el caso de una llamada telefónica, los datos son el audio de la conversación. Los metadatos son los números de teléfono de los intervinientes en la llamada, la hora en que se realizó, el tiempo en que duró, y datos relevantes. Los metadatos son almacenados por un tiempo mayor que los datos ya que permiten tener un contexto sobre las comunicaciones y ocupan menos recursos de almacenamiento.

El daño individual producido por el mal uso de los datos masivos puede ser imperceptible para el derecho a la intimidad desde la perspectiva del individuo titular del derecho, pero puede afectar a gran escala este derecho fundamental de grupos sociales de una manera relevante. De la misma forma que el internet cambió radicalmente el mundo, los datos masivos modificarán diversos aspectos fundamentales de la vida, por lo que esto nos invita a tener una mejor preparación y así aprovechar de una manera positiva las tecnologías, lo que nos cambiará a nosotros y a nuestras instituciones.

Lo que sí podemos decir es que con los datos masivos se accede invasivamente a información privada, el tratamiento que se les da a estos es un secreto, por lo que al *big data* se le debe regular de manera más estricta, es decir; establecer directrices, normativas, lineamientos y directivas, para así evitar su uso poco ético, contrario a los derechos

fundamentales y principios, en especial los vinculados con la privacidad e intimidad, así como fortalecer las garantías de cada persona.

1.2.2 *La vigilancia masiva como mecanismo para garantizar la seguridad nacional*

Los gobiernos han sacado provecho de estos datos masivos y de las nuevas herramientas tecnológicas con la finalidad de garantizar la seguridad nacional y así enfrentar diversos delitos que la pongan en riesgo, pero para tener un panorama más claro debemos saber que se entiende por seguridad nacional.

Para Espinosa "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"[7]. En la misma línea encontramos que la definición de seguridad nacional "es un concepto que ofrece dificultades para definirlo y que cada Estado, lo debe establecer en función de las realidades que observa en su desarrollo político, económico, social, y militar"[8]. Asimismo, la definición de seguridad nacional "varía de acuerdo con las amenazas que en materia de seguridad enfrentan los Estados, a los intereses que buscan proteger en cada época y a las políticas públicas de defensa exterior, y en algunos casos de seguridad interior"[9]. Sin embargo, muchas veces se ha buscado dar una definición objetiva y delimitar el concepto de seguridad, es así que encontramos una pluralidad de conceptos.

Para Muñoz la seguridad nacional "se manifiesta como un proceso continuo e incesante, es la condición política, económica, social y militar que garantiza el desarrollo y la estabilidad de un Estado. Permite el equilibrio necesario para asegurar, mediante la aplicación del poder nacional, la obtención y el mantenimiento de los objetivos nacionales, previniendo y actuando ante cualquier amenaza interna o externa que ponga en peligro los intereses de la sociedad"[10]. En el año 2003 se llevó a cabo la tercera sesión plenaria de la Organización de

---

7 ESPINOSA, P. Vigilancia masiva: Conflicto entre seguridad nacional, derecho a la protección de datos personales y vida privada. *Revista Cálamo*, 13, 2023, p. 132. Disponible en: https://doi.org/10.61243/calamo.13.167

8 VASOLI, M. J. Seguridad Nacional o Defensa Nacional: La implicancia de la tecnología en el planeamiento del Sistema de Defensa Nacional. *Red de Seguridad y Defensa de América Latina.* 2002. Disponible en*:* https://www.resdal.org/Archivo/d0000271.htm

9 BERTONI, E.; LANZA, E.; MAS, M. y TORRES, N. *Seguridad Nacional y Acceso a la Información en América Latina: Estado de situación y desafíos*. Documento preparado por Centro de Archivos y Acceso a la Información Pública (CAinfo) con la asistencia técnica del Centro de Estudios para la Libertad de Expresión y Acceso a la información (CELE) de la Facultad de Derecho de la Universidad de Palermo, Argentina, 2012, p. 14. Disponible en: https://www.palermo.edu/cele/noticias/acceso-informacion-seguridad-nacional.html

10 MUÑOZ PETERSEN, B. A. *La corrupción como amenaza a la seguridad nacional tras la transición democrática en México*. Tesis de licenciatura en Relaciones Internacionales. Universidad de las Américas

Estados Americanos, donde adoptaron la Declaración sobre Seguridad en las Américas, estableciendo lo siguiente en el numeral 2 de la segunda declaración denominada Valores compartidos y enfoques comunes: "Nuestra nueva concepción de la seguridad en el Hemisferio es de alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio, incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, y se basa en valores democráticos, el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional".

En el Perú también se ha buscado regular y definir este concepto. La Constitución ha establecido en su capítulo XII la seguridad y defensa nacional, es así que recoge en el artículo 163 lo siguiente: "El Estado garantiza la seguridad de la Nación mediante el Sistema de Defensa Nacional (…)". Asimismo, el Tribunal Constitucional se ha pronunciado sobre el concepto de seguridad nacional diciendo que "la Constitución, sin embargo, caracteriza a la *Seguridad Nacional* como un **bien jurídico** íntimamente vinculado a la *Defensa Nacional*, más que a la seguridad ciudadana o al llamado orden público interno"[11] (el énfasis es nuestro). También establece una distinción entre seguridad nacional y seguridad ciudadana:

> El concepto de *Seguridad Nacional no debe confundirse con el de seguridad ciudadana*. Aquélla implica un peligro grave para la integridad territorial, para el Estado de Derecho, para el orden constitucional establecido: es la violencia contra el Estado y afecta los cimientos del sistema democrático, como se expresó en la vigésima cuarta reunión de ministros de Relaciones Exteriores de la Organización de Estados Americanos, este 20 de setiembre de 2001. Supone, pues, un elemento político o una ideología que se pretende imponer, y sólo puede equipararse a la *seguridad ciudadana* por excepción o emergencia, cuando ésta es perturbada gravemente. La *seguridad ciudadana* normalmente preserva la paz, la tranquilidad y la seguridad de los ciudadanos, sin mediar el factor político y/o el trasfondo ideológico en su vulneración. Quien delinque contra la *seguridad ciudadana*, no se propone derrocar o amenazar al régimen político constitucionalmente establecido, a fin de imponer uno distinto o una distinta ideología[12].

Puebla, Departamento de Relaciones Internacionales e Historia. Escuela de Ciencias Sociales. 2005, p.32. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/

11 Expediente 005-2001-AI/TC, f.j. 2.

12 Ibídem.

De igual manera encontramos que se la define como un servicio público: "la Seguridad Nacional es un servicio público objeto de una Política de Estado, es responsabilidad del Gobierno, que, bajo la dirección y liderazgo del Presidente de la Republica implica a todas las Administraciones Públicas y precisa la colaboración de la sociedad en su conjunto"[13]. También encontramos una definición en el Decreto Supremo N° 005-2021-DE, que aprueba la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030, la cual la define como la "situación que alcanza el Estado en la que tiene garantizada la soberanía, independencia e integridad territorial, el Estado constitucional de derecho, la paz social y los intereses nacionales; así como la protección de la persona humana y los derechos humanos, mediante acciones de naturaleza diversa y carácter multidimensional, que permitan hacer frente a las amenazas y las preocupaciones, con la finalidad de crear las condiciones propicias para el bienestar general".

Habiendo dicho esto, podemos decir que, si bien no hay uniformidad sobre el concepto de seguridad nacional, ya que es un término que se encuentra en constante evolución, cada Estado tiene la obligación de determinar su concepto de acuerdo a las amenazas que perciben y a su desarrollo político, económico, social y militar, es así que el Estado Peruano ha buscado otorgarle una definición para garantizar su plena protección, promoviendo así el respeto por la persona humana, su paz, tranquilidad, derechos y libertades.

Es por esto que, en el Perú, así como en otros países; surge la figura de la vigilancia masiva como un mecanismo para preservar la seguridad nacional y estabilidad del Estado, y brindar una "respuesta a los ataques y peligros contra la seguridad nacional, con la utilización de tecnologías que permiten a los gobiernos escuchar las llamadas telefónicas, escanear las redes de datos, leer correos electrónicos y mensajes de texto, seguimiento de personas, incluso cambiar el contenido de los mensajes"[14].

Inicialmente la vigilancia solo se realizaba entre Estados, pero eso ha evolucionado, ya que ahora se ha extendido a la población y esto pone en peligro la intimidad de las personas, situación que se ha visto aumentada con la utilización de la tecnología. Esta vigilancia masiva, aparte de atentar contra los derechos y libertades de los ciudadanos, crea una gran inseguridad, especialmente a las empresas o personas que trabajan con banco de datos.

---

13 SECRETARÍA DE SEGURIDAD Y DEFENSA NACIONAL (SEDENA), 2015. *Doctrina de seguridad y defensa nacional.* Lima. p. 51. Disponible en: https://www.esup.edu.pe/wp-content/uploads/2021/01/8.%20Doctrina%20de%20Seguridad%20y%20Defensa%20Nacional%202015.pdf

14 GONZÁLEZ PORRAS, A.J. *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, Departamento de Ciencia Jurídica y Derecho Público. 2016. p. 22. Disponible en: https://hdl.handle.net/10578/10092

La idea que se presentó en materia de seguridad es intentar saber cuándo se van a producir determinados delitos para así poder evitarlos. Esto es normalmente lo que hace la Agencia de Seguridad Nacional, cuyos planes secretos de espionaje masivo y selectivo fueron de conocimiento gracias a la revelación de información realizada por Edward Snowden. Los atentados terroristas del 11 de setiembre fueron un punto de inflexión que hicieron comprender, no sólo a Estados Unidos sino a todo el mundo, que eran totalmente vulnerables. Esto trajo como consecuencia que Estados Unidos desarrolle una política de seguridad, para mantener el orden frente a la agresión sufrida. Se implementaron leyes y directrices de seguridad, la mayoría de estas generaban un menoscabo en las libertades civiles, ejemplo de ello es la *Patriot Act* o ley "Patriot" la cual "violaba cinco de las diez enmiendas de la Constitución: la libertad de expresión y reunión, la protección frente a registro y detenciones arbitrarias, el respeto de las garantías legales, el derecho a juicio público y la protección frente a castigos crueles e inusuales. […] además, se aprobaron decretos en los que se establecían tribunales militares para juzgar a extranjeros sin posibilidad de que éstos pudieran recurrir su sentencia ante la justicia civil. También se expandieron los poderes de vigilancia del gobierno reduciendo los criterios mínimos exigibles para su autorización y limitando la competencia de los tribunales a la hora de autorizar el espionaje"[15]. La situación de amenaza nacional llevo a que todas estas leyes fueran aceptadas, pese a que recortaban los derechos civiles de las personas.

El Estado Peruano no ha sido ajeno a esta problemática, ya que entre la década de los 80 hasta finales de los 90 fue el escenario propicio para el desarrollo pleno de las actividades de vigilancia masiva, teniendo como fundamento la seguridad nacional. La vigilancia era ejercida por los servicios de inteligencia del Estado, cuyo sustento a dichas prácticas era el momento convulsionado por el que pasaba el país debido al terrorismo. Se recolectaba información que sirviera para descabezar las estructuras organizativas, y evitar tácticas de contrainsurgencia basadas en la violencia indiscriminada que en el pasado habían distanciado a la población rural de las Fuerzas Armadas y el Estado Peruano. Si bien estos mecanismos ayudaban a aminorar el panorama, personas involucradas políticamente dieron un mal uso del sistema de inteligencia, utilizándolos de este modo para fines personales y acusando a muchas personas inocentes.

---

[15] PALOMO GARRIDO, A. La lucha antiterrorista y el nuevo sistema de seguridad internacional tras el 11 de septiembre: ¿una consecuencia lógica? *Foro Internacional*. México: Vol. 56, n° 4, 2016. p. 945. Disponible en: https://doi.org/10.24201/fi.v56i4.2379

El justificativo de la vigilancia masiva es hacer frente a actividades delictivas, especialmente a las vinculadas al terrorismo y en un mundo interconectado gracias a los avances tecnológicos, es de suma importancia para las autoridades tener acceso a datos que permitan identificar personas con posibles conductas delictivas y anticiparse a la amenaza que genera, garantizando así la paz social y armonía. Sin embargo, esta recopilación de datos puede llegar a no diferenciar a personas que sí cometen delitos con las que no los cometen, involucrando a personas inocentes y vulnerando así sus derechos y libertades.

El gran problema es que cuando se hace un mal uso de este mecanismo, se utiliza como una "excusa para otros propósitos no autorizados, como espiar contrarios políticos, conocer las costumbres de los consumidores, averiguar datos para extorsionar a ciertos personajes relevantes, (…)"[16]. Esta vulneración se acrecienta más a través del Internet, atentando contra "derechos, bienes e intereses jurídicos, con especial referencia a derechos como la intimidad, imagen, la libertad sexual, la dignidad y el honor de las personas; así como también afectaciones a bienes e intereses jurídicos como la propiedad intelectual e industrial y la seguridad nacional y el orden público"[17].

Tiene que existir una transparencia en la utilización de la vigilancia masiva de tal manera que los ciudadanos tengan una garantía de los fines con los que se está utilizando, qué datos se están utilizando y a quien se está vigilando. Los Estados y las empresas tienen que trabajar en conjunto: las empresas como suministradoras de datos solo en las ocasiones donde haya una amenaza real a la seguridad nacional, y, por otro lado; evitar que los Estados obliguen a las empresas que tengan que suministrar este tipo de datos obligatoriamente. Es por esto que existe el desafío de equilibrar la seguridad nacional con la protección de los derechos individuales, debido a que cuando se utiliza este mecanismo se termina afectando también, en muchos casos; la intimidad de las personas.

1.2.2.1 La Agencia de Seguridad Nacional y la alianza de los «Cinco Ojos». La Agencia de Seguridad Nacional de los Estados Unidos se encarga de recopilar y analizar señales de inteligencia que contienen información sobre los adversarios y pueden ayudar a determinar donde se encuentran, que están planeando y que tipo de armas están usando; todo esto con el fin de garantizar la seguridad nacional. Pero para tener un panorama más amplio

---

16 GONZÁLEZ PORRAS, A.J. *Privacidad en internet*. p. 529.

17 RIBAS, J. 1996. Aspectos legislativos de las autopistas de la información: Delitos en Internet. *Jornadas Profesionales Informat-96*. Barcelona, citado por PEREZ LUÑO, A.E., "Impactos sociales y jurídicos de internet". Argumentos de razón técnica". *Revista Española de Ciencia, Tecnología y Sociedad, y Filosofía de la Tecnología* (1) 1998, pp.33-48.

del trabajo que realiza esta agencia, es necesario realizar un pequeño resumen histórico del origen y sucesos más importantes que la han marcado a lo largo de su existencia.

El 20 de mayo de 1949, el entonces secretario de defensa de los Estados Unidos, Luis A. Johnson creó la Agencia de Seguridad de las Fuerzas Armadas. Su propósito era el de coordinar todas las comunicaciones electrónicas y trabajos de inteligencia de las diferentes agencias pertenecientes a las Fuerzas Armadas, como por ejemplo el Servicio de Seguridad de las Fuerzas Aéreas o el Grupo de Seguridad de la Marina. Sin embargo, la Agencia de Seguridad de las Fuerzas Armadas fue un rotundo fracaso debido a la gran rivalidad que existía entre las diferentes agencias, lo que tenía como consecuencia que nunca compartieran información.

Por este motivo, y dado que la Agencia de Seguridad de las Fuerzas Armadas quedó totalmente inoperativa e incapaz de responder a las necesidades que planteaba la Guerra Fría, el presidente Truman autorizó la creación de una nueva agencia secreta, que se llevó a cabo mediante un memorándum confidencial, que ni siquiera el Congreso sabía de su existencia. Es así que el 4 de noviembre de 1952 nació la Agencia de Seguridad Nacional de los Estados Unidos (en adelante la Agencia), entidad que fue puesta en marcha directamente por el poder ejecutivo, es decir por el gobierno de los Estados Unidos.

Durante décadas la Casa Blanca realizó un minucioso trabajo que la hizo pasar totalmente desapercibida y no se supo de ella hasta más de veinte años después gracias a unas investigaciones llevadas a cabo en 1975 por el Senado (después de sucedido el escándalo Watergate) sobre los posibles abusos de los servicios de inteligencia. Fue entonces que el Senado conformó un comité especial al que se le denominó Comité Church (llamado así porque quien lo presidía era el senador Frank Church), el cual desveló que existía una agencia con un presupuesto multimillonario, agencia de la que nadie había oído hablar. Este comité también descubrió que la Agencia se había dedicado a interceptar las conversaciones de casi 1700 norteamericanos en 1969 bajo la administración del presidente Nixon, administración que llegó a poner nombre a esta particular lista de personas a vigilar, conocido como el proyecto Minaret: personajes destacados de la época como Martin Luther King, Jane Fonda o Muhammad Ali, todos ellos personas contrarias al gobierno, promotoras de derechos civiles o que estaban disconformes con la Guerra de Vietnam. Incluso se dedicaron a espiar o vigilar a gente de la entera confianza del presidente Nixon[18].

[18] UNITED STATES SENATE. Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Internet Archive, 1976. Disponible en: https://archive.org/details/finalreportofsel01unit

En 1978, después de conocido todo este caso, el congreso aprobó la Ley de Vigilancia de la Inteligencia Extranjera (en inglés: *Foreign Intelligence Surveillance Act*, o, por sus siglas, FISA). Esta ley puso un freno legal para que la Agencia escuche las comunicaciones de las personas de manera libre y solo podía interceptar comunicaciones que tuvieran lugar en el extranjero, prohibiendo la vigilancia en suelo estadounidense, salvo en aquellos casos donde las personas actúen como espías de otros países. Desde la aprobación de la Ley de Vigilancia de la Inteligencia Extranjera, para poder iniciar el monitoreo de un ciudadano la Agencia necesita la aprobación mediante una orden judicial. Sin embargo, los acontecimientos que suscitaron el 11 de setiembre del 2001 cambiarían por completo los límites de la Agencia.

Estos atentados marcarían un antes y un después en la Agencia. Más de dos décadas después de ese trágico día, podemos decir que es el atentado terrorista que más consecuencias ha desencadenado en toda la historia de la humanidad. El congreso le dio vía libre al entonces presidente George Bush para poder utilizar a las Fuerzas Armadas de la forma que considere necesaria para perseguir y castigar a todo aquel que hubiera estado implicado en los atentados. Un mes después de los atentados el congreso aprobó la *Patriot Act* o ley "Patriot", que daba la potestad a los cuerpos de seguridad para luchar contra el terrorismo con las mismas tácticas con las que luchaban contra el crimen organizado o el narcotráfico. Ejemplo de esto es que los agentes podían conseguir acceso a los datos personales, historial de llamadas, planes de viaje o cualquier otra información disponible en otras agencias federales de un sospechoso de terrorismo.

En el 2002, el presidente Bush firmó una orden presidencial que permitía a la Agencia monitorizar las llamadas y los correos electrónicos de miles de ciudadanos y residentes legales en los Estados Unidos sin la necesidad de una orden judicial. Es así que surgió el programa Stellarwind.

El 01 de agosto del 2005, el general Keith Alexander asumió las riendas de la Agencia siendo la persona con mayor tiempo en el cargo y quien además obtuvo gran poder. Durante su mandato uno de sus objetivos principales fue renovar tecnológicamente la Agencia y reclutar a personas jóvenes, ya que era inminente la llegada de la era digital. Es así que el general Alexander llevó a cabo nuevos programas de vigilancia, siendo el más controvertido el programa PRISM. Con este programa la Agencia comenzó a almacenar información de Internet y de compañías tecnológicas (entre ellas se encontraban Google, Apple, Facebook,

Microsoft, YouTube) que permitieran encontrar amenazas terroristas. Se estima que la Agencia almacenó información de decenas de millones de estadounidenses[19].

En el año 2013, una filtración de un consultor tecnológico, un hasta entonces desconocido Edward Snowden, hizo temblar las bases del poder en Washington. A través de periodistas del The Washington Post y The Guardian, el ex empleado de la Agencia filtró documentos clasificados como alto secreto que revelaban la existencia de varios programas de inteligencia, los mismos que recolectaban metadatos de ciudadanos estadounidenses de forma masiva. Todo este actuar trascendió fronteras, ya que con la filtración se conoció también que se interceptaban llamadas, correos electrónicos, mensajes de otros jefes de Estado.

El 02 de junio del 2015 se promulgó la Ley de Libertad de Estados Unidos (en inglés: *USA Freedom Act)* que impone limitaciones a la recopilación de datos a través de las herramientas de telecomunicaciones sobre ciudadanos estadounidenses y que debilitó en gran magnitud la capacidad de acción de la Agencia, la misma que anunció a principios del 2019 la suspensión del programa PRISM por el cual las operadoras telefónicas tenían que pasarle los registros de sus clientes.

Asimismo, la Agencia promueve intereses y alianzas con todo el mundo, ya que así ayuda contrarrestar la proliferación de armas químicas, biológicas y nucleares, o frustrar el ingreso de sustancias ilegales a territorio norteamericano. La alianza más conocida es la llamada alianza de los "Cinco Ojos"[20], y de la que para hacer mención tenemos que rememorarnos hacia el siglo XX, específicamente la Segunda Guerra Mundial. Esta se encontraba en su punto más convulsionado, por lo que Estados Unidos y Reino Unido estrechaban sus relaciones de colaboración con la suscripción del acuerdo llamado UKUSA, esto con la idea de terminar la expansión que venía desarrollando la Alemania nazi en Europa y el mundo.

La idea que tenían estos dos países era que se interceptaran las comunicaciones del ejército nazi y sus aliados, y así poder adelantarse a sus maniobras militares para derrotar a Hitler y dar fin a las acciones bélicas que afectaban a todo el mundo. Una vez finalizada la Segunda Guerra Mundial, esta alianza continua e inició la llamada Guerra Fría, la cual consistía justamente en un espionaje y vigilancia mundial.

Así poco a poco la Alianza fue involucrando a otros países, llegando a integrarse tres países más y recibió el nombre de la alianza de los "Cinco Ojos", conformada en la actualidad

---

19 VISUALPOLITIK. *NSA: la agencia que espiaba a Merkel (Y a otros muchos líderes mundiales)* [video]. *YouTube*. 27 de mayo de 2020. Disponible en: https://www.youtube.com/watch?v=cn7TwjiH4DQ

20 Alianza que estuvo más de 70 años en el anonimato y que llevó a cabo labores de vigilancia militar y diplomática, todo esto en el marco de la guerra fría.

por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda. El principal objetivo de esta alianza es espiar las comunicaciones estratégicas, intervenir las telecomunicaciones y compartir entre ellos la información que logran obtener (inteligencia compartida) para así lograr una supremacía económica, política y social con respecto de los demás países del mundo.

Gracias a la filtración de información realizada por Edward Snowden, quien además mencionó que estos países tenían bases de escucha e intervención satelital en varias partes del mundo, se tuvo conocimiento que los países miembros de esta alianza "son capaces de acceder y procesar inmensas cantidades de comunicaciones de personas totalmente inocentes. Los datos interceptados abarcan toda clase de actividad online incluyendo registros de llamadas telefónicas, contenidos de mensajes de correo electrónico, entradas en Facebook o el historial de accesos a páginas web de cualquier usuario de internet"[21].

Hemos podido observar que los programas que la Agencia implementó y las alianzas que promovió, entre ellas la mencionada alianza de los "Cinco Ojos", más se usaron para fines políticos y personales, redirigiendo su mirada hacia personas u objetivos que en muchos casos no ponían en peligro la seguridad nacional y alejándose en sobremanera de la finalidad para las que fueron creadas.

1.2.3 *El rastro digital*

En un mundo tan digitalizado como en el que nos encontramos, donde nuestra vida está prácticamente en la red, es importante que se conozcan todos los peligros que ello implica y cómo podemos actuar cuando se ha vulnerado alguno de nuestros derechos. Explicaba Tene "debemos tener en cuenta que somos nosotros mismos los que difundimos de manera activa grandes cantidades de información personal en línea, a través de los distintos proveedores de servicios de plataforma que actúan a la vez como facilitadores de flujos de datos"[22]. Rallo sostiene que "cada clic que demos en Internet, cada web que visitemos, incluso cada *like*, se puede transformar en conocimiento y se pueden crear perfiles en función

---

[21] GREENWALD, G. *Sin un lugar donde esconderse: Edward Snowden, la NSA y el estado de vigilancia de EE. UU*, Ediciones B, Barcelona, 2014, p. 149. Disponible en: https://www.proglocode.unam.mx/sites/proglocode.unam.mx/files/Greenwald,%20G.%20(2014)%20Edward%20Snowden%20(red).pdf

[22] TENE, Omar. Reforming data protection in Europe and beyond: a critical assessment of the second wave of global privacy laws. En: RALLO LOMBARTE, A. y GARCÍA MAHAMUT, R., coord. *Hacia un nuevo derecho europeo de protección de datos*. Valencia: Tirant lo Blanch. 2015, pp.143-206, citado en GUEVARA SANMATEO, M. *El impacto del Big Data en la protección de datos personales*. Tesis fin de grado en derecho. Universitat Jaume I. 2018, p. 4. Disponible en: http://hdl.handle.net/10234/175806

de este conocimiento. Perfiles, que pondrán en peligro nuestra privacidad, la reputación y, con esto, la libertad del individuo y su dignidad"[23].

Este rastro, es la llamada huella digital[24], algo que nos define. La huella digital es la materia prima principal de la era digital en la que nos encontramos. Cuando publicas en redes sociales, compras en línea, te suscribes a un diario o boletín informativo, dejamos este rastro digital. Es así que al interactuar con los diferentes servicios que la red nos ofrece, somos nosotros mismos los que generamos ese universo digital.

Al ser partícipes del uso de la red, estamos brindando de alguna manera una autorización tácita para que las diferentes plataformas digitales hagan uso de nuestros datos personales que en principio es nuestra responsabilidad mantener en reserva, pero al hacer uso de la red delegamos esa responsabilidad de nuestras acciones a un aparente determinismo tecnológico y a quienes lo propagan, así como también a quienes pretenden convencernos que no hay nada mejor que delegar nuestra responsabilidad a los algoritmos.

Es imprescindible que reflexionemos al desafío que nos estamos enfrentando y en qué situaciones esta delegación tiene sentido, para así poder determinar a quién estamos finalmente delegando la responsabilidad, cuando los algoritmos no funcionan o funcionan mal y cuando otros sacan provecho de nuestros datos sin nuestro consentimiento.

Debemos ser conscientes de que todo lo que compartimos en la web, quedará en línea y podrá ser usado y controlado por terceros, ya que consideramos a las redes sociales como un diario de nuestra vida privada. Así es como sin saberlo nos exponemos a otras personas y nos convertimos en libros abiertos a los ojos de los seres externos. Este constante y permanente control de la información, mediante algoritmos hace que día a día la *web* nos recomiende productos de nuestro "interés"; ya sea grupos musicales, ofertas de viajes, libros, tecnología, ropa, créditos, etc. Y es que esto lo hacen con toda la información que procesan y almacenan en su base de datos, gracias a los rastros digitales que nosotros dejamos en la red, cuando hacemos uso del navegador. Nuestra identidad digital pasa a ser determinada de manera más o menos implícita, orientándola a un cierto orden y convergencia.

1.3 El impacto de la vigilancia masiva en los datos personales

Habiendo dicho esto, tenemos claro que el derecho a la intimidad es muy importante y necesario, puesto que es parte esencial del desarrollo de la persona, pero en la última década

---

[23] RALLO LOMBARTE, A. *El derecho al olvido en Internet: Google versus España*, 1ª edición, Madrid. Centro de Estudios Políticos y Constitucionales. 2014. p.28, citado en GUEVARA SANMATEO, M., *El impacto del Big Data*. p. 4. Disponible en: http://hdl.handle.net/10234/175806

[24] La huella digital es toda la información nuestra que vamos dejando en la red a medida que interactuamos en ella, recopilada gracias, por ejemplo, a las cookies que favorecen que nuestro ordenador sea único. Es una combinación de valores de datos que permiten identificar a una persona.

se ha tomado conocimiento por noticias nacionales e internacionales, que los gobiernos con ayuda de las agencias de seguridad utilizan los rastros digitales como una herramienta de vigilancia para garantizar la seguridad nacional. Sin embargo, al hacer uso de estos, muchas veces se inmiscuyen en la vida privada de las personas. Es así que ejercen todo tipo de control sobre la actividad que las personas realizan en internet al momento de navegar y en su quehacer cotidiano.

Por esta razón, los Estados basados en una democracia constitucional no pueden pretender controlar a la población a través de vigilancias que atenten contra sus derechos fundamentales, pues este control se traduce en una vulneración. Gonzales nos decía que "una persona bajo vigilancia ya no es libre y una sociedad bajo vigilancia ya no es una democracia"[25].

La defensa de la seguridad nacional es el fundamento que dan los Estados para interferir en la esfera privada de las personas, este sería el fin legítimo que justifica la injerencia en la vida privada (secreto de las comunicaciones). Sin embargo, este argumento no es suficiente, sino que deben justificar que dichas injerencias son necesarias en una sociedad democrática para lograr dicho fin y proporcionadas al fin perseguido.

Cualquier tipo de excepción que permite la disminución de garantías fundamentales en un Estado debe ser informada y acordada de conformidad con las reglas y lineamientos generales que sirven de guía en los casos en los cuales no existe otra posibilidad que ejecutar medidas que afecten derechos fundamentales. Es indudable que los intereses particulares ceden ante los intereses colectivos, sin embargo, en los casos de vigilancia masiva los derechos afectados son los de una gran masa de personas.

Para el Tribunal Constitucional "todos los derechos fundamentales pueden ser objeto de limitaciones o restricciones en su ejercicio. Pero, cuando ello se haga, tales límites no pueden afectar el contenido constitucional de ellos, pues la limitación de un derecho no puede entenderse como autorización para suprimirlo"[26]. Para esto, tenemos que analizar el caso en concreto para determinar dichas limitaciones en su ejercicio. Habiendo señalado esto, podemos decir que es necesario que exista un equilibrio entre la vigilancia masiva, que es el derecho a la seguridad nacional y el derecho a la intimidad, en caso de una eventual discrepancia entre ambos.

De lo mencionado, inferimos que cuando esas medidas dejen de ser necesarias, deberán restituirse los derechos que fueron suspendidos a su protección original. Si bien es

---

25 GONZÁLEZ PORRAS, A.J. *Privacidad en internet*, p. 541.

26 Expediente 0905–2001–AA/TC, f.j. 09.

cierto que todo individuo tiene derecho a la seguridad, también tiene derecho a desarrollarse como sujeto de derecho en un ámbito de privacidad.

Es por ello que la vigilancia masiva debe hacerse a partir de indicios razonables, que justifiquen su actuación, porque de lo contrario la persona podrá sentir que su esfera de privacidad está en peligro de ser vulnerada y termina erosionando la libertad que toda persona tiene en virtud de su dignidad humana. Por lo tanto, cualquier intervención por parte de los Estados que no se ajuste a los lineamientos antes mencionados será una violación de derechos humanos, en dicho contexto es necesario que se respeten ciertos límites, es decir, esta injerencia del gobierno debe perseguir un fin legítimo y estar prevista por ley. Al final, es la vigilancia selectiva y cuidadosa la que logra los fines de la seguridad nacional y evita el uso de poder extralimitado por parte de los gobiernos. El uso o no uso de los datos personales recopilados será determinado por la inteligencia y los indicios razonables que definirán y van a elegir a los destinatarios de la vigilancia y además justificar esa actividad. En cambio, cuando se tiene la información de cualquiera resulta más fácil aprovecharla para vigilar con otros fines a personas u organizaciones que no son sospechosas de mala conducta.

Asimismo, "los individuos deben tener libertad para proteger su privacidad y por ello se debe asegurar que todos tengan la capacidad de hacerlo"[27]. Se debe determinar qué capacidades hay que fomentar entre la ciudadanía, que barreras se deben imponer y que mecanismos de protección se deben proporcionar para lograrlo. Si bien pueden existir razones legítimas en las que los gobiernos puedan utilizar la vigilancia masiva, ya sea en ocasiones de extorsiones, delitos cibernéticos o para proteger la seguridad de los estados, esta deberá hacerse de acuerdo a ciertos criterios, puesto que supone una injerencia directa al derecho a la intimidad, es así que esta vigilancia debe ser selectiva, basada en conjeturas razonables, que se ajusten y se fundamenten en la ley, necesaria para alcanzar un objetivo legítimo y realizada de manera justa, y no discriminatoria.

1.4 El tratamiento de los datos personales en el auge de la digitalización

El derecho a la protección de datos personales está (y ha estado) íntimamente vinculado con el derecho fundamental a la intimidad. Para asegurar un adecuado tratamiento de los datos personales, los Estados deben adecuar sus normativas existentes e implementar regulaciones adaptadas a las nuevas tecnologías, a fin de que los responsables del manejo de los mismos tengan directrices o lineamientos para "realizar un uso correcto de la información

---

[27] SUÁREZ GONZALO, S. *Big data, poder y libertad. Sobre el impacto social y político de la vigilancia masiva*. Trabajo tesis doctoral. Universidad Pompeu Fabra, Departamento de Comunicación. 2019. Disponible en: http://hdl.handle.net/10803/668235

personal cuando desarrollen y usen nuevas tecnologías, priorizando la protección de los derechos de los titulares"[28]. Esto es una tarea titánica, pero no imposible.

De acuerdo con el principio de pertinencia y necesidad, "los datos personales deberían ser únicamente los que resulten adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior"[29]. Este principio es crucial para la protección de los datos personales y la privacidad de cada una de las personas. Los datos que se recopilen deben guardar una relación razonable con la finalidad para la cual se han previsto, es decir, debe existir un equilibrio entre el interés público en el tratamiento de los datos personales y la protección de los intereses de las personas en su ámbito de privacidad.

De acuerdo con estos principios, los conceptos de "necesidad" y "proporcionalidad" imponen limitaciones al uso, lo que quiere decir que los datos personales sólo deberían usarse para cumplir los propósitos para los cuales han sido recopilados. Tiene que existir una proporcionalidad con el objetivo perseguido, es decir, el uso y tratamiento de los datos se debe ajustar solamente a la recopilación que se hace de los mismos, no para fines distintos, pues un uso arbitrario y malicioso de los mismos puede amenazar la dignidad de las personas.

Debemos considerar que, así como avanza la era digital, debe existir una regulación que se adapte y vaya a la par de esta nueva realidad, estableciendo parámetros necesarios para que se respete el tratamiento de los datos personales, disponiendo cuáles son los límites de actuación para que las compañías que manejan información digital hagan un uso consentido y transparente del mismo.

El derecho de protección de datos personales se sostiene en el consentimiento que otorga su titular, pues solo él tiene la potestad de consentir el uso y tratamiento de sus datos, ya que el consentimiento es esencial en la protección de los mismos, puesto que supone la autorización previa del sujeto activo sobre qué datos serán objeto del tratamiento, además tiene su fundamento inicial en la protección del derecho a la intimidad personal.

Este derecho fundamental depara a su titular una serie de atribuciones de las que destacan un conjunto de derechos llamados Derechos ARCO: Acceso, Rectificación, Cancelación y Oposición.

---

[28] MARTÍNEZ DEVIA, A. La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *Revista La Propiedad Inmaterial*. n° 27 ene-jun, 2019, p. 5. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/6071

[29] DEPARTAMENTO DE DERECHO INTERNACIONAL, *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. Departamento de Derecho Internacional. Secretaria de Asuntos Jurídicos de la Organización de Estados Americanos, Washington. 2022, p. 50

La definición que da la Autoridad Nacional de Protección de Datos Personales (ANPD), sobre la protección que engloba cada uno de estos derechos es la siguiente:

a. "Acceso: entendido como el derecho a saber qué datos personales tienen sobre ti, preguntar cómo los obtuvieron, para qué los utilizaron, con quién los han compartido y todos los detalles de su uso.
b. Rectificación: el derecho a modificar y actualizar tus datos personales, cuando estos sean erróneos, inexactos o incompletos.
c. Cancelación: el derecho a cancelar el uso de tus datos personales cuando la finalidad para la que los entregaste ha concluido, venció el plazo establecido para su tratamiento, revocar el consentimiento.
d. Oposición: el derecho a oponerte al uso de tus datos porque te están generando un perjuicio en diversos ámbitos, situación que se presenta con mayor frecuencia en plataformas digitales"[30].

Estos derechos son atribuciones que provienen del derecho a la autodeterminación informativa, reconocido en el artículo 2.6 de la Constitución, y otorgan una serie de facultades a su titular que sirven de control ante posibles excesos, además permiten al ciudadano tener un panorama sobre sus datos y el tratamiento que a estos se les dan; desde cómo se obtuvieron, el para qué y la forma en la que se están compartiendo y transmitiendo. El ciudadano los ejercita ante el titular de un banco de datos personales y tienen carácter personal.

Sin embargo, esta protección que se brinda a los datos personales se ha ido perdiendo con el avance de la tecnología y esto ha sido en gran parte por las excepciones legales que se han ido dando debido a las nuevas exigencias de consentimiento informado para el acopio de datos. Otro motivo es que las grandes empresas encargadas de recolección de datos se escudan en el interés legítimo del responsable del tratamiento. Por estas razones no es concebible, en modo alguno, creer que existe un efectivo control de la información personal a través del consentimiento y los derechos que lo complementan.

1.5 Datos personales. Legalidad de su uso

Tal como hemos visto en los apartados anteriores, es innegable que las personas deben tener una efectiva protección de sus datos personales, y qué mejor que esta protección se vea reflejada en normativas que regulen su uso. Las normas sobre protección de datos personales

---

[30] AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (APDP). *Directiva de seguridad*. Ministerio de Justicia y Derechos Humanos. Lima: Editora Diskcopy S.A.C. 2013. https://cdn.www.gob.pe/uploads/document/file/1401560/Directiva%20de%20seguridad.pdf

ofrecen a los ciudadanos garantías y mecanismos que son necesarios para la protección y control de sus datos personales. Para garantizar su protección, se establecen obligaciones[31] para una entidad pública, persona jurídica o persona natural que maneje bancos de datos personales.

En el artículo 12[32] de la Declaración Universal de los Derechos Humanos se registra el primer antecedente acerca de la protección de la información personal. Sin embargo, dado el contexto social y político en el que se dio esta norma, no tuvo gran acogida, debido a que muchos países aún se encontraban bajo modelos de gobiernos totalitarios que tenían poco respeto por los derechos de las personas, además la Declaración se dio, en sus inicios, como un ideal orientativo y no tenía un carácter obligatorio. En 1966, se recoge ese mismo lineamiento en el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos. Ambos textos son reflejo de los primeros intentos de los Estados para proteger la privacidad de los ciudadanos prohibiendo cualquier intromisión ilegítima.

Los primeros aportes sobre la importancia del control de la información personal estuvieron dados a través de una sentencia de la Primera Sala del Tribunal Constitucional Alemán, el 15 de diciembre del año 1983, en la que se configura el derecho a la privacidad y a la protección de datos, puesto que se pone de manifiesto la carencia que existía en cuanto a mecanismos jurídicos destinados a la protección del uso debido de los datos personales. Para la creación de estos mecanismos se tuvo como cimiento el derecho a la dignidad humana y al libre desarrollo de la personalidad (que permite el ejercicio de la autonomía moral del ser humano), optando de esta manera por proteger la garantía y la continuidad de las libertades básicas. Es así como surge el llamado derecho de autodeterminación informativa.

Asimismo, tras la sentencia del Tribunal Constitucional Alemán, este concepto vuelve a ser recogido por el Tribunal Constitucional Español en sus sentencias 290/2000 y 292/2000 del 30 de noviembre del año 2000. Resulta necesario citar la STC 292/2000 la cual desarrolla el contenido de este derecho. Al respecto el Tribunal español señala que:

> El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos

---

31 Estas obligaciones están reguladas en el Título IV de la Ley de Protección de Datos Personales- Ley N° 29733.

32 Artículo 12: "*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*".

> poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos[33].

La Asamblea General de la Organización de las Naciones Unidas aprobó el 18 de diciembre de 2013 la resolución 68/167 relativa al derecho a la privacidad en la era digital, con motivo de la propuesta de Brasil y Alemania pidiendo respeto y protección para el derecho a la privacidad. La ONU expresa mediante esa resolución su preocupación por los "efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones"; menciona, en concreto, la "interceptación extraterritorial" y "a gran escala", haciendo clara referencia a la red de espionaje masivo operada por Estados Unidos a través de su Agencia de Seguridad Nacional.

Es necesario un marco legal para proteger la libertad informática del procesamiento automático de datos personales. Y este marco legal está formulado a través de varios documentos como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, las observaciones e informes de la ONU, las directrices de la Organización para la Cooperación y el Desarrollo Económico y la Organización de los Estados Americanos.

Nuestro país no ha sido ajeno a esta realidad. Desde 1993 este derecho fue reconocido en nuestro ordenamiento jurídico al ser reconocido en el artículo 2.6 de la Constitución. Desde entonces, su impulso ha sido importante, en particular por el trabajo de la Autoridad Nacional de Protección de Datos Personales, actualmente absorbida por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que han contribuido significativamente con este logro.

1.5.1 *El derecho a la autodeterminación informativa en el ordenamiento jurídico peruano*

Si buscamos los primeros estivos de lo que ahora conocemos como el derecho a la autodeterminación informativa, este se recoge en nuestro ordenamiento en el inciso seis del

---

[33] STC 292/2000, f. j. 7.

artículo dos de la Constitución de 1993. Se debe reconocer que no se brinda un alcance completo de este derecho y es que este derecho, también llamado hábeas data, reconocido así en otros países latinoamericanos como Chile o Argentina; conlleva a una protección frente a probables abusos derivados de la recopilación y utilización informática de los datos personales y tiene como finalidad "darle la posibilidad a todo sujeto de disponer real y efectivamente de los datos referidos a su persona, de modo que esté en condiciones de poder evitar extralimitaciones en el ejercicio de la tecnología informática aplicada a la organización y tratamiento de sus datos personales"[34], proporcionando al posible afectado, desde un punto de vista jurídico, las siguientes atribuciones o facultades:

a. Acceso a todo tipo de información que esté relacionada con su persona o su entorno, ya sea a archivos o base de datos.
b. Actualización de los mismos, además el posible afectado o titular tiene la facultad de rectificar o aclarar la información sobre datos erróneos.
c. La exclusión o eliminación de datos que este considere que son de carácter privado y de todos los datos que crea que no deben ser objeto de recopilación
d. Por último, la confidencialidad de los mismos, el sujeto titular de derecho está plenamente facultado para oponerse a la trasmisión o difusión de los datos que el considere de carácter reservado.

Sin embargo, el texto contenido en el artículo 2.6 de la Constitución del 93, solamente se reduce a establecer que "toda persona tiene derecho (...) a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". En todo caso se debe precisar que este artículo contiene una regulación limitante, para lo que ahora vivimos, dado que al momento de la creación de esta norma no se contaba con todos los avances tecnológicos e informáticos que hoy tenemos. Es así como en la sustentación del presidente de la Comisión de la Constitución del Congreso Constituyente Democrático, el Dr. Carlos Torres y Torres Lara, sostuvo lo siguiente:

> Se trata de una importante innovación que no contiene nuestra Constitución, y que, si la contienen algunas constituciones modernas, como la de Brasil, especialmente, y, de modo parcial, la de España o la de Portugal. Cuando se elaboró la Constitución de 1979, todavía no se advertía la revolución de la informática que se estaba produciendo en el mundo (…) hemos llegado a la conclusión de que la obtención de la información

[34] CASTILLO CORDOVA, Luis. *La finalidad del derecho de autodeterminación informativa y su afianzamiento a través del hábeas data*. *Transparencia, información pública, datos personales.* 2012. Disponible en: https://sumaciudadana.wordpress.com/2012/07/31/la-finalidad-del-derecho-de-autodeterminacion-informativa-y-su-afianzamiento-a-traves-del-habeas-data/

> y su conservación no es el problema fundamental, sino la comunicación de esta información. Mucho más daño se hace comunicando una información negativa sobre una persona que simplemente acumulándola. En consecuencia, la protección que debe dar la Constitución es que nadie pueda transmitir informaciones que estén referidas a la intimidad personal a través de los medios comunes; por tanto, el derecho de cualquier persona a proteger su propia intimidad tiene que llevar a impedir que se transmita información que va contra su intimidad personal[35].

Queda en evidencia que este artículo tenía mucha influencia extranjera, puesto que nuestro órgano constitucional tenía muy poco o nada de conocimiento sobre lo que este derecho engloba, centrándose únicamente a restringirlo y limitarlo solo a la prohibición de transmitir información sobre datos personales de carácter íntimo. Con el fin de reforzar esta protección se instituye el proceso constitucional de habeas data regulado en el artículo 200 inciso 3, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución.

Sobre el reconocimiento del derecho a la autodeterminación informativa, la jurisprudencia ha logrado determinar entre sus decisiones adoptadas el objeto de este derecho, su naturaleza y marcar las diferencias que existen con el derecho a la intimidad. Entre las primeras sentencias que se produjeron después de que se haya reconocido este derecho, tenemos al Expediente N° 666-1996-HD/TC, donde en su fundamento jurídico 3 aporta la gran posibilidad de limitar el contenido constitucional, permitiendo la aparición de los Derechos ARCO.

El Tribunal Constitucional señaló en el Expediente N°1797-2002-HD/TC, en el fundamento jurídico 3, que no debe confundirse el derecho a la autodeterminación informativa con el derecho a la intimidad, estableciendo lo siguiente: “El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina *derecho a la autodeterminación informativa* y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el

---

[35] CONGRESO CONSTITUYENTE DEMOCRÁTICO. *Debate Constitucional Pleno 1993* (publicación oficial); julio 1998; tomo I; Págs. 111-112. Disponible en: https://spij.minjus.gob.pe/Textos-PDF/Constitucion_1993/DebConst-Pleno93/DebConst-Pleno93TOMO1.pdf

inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen".

Posteriormente, la sentencia que consolida las facultades de este derecho fundamental y donde se le brinda la facultad al titular de los datos de poder excluir aquella información privada o de carácter íntimo es el Expediente N° 04739-2007-PHD/TC donde se "protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera «sensibles» y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos"[36]. En el Expediente N° 746-2010-PHD/TC, específicamente en los fundamentos jurídicos 5 y 6, el Tribunal considera dentro de las facultades del derecho a la autodeterminación informativa la "posibilidad de tener acceso a la información particular que sea de su interés y poder hacer uso de esta". Asimismo, la Sala del Tribunal Constitucional señala que el "ámbito de protección del derecho fundamental a la autodeterminación informativa comprende un vasto espectro de posiciones *iusfundamentales* que incluso va más allá de lo expresamente regulado en la ley de desarrollo constitucional y el reglamento de esta última, pues el catálogo de facultades del titular del dato personal no es cerrado sino abierto"[37].

Vemos entonces que la finalidad de este derecho es "darle la posibilidad a todo sujeto de disponer real y efectivamente de los datos referidos a su persona, de modo que esté en condiciones de poder evitar extralimitaciones en el ejercicio de la tecnología informática aplicada a la organización y tratamiento de sus datos personales. En buena cuenta, que se logre un verdadero control de la información sobre uno mismo"[38].

En la actualidad, las personas generan y entregan, de manera consciente o inconsciente, información personal, e incluso consienten, de manera voluntaria o involuntaria, el tratamiento de dicha información por parte de los titulares de bancos de datos personales. Esto genera que la esfera personal y la dignidad del ser humano se vea expuesta a los adelantos informáticos que supone el avance de la era tecnológica. Ante esto, las personas deben tener conocimiento que cuentan con herramientas legales, recogidas en la Constitución

---

36 Expediente 4739-2007-PHD/TC, f.j.4.
37 Expediente 00473-2022-PHD/TC, f.j.11.
38 CASTILLO CÓRDOVA, Luis. *La finalidad del derecho de autodeterminación informativa*. 2012.

y que tienen un desarrollo legislativo, como es el caso de la Ley N° 29733, que permiten el pleno dominio y control sobre sus datos personales.

1.5.2 *Ley 29733, Ley de Protección de Datos Personales*

En el 2011, se promulgó la Ley N° 29733, Ley de Protección de Datos Personales. Esta tiene como principal objetivo garantizar la defensa de los datos personales y en ella se establecieron los principios, derechos y obligaciones que deben seguir las personas naturales, entidades públicas o instituciones del sector privado en el tratamiento de los mismos. Estos principios, derechos y obligaciones están recogidos en la Ley en los títulos I, III y IV, respectivamente. Asimismo, se creó la Autoridad Nacional de Protección de Datos Personales (ANPD en adelante), institución encargada de aplicar dicha norma y velar por su cumplimiento. Su reglamento se aprobó mediante Decreto Supremo N° 003-2013-JUS, el 21 de marzo de 2013, en el que se estableció, en la primera disposición complementaria transitoria, un plazo de dos años a las entidades públicas, privadas y personas naturales que trabajan con banco de datos para que se adecúen a esta norma, de lo contrario serían sujetos pasibles de multa.

El artículo 39 de la Ley N° 29733 nos señala que en caso de vulneración a las normas de esta Ley o de su reglamento, las multas que puede imponer la ANPD por infracciones en materia de protección de datos personales oscilan desde 0,5 unidades impositivas tributarias hasta 100 unidades impositivas tributarias. En palabras de Mishima "solo en el 2022, esta institución fiscalizó a 317 entidades e impuso multas por un total superior a S/ 8 millones"[39]. Las disposiciones tanto de la Ley como del Reglamento mencionados alcanzan a todos los privados y a las administraciones públicas. Sin embargo, en éstas últimas el artículo 3, numeral 2 de la Ley, establece que las disposiciones de esta ley no se aplican a los siguientes datos personales: "3.2. A los contenidos o destinados a ser contenidos en bancos de datos de la administración pública, sólo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito".

En cuanto a las personas de titularidad privada, éstas se rigen en su totalidad por la Ley N° 29733 y su reglamento, y son supervisadas por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIDP

---

[39] MISHIMA, M. Multas por infracciones en materia de protección de datos personales pueden ascender hasta S/ 495,000.00. *EY Building a better working world*. 2023. Disponible en: https://www.ey.com/es_pe/news/2023/02/multas-infracciones-proteccion-datos-personales

en adelante), la cual tiene facultades orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras. El artículo XX de esta ley define al titular del banco de datos personales como aquella "persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad".

Sin embargo, estos tratamientos y medidas de seguridad no quedan a la libre determinación del titular, sino que vienen determinadas por la misma ley o por la DGTAIDP. Además, se tiene que considerar la categoría o calidad de información para que en función a eso se otorgue un tratamiento determinado a los datos.

1.5.2.1 Clasificación de categorías en el tratamiento de datos personales y el principio de proporcionalidad descrito en el artículo 7 de la Ley N°29733. Corresponde ahora explicar cómo se encuentran clasificados los datos personales y las consecuencias legales del incumplimiento de la normatividad. En el año 2013, la ANPD junto con el Ministerio de Justicia y Derechos Humanos (MINJUS en adelante) emitió una Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales la cual busca orientar sobre las medidas, condiciones y requisitos que se deben considerar para el cumplimiento de la Ley N° 29733. Esta directiva establece unas categorías especiales de datos personales que son: básico, simple, intermedio, complejo y crítico; las cuales permiten que las entidades públicas y privadas tomen conocimiento de la clasificación de acuerdo a la protección de datos personales. Estas categorías se materializan en:

a) **"Básico**, corresponde a la categoría de menor nivel e incluye a bancos de datos personales que no contengan la información de más de cincuenta personas, número de datos personales no mayor a cinco (nombres, apellidos, DNI, dirección y teléfono), no incluyen datos sensibles y tienen como titular a una persona natural.

b) **Simple**, corresponde a bancos de datos personales que no contengan la información de más de cien personas, el periodo de tiempo del tratamiento para cumplir con la finalidad es inferior a un año, no incluyen datos sensibles y tiene como titular a una persona natural o jurídica.

c) **Intermedio**, corresponde a bancos de datos personales que contienen la información de hasta mil personas, sirven para tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un año, puede incluir datos sensibles y tiene como titular a una persona natural o jurídica.

d) **Complejo**, corresponde a bancos de datos personales que sirven para el tratamiento de los mismos cuya finalidad se cumple en un plazo indeterminado o superior a un año y que

es realizado en múltiples localizaciones (oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares), puede incluir datos sensibles y tiene como titular a una persona jurídica o entidad pública.

e) Crítico, corresponde la categoría de mayor nivel e incluye a bancos de datos personales que sirven para el tratamiento de datos personales cuya finalidad está respaldada por una norma legal y que se cumple en un plazo indeterminado o superior a un año. Asimismo, este tratamiento es realizado en múltiples localizaciones (oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares), puede incluir datos sensibles y tiene como titular a una persona jurídica o entidad pública"[40].

Dicho esto, es importante señalar que existen criterios que justifican la categorización de los bancos de datos, los cuales han sido determinados de la siguiente manera:

a) "Volumen de registros.- Es importante considerar que existe una diferencia importante entre realizar el tratamiento manual de los datos personales de veinte personas que, de un millón, toda vez que se requiere mecanismos, procesos y herramientas diferentes. El tratamiento de altos volúmenes de datos personales requiere, actualmente, el uso de tecnologías de la información, lo cual, incorpora mejoras fundamentales en los tiempos de procesamiento, pero también incorpora un conjunto de vulnerabilidades asociadas a la tecnología utilizada, por lo que los niveles de protección deben ser adecuados y comúnmente son mayores a los de un tratamiento sin tecnologías de la información.

b) Número de datos.- El número de datos personales que se procesa es un criterio a considerar porque incluye un mayor nivel de detalle sobre el titular de los datos personales con o sin la inclusión de datos sensibles.

c) Periodo de tiempo para la finalidad del tratamiento de datos personales.- El tener un periodo de tiempo indeterminado o muy largo, para cumplir la finalidad del tratamiento, implica un aumento en el nivel de seguridad que debe observarse en el almacenamiento que se dé a los datos personales durante el periodo del tratamiento, así como en el nivel de impacto sobre el titular de los datos personales en caso de pérdida de la información, lo que puede conducir a la implementación de mecanismos de recuperación ante desastres o no.

---

[40] AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (APDP), 2013. *Directiva de seguridad.* p. 11

d) La titularidad del banco de datos personales.- Proporciona un criterio de selección que principalmente separa los extremos de las categorías. Es decir, no se le puede asignar a una persona natural una categoría de altísimo nivel porque no dispone de los recursos necesarios, ni será necesario, como regla general, que implemente las medidas más complejas. En el caso de las entidades públicas, se cuenta con la Resolución Ministerial 129-2012-PCM, que las obliga a implementar un sistema de gestión de seguridad de la información. Con lo cual, no se les puede asignar una categoría de menor nivel, debido a que la información que manejan impacta directamente en los titulares de datos personales. Sin embargo, para las categorías simple, intermedio y complejo se pueden tener combinaciones más acordes al tipo de tratamiento que se realice.

e) Finalidad del tratamiento de datos personales respaldada por norma legal.- Tiene especial impacto por ser obligatorio, esto determina el tipo crítico.

f) Múltiples localizaciones.- El acceso o tratamiento distribuido incorpora un nivel de atención especial porque incluye la transferencia de datos entre múltiples locales de tratamiento (ubicaciones diferentes, pueden ser inmuebles diferentes en la misma ciudad o ciudades diferentes), lo que genera complejidad y puede hacerlo crítico.

g) Tratamiento de datos sensible.- Al incluir estos datos se debe tomar medidas de protección como mínimo de categoría intermedio"[41].

Para finalizar, la directiva, ya habiendo explicado las categorías especiales y los criterios que categorizan los bancos de datos, establece la matriz de apoyo para la selección de categoría en el tratamiento de datos personales, donde reúne en un cuadro todo lo anteriormente explicado:

Tabla 1

Matriz de apoyo para la selección de categoría en el tratamiento de datos personales

Ítem	Criterio	Básico	Simple	Intermedio	Complejo	Crítico
1	Volumen de registros, numero de titulares de datos personales que consienten el tratamiento de sus datos (Criterio utilizado para determinar las categorías)	Hasta 50	Hasta 100	Hasta 1000	Indeterminado	Indeterminado
2	Número de datos personales en banco de datos personales que no contienen datos sensibles (Criterio utilizado para determinar el tipo básico)	Hasta 5	Más de 5	Más de 5	Más de 5	Más de 5

41 Ibídem, p. 12.

3	Finalidad del tratamiento de datos personales respaldada por ley o similar (Criterio utilizado para determinar el tipo básico)	No aplica	No aplica	No aplica	No aplica	Aplica
4	Periodo mayor a un (01) año o indeterminado para cumplir la finalidad (tiempo de tratamiento de los datos personales)	No aplica	No aplica	Aplica	Aplica	Aplica
5	Tipo de titular del banco de datos personales: persona natural (Criterio utilizado para determinar el tipo entre básico a intermedio)	Aplica	Aplica	Aplica	No aplica	No aplica
6	Tipo de titular del banco de datos personales: persona jurídica (Criterio utilizado para determinar el tipo entre simple a complejo)	No aplica	Aplica	Aplica	Aplica	Aplica
7	Titular del banco de datos personales del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al banco de datos o se realiza el tratamiento de los datos personales (Criterio utilizado para determinar la categoría compleja a crítica)	No aplica	No aplica	No aplica	Aplica	Aplica
8	El banco de datos personales puede incluir datos sensibles (Criterio utilizado para determinar la categoría entre intermedio a crítico)	No aplica	No aplica	Aplica	Aplica	Aplica»

Nota. Tomado de la Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales (APDP)-2013[42]. *Los colores son para una mejor identificación en el cuadro.

Aunque la Ley señala que su ámbito de aplicación es sólo sobre el territorio nacional, su reglamento dedica tres artículos, del 24 al 26, al flujo transfronterizo de datos, el cual será posible si es que el receptor ofrece garantías similares a la ley peruana o medien tratados bilaterales o se encuentren dentro de una convención. Lo que es distinto a la regulación de la Unión Europea, en la cual es la Comisión Europea la que da directivas que rigen para toda la zona común, haciendo innecesario establecer acuerdos bilaterales para el flujo de datos, incluso para los países que no se encuentren dentro de la zona común, mediante la Directiva 95/46/CE, es más flexible y seguro el flujo transfronterizo, aunque sin perjuicio de lo establecido por la normativa nacional. En el caso Latinoamericano tenemos la Comunidad Andina, sin embargo, la proyección a una legislación y aplicación similar a la de la Comisión Europea es precaria.

1.5.2.2 Regulación en cuanto a las materias excluidas. Como se ha visto en la Ley N° 29733 se establecen determinadas materias que son excluidas del ámbito de su aplicación, como la defensa nacional, seguridad pública y aquellas actividades relacionadas con el ámbito penal en cuanto a la prevención y represión del delito. El fundamento de la exclusión subyace

[42] Ibídem, p. 16.

en el interés general que existe en la realización de dichas actividades, es por eso que en estas materias también están permitidas y legalizadas unas determinadas prácticas de vigilancia, las cuales solamente pueden ser ejercidas por el Estado y dentro de los parámetros de la materia bajo la cual actúan y respetando los derechos fundamentales.

Para concluir, quisiéramos señalar que esta ley prevé además la observancia de otros principios y derechos, cuya vigencia es de decisiva importancia en las democracias. En este sentido, el desarrollo legislativo del derecho a la protección de datos personales es un desafío que exige armonizar los principios de transparencia y publicidad en la gestión de los asuntos públicos y el derecho de acceso a la información pública con la necesidad del derecho de cada persona a la protección de datos personales. Controlar la información que les concierne para proteger su dignidad y libertad. Si bien es necesario y útil el aporte de los ordenamientos jurídicos extranjeros, hay que mirar hacia adentro y no perder de vista el objetivo planteado, que es la eficaz y correcta protección de los datos personales.

1.5.3 *Convenio para la protección de las personas con respecto al procesamiento automatizado de datos personales*

Hace más de cuatro décadas que el Consejo de Europa instauró el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Nos referimos al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, también conocido como el Convenio 108. Este convenio se promulgó el 28 de enero de 1981 en Estrasburgo; y entró el vigor el 1 de octubre de 1985.

El Convenio 108[43] es la primera norma de la comunidad europea que fijó las pautas sobre un modelo común de protección a los datos personales. Esta se dio debido a que, en Europa, la protección de los datos personales se fijó como un "objetivo político y jurídico de la Organización Europea como una manifestación más del respeto de los derechos humanos"[44]. A lo largo de sus siete capítulos y veintisiete artículos ha logrado armonizar y respetar la vida privada de las personas con la libre circulación de información, garantizar a cualquier persona física la correcta atención a sus derechos y libertades fundamentales, en concreto su derecho a la intimidad, además de brindar garantías en cuanto al procesamiento y recolección de datos personales.

---

43 CONSEJO DE EUROPA. OFICINA DE TRATADOS. *Convenio para la Protección de las Personas con respecto al Procesamiento Automatizado de Datos Personales (ETS No. 108)*. Estrasburgo. 1981. Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

44 PAVÓN PÉREZ, J. A. La protección de datos personales en el consejo de Europa. *Anuario de la Facultad de Derecho*. España: Universidad de Extremadura, N°. 19, 2001. p. 238. ISSN-e 2695-7728, ISSN 0213-988X. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=831270

El objeto de este Convenio se recoge en su artículo 1 en estos términos: "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos)"[45]. El capítulo segundo del Convenio recoge una serie de principios básicos para la protección de datos: "principio de lealtad, principio de exactitud, principio finalista, principio de pertinencia, principio de utilización no abusiva, principio del derecho al olvido, principio de publicidad, principio de acceso individual, principio de seguridad, principio de prohibición de tratamiento automático de datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas o de otro tipo, o datos relativos a la salud o vida sexual, a menos que el derecho interno prevea garantías adecuadas"[46]. Estos principios son de mucha utilidad para preservar la esencia, calidad y legalidad de los datos personales y el derecho de acceso a la información.

Es así que el Convenio, a nuestro entender, unifica los valores fundamentales del derecho a la intimidad y el de libre circulación de la información de los datos de carácter personal; dando una serie de sugerencias y recomendaciones jurídicas dirigidas a los Gobiernos sobre temas más necesitados de protección. El ascenso del internet y la facilidad para poder acceder a este ha creado la necesidad de realizar cambios sobre el Convenio 108, puesto que era necesario cubrir ciertos vacíos en cuanto a su ámbito de aplicación, es así que se adiciona a este documento, el Protocolo adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales.

La validez del Convenio 108 ha tenido casi dos decenios antes de haber sido potenciado por el mencionado Protocolo, cuyo texto mejoró la protección y privacidad de los datos personales. Fue adoptado el 23 de mayo de 2001 por el Comité de Ministros del Consejo de Europa, y abierto a la firma el 08 de noviembre del mismo año. Tiene como finalidad aumentar la protección de los datos personales y la privacidad al mejorar el Convenio original de 1981, en los siguientes aspectos: "En primer lugar, prevé la creación de autoridades nacionales de control responsables de garantizar el cumplimiento de las leyes o reglamentos adoptados en virtud del convenio, en materia de protección de datos personales y flujos transfronterizos de datos. La segunda mejora se refiere a los flujos de datos

---

45 Artículo 1 del Convenio para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. *STE 108 – Tratamiento automatizado de datos de carácter personal, 28.I.1981*

46 BRU CUADRADA, E. La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *IDP. Revista de Internet, Derecho y Política*. n° 5, 2007. p.82. Disponible en: https://www.redalyc.org/articulo.oa?id=78812861008

transfronterizos a terceros países. Los datos sólo pueden transferirse si el Estado receptor o la organización internacional puede proporcionar un nivel adecuado de protección"[47].

El Convenio 108 fue actualizado en 2018, dando lugar al Convenio 108+ o Convenio 108 modernizado. Esta modernización se dio con el fin de perseguir dos elementos claves: hacer frente a los retos derivados de la utilización de las nuevas tecnologías de la información y la comunicación; y reforzar su efectiva aplicación. El Convenio 108+ está llamado a convertirse en la norma internacional sobre privacidad en la era digital. Se recomendó a todos los Estados Miembros de las Naciones Unidas que se adhieran a este Convenio, reconociendo así su potencial.

Lo que más destaca del Convenio 108+ es que se reconocen nuevos derechos para los titulares de datos, se amplía el concepto de datos sensibles (pasando a incluir datos genéticos y biométricos), se incorporan requisitos más estrictos respecto a los principios generales sobre tratamiento de datos, como el principio de proporcionalidad, de minimización de datos y licitud, se incluyen condiciones especiales para el tratamiento de datos personales de niños y niñas, mayor injerencia del principio de responsabilidad proactiva, lo que implica mayor obligación para las organizaciones que tratan datos personales, no sólo de cumplir las normas de protección de datos, sino, en especial de demostrar su cumplimiento.

1.5.4 *Reglamento general de protección de datos de la Unión Europea*

A raíz de la globalización hay un creciente intercambio internacional de datos que hacen más indefensas a las personas en lo concerniente a su esfera de intimidad y vida privada. Esa es una de las razones por las que la Directiva de Protección de Datos de la Unión Europea (Directiva 95/46/CE) en 1995, regula la protección de las personas naturales en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes. Su finalidad es prevenir, investigar y ejecutar sanciones frente al uso arbitrario y extralimitado de los datos personales.

En dicho cuerpo normativo podemos verificar la existencia de disposiciones que tienen gran repercusión más allá de lo que es considerado su ámbito jurídico. Un claro ejemplo de esto es el art. 25 de la Directiva que dispone: "Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen

---

47 CONSEJO DE EUROPA. OFICINA DE TRATADOS. Protocolo Adicional al Convenio para la Protección de las Personas en lo que respecta al Tratamiento Automatizado de Datos Personales, en relación con las autoridades de control y los flujos transfronterizos de datos (STE n.º 181). Estrasburgo: Consejo de Europa. 2021. Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181

tratamientos- obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias*"*. Estas líneas citadas funcionan como base de la protección de datos personales en la que los Estados Miembros de la Unión Europea sólo podrán consentir el traspaso de datos personales a otros países, si estos garantizan un nivel adecuado de garantía frente a posibles vulneraciones.

Sin embargo, esta directiva se emitió en una época en la que recién se daban los primeros pasos de la era digital y tecnológica en la que ahora nos encontramos, por lo que se necesitaba una actualización de la misma que abarque un tratamiento general y eficaz en todos los aspectos de la era digital en la que vivimos. Fue así, que el Parlamento Europeo aprobó el 04 de mayo de 2016 el nuevo Reglamento General de Protección de Datos (RGPD en adelante), que pasó a ser de obligatorio cumplimiento para todos los países miembros el 25 de mayo de 2018, ya que hubo un plazo de adecuación tanto para las instituciones, órganos y organismos de la Unión Europea que trabajan con banco de datos.

El RGPD es un pilar en la protección de datos personales. En palabras de Marcén "el RGPD es considerado como la tercera generación de reglas de protección de datos personales y se usan como parámetro de medida para valorar cómo de modernas son las leyes que se van adoptando en todo el mundo. Las normas de primera generación estarían recogidas en las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE (Organización para la Cooperación y el Desarrollo Económico) de 1980 y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa de 1981 (conocido como Convenio 108). Las normas de segunda generación estarían recogidas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos"[48].

Muchas empresas que radican fuera de Europa se han adaptado a este reglamento, aunque no estén legalmente obligadas a hacerlo. Esto se ha llamado el "efecto Bruselas", según el cual las empresas aplican y exportan normas europeas a nivel global con el fin de

[48] GASCÓN MARCÉN, A., El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. *Cuadernos de Derecho Transnacional*. Vol. *XIII*, n.° 2, 2021. p. 210. Disponible en: https://doi.org/10.20318/cdt.2021.6256

acceder legítimamente al mercado. Asimismo, varios países de Latinoamérica y el Caribe como "Argentina, Uruguay, México, Perú, Colombia (entre otros) desarrollaron sus leyes de protección de datos personales a partir de los años 2000. Estas leyes fueron muy influenciadas por la visión sobre el derecho a la vida privada de la Unión Europea, plasmadas en la Directiva Europea 95/46/CE"[49].

Sin embargo, el RGDP, tiene sus detractores, quienes sostienen que esta norma es excesivamente burocrática y formalista, como es el caso de Estados Unidos, que considera que la aplicación de este reglamento supone "una barrera desproporcionada al comercio, que afecta a todos los Estados fuera de la Unión Europea"[50]. También grandes empresas multinacionales como *British Telecom*, *Yahoo!*, *Facebook*, *eBay* o *Amazon* consideran que la formalidad del RGPD limita la libertad para usar datos de los clientes y creen que ciertos derechos, como el de acceso a la información, no son prácticos. La dificultad de su aplicación o la falta de recursos para hacerlo no debe mermar la protección de los datos personales, ya que el RGPD ha tenido un fuerte impacto en el ámbito de la protección de datos tanto dentro como fuera de las fronteras de la Unión Europea. El Convenio 108 junto al RGPD contribuirán a la convergencia hacia un conjunto de normas de protección de datos de alto nivel permitiendo al mismo tiempo un entorno aún más propicio a la innovación y al crecimiento económico digital inclusivo.

---

49 ENRÍQUEZ ÁLVAREZ, L. "La visión de América Latina sobre el Reglamento General de Protección de Datos". *Comentario Internacional*, n.º 19, 2020. p. 100. Disponible en: https://doi.org/10.32719/26312549.2019.19.4

50 UNITED STATES TRADE REPRESENTATIVE. *National Trade Estimate Report on Foreign Trade Barriers*, 2021. p. 215. Disponible en: https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf

Capítulo 2

Derecho a la intimidad como derecho fundamental

2.1 Origen y concepto del derecho a la intimidad

El amplio desarrollo tecnológico que se ha ido dando en los últimos años nos plantea la siguiente interrogante: ¿la protección de los datos personales es suficiente para garantizar la plena protección del derecho a la intimidad? Como hemos visto, ambos están íntimamente ligados ya que el derecho a la protección de datos personales se construye particularmente sobre la base del derecho a la intimidad. La aparición del internet permite cuestionar si las actividades que realizamos en la red garantizan el respeto de la intimidad de los usuarios. El avance de las tecnologías de la información y cómo se materializan en la vida de las personas justifica realizar un análisis detallado de la noción básica de "intimidad" y, con ello, a desarrollar una serie de mecanismos jurídicos actualizados para la época en la que nos encontramos. De esta manera resguardar, no sólo a la intimidad de la persona, sino también su dignidad. Es por eso que "este nuevo contexto nos conduce a la revisión del concepto de intimidad y a valorar la ineludible necesidad de adaptarlo a las nuevas características de las sociedades con un alto grado de innovación y desarrollo tecnológico, especialmente en el ámbito de la información y la comunicación"[51].

La palabra íntimo proviene de *intimus*, que es una variación filológica de *intumus*, forma superlativa del adverbio *intus*, dentro. Intimo es aquello que está dentro del hombre, no solo lo que está en su interior, sino con el hecho propio de su humanidad. El Diccionario de la Real Academia Española recoge el concepto de intimidad como la "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"[52].

La intimidad a la que nos referimos es importante porque con ella podemos diferenciar a los hombres de los animales, pues si bien es cierto los animales tienen cierto grado de interioridad no es a la misma potencia con la que los seres humanos la poseen. De esta cuestión nos habla Ortega y Gasset en estos términos: "El hombre sería, según esto, y en varios sentidos del vocablo, un animal fantástico. Esta riqueza interna, ajena a los demás animales, dio a la convivencia y al tipo de comunicación que entre estos existe un carácter

---

51 LUCENA CID, I. V. La protección de la intimidad en la era tecnológica: hacia una reconceptualización. *Revista Internacional De Pensamiento Político*, VII, 2012. p. 120. Disponible en: https://www.upo.es/revistas/index.php/ripp/article/view/3683

52 REAL ACADEMIA ESPAÑOLA. *Diccionario de la Lengua Española*, 1992. Vigésimo primera edición.

totalmente nuevo porque no se trató ya solo del envío y recepción de señales útiles referentes a la situación en su contorno, sino de manifestar la intimidad"[53].

Entonces todos los aspectos que formen parte de lo personal pertenecen a su fuero interior y, por tanto, a nadie le debería interesar desvelar. Como derecho es netamente personalísimo, inherente a la propia naturaleza del hombre como tal y fue afianzándose en el derecho positivo post Revolución Francesa de 1789. Sin embargo, no debemos pasar por alto los aportes filosóficos del Liberalismo sobre derecho a la intimidad y a la vida privada, donde autores como John Stuart Mill, Locke y Price afirman que es "la libertad como sustento de un régimen político que acabe con el poder absoluto del gobernante, sirviendo de base para el desarrollo del constitucionalismo británico y moderno"[54].

En 1879, es en los Estados Unidos donde se afirma las primeras referencias al derecho a la intimidad o privacidad, y es aquí que surge la figura del juez Thomas Cooley, quien define el derecho a la privacidad como *"the right to be let alone",* que no es otra cosa que el derecho a ser dejado solo o derecho a estar en soledad. Sin embargo, la elaboración teórica del derecho a la intimidad (como se le conoce en nuestro sistema jurídico), a la privacidad o la vida privada, como derecho de la persona humana y su solidificación, se da en el ensayo elaborado por dos abogados neoyorquinos, Louis D. Brandeis y Samuel D. Warren, titulado *The right to privacy*[55], publicado en 1890. Este ensayo define al derecho a la privacidad como el que comprende todo el ámbito personal de la persona y todo aquello que implica su desarrollo, ámbito que constituye una zona de reserva donde nada ni nadie puede inmiscuirse.

Ambos sentían que la vida privada de las personas se vería amenazada por la proliferación de avances tecnológicos para la época, como el teléfono y el fotógrafo, y también por el desarrollo de la prensa, publicándose los más íntimos detalles en columnas de los periódicos que buscaban satisfacer la curiosidad de las personas mediante la intromisión de la esfera privada de las mismas. Es así que los autores señalan:

> Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y garantizar

---

53 ORTEGA Y GASSET, J. El hombre y la gente. *Revista de Occidente en Alianza Editorial*, España:1980. p. 100. Disponible en: http://manuelosses.cl/VU/El%20Hombre%20y%20la%20gente.%20O.Gasset.pdf.

54 EGUIGUREN PRAELI, F. La libertad de información y su relación con los derechos a la intimidad y al honor en el caso peruano. *IUS ET VERITAS*, n.° 20, 2000. pp. 52-53. Disponible en: https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15924

55 El objeto de los autores no es simplemente realizar una aportación doctrinal, sino que su verdadera pretensión es poner de manifiesto la necesidad del reconocimiento de un nuevo derecho, el derecho a la *privacy.* Y sus objetivos tuvieron efectos cuando nada más transcurridos tres años desde su publicación, un Tribunal utiliza por vez primera el concepto de *privacy* como argumento dilucidador del sentido de una sentencia.

> al individuo lo que el juez Cooley denomina el derecho "a no ser molestado". Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: "lo que se susurre en la intimidad, será proclamado a los cuatro vientos" [...] La intensidad y la complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales[56].

Ambos se vieron en la necesidad de definir un principio que límite la invasión de la prensa y ampare la intimidad del individuo sin importar su clase social, que sea ajena al elitismo social de la época. Es por esto que afirman que el derecho a la privacidad es un derecho de toda persona, sin importar su clase económica y social, que protege de manera igualitaria la personalidad del individuo, ya que cuando se vulnera, se afecta el núcleo de la personalidad individual. Por lo que la finalidad de este derecho "debe ser garantizar a aquellas personas cuyos asuntos no son causa de preocupación legítima para la comunidad que no se han de ver arrastradas a una publicidad indeseable e indeseada, como proteger a toda persona, sea quien sea por su status o por su posición, de ver divulgados, contra su voluntad, asuntos que pudiese preferir, en verdad, mantener reservados"[57].

Sin embargo, Warren y Brandeis reconocen que hay circunstancias donde cede este derecho, cuando se trata de exigencias que buscan el bienestar de toda la comunidad o de justicia. Para los abogados "el derecho a la privacidad no impide la publicación de aquello que es de interés público o general; en segundo lugar, cuando la revelación de la información privada se realiza en circunstancias que conforme al régimen jurídico del Derecho de libelo y difamación sería calificada de información privilegiada o cuando la revelación se produce en cumplimiento de un deber público, de carácter jurídico o moral; en tercer lugar, cuando la publicación se hace en forma oral y sin causar daños especiales; y, finalmente, la protección

---

56 WARREN, S. D. Y BRANDEIS, L. D. (1995). *El derecho a la intimidad*, págs. 26 y 27. Para la edición original, vid. «The Right to Privacy», op. cit., pág. 196, citado en NIEVES SALDAÑA, M., "The Right to Privacy". La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. *Revista de Derecho Político*, Núm. 85, 2012. p. 210. Disponible en: https://doi.org/10.5944/rdp.85.2012.10723

57 Ibídem, pág. 211-212. Para la edición original, vid. "The Right to Privacy", op. cit., pp. 214-215.

del derecho decae cuando es el propio sujeto quien publica los hechos reservados u otorga su expreso consentimiento"[58].

Por todo lo expuesto, llegamos a la conclusión que los abogados Warren y Brandeis velaron porque el derecho a la privacidad sea protegido y reconocido por el sistema jurídico de la época, y consideraron que el núcleo de la personalidad individual se menoscaba cuando terceros vulneran la vida íntima de las personas con tal de obtener información personal que no es de interés general. Este ensayo sirvió como sustento para los diversos pronunciamientos jurisprudenciales que se fueron dando de manera posterior a su publicación.

En 1928, Brandeis, ya como juez de la Corte Suprema, realizó una extensa interpretación del contenido de este derecho y resolvió en el caso Olmstead v. United States por violación de la Cuarta y Quinta Enmiendas, y se apartó de la opinión mayoritaria del Tribunal y emitió un voto discrepante, en el cual manifestó "una profunda preocupación frente a los avances tecnológicos invasivos de la privacidad, especialmente aquellos que podían interceptar las comunicaciones por cable, afirmando que la invasión de la privacidad de la comunicación telefónica es mucho peor que la de la correspondencia, por cuanto que cuando se intercepta una línea de teléfono se invade la privacidad en ambos extremos de la línea"[59]. Asimismo, Brandeis en su voto señaló:

> Los autores de nuestra Constitución se propusieron garantizar las condiciones propicias para la búsqueda de la felicidad. Reconocieron la importancia del carácter espiritual del hombre, sus sentimientos y su intelecto. […] Trataron de proteger a los estadounidenses en sus creencias, ideas, emociones y sensaciones. Otorgaron frente al gobierno el derecho a ser dejado solo, el más completo de los derechos, y el más apreciado por el hombre civilizado. Para proteger ese derecho, toda intrusión no justificada del gobierno en la privacidad del individuo, cualesquiera que sean los medios empleados, debe considerarse una violación de la Cuarta Enmienda. Y la utilización como prueba en un proceso penal de hechos averiguados por esa intrusión debe considerarse una violación de la Quinta Enmienda[60].

Brandeis siempre temía de la tecnología y las consecuencias negativas que acarrearía su mal uso en la esfera íntima e individual de la persona, temor que se materializó con el pasar de los años debido a que el rápido avance tecnológico conllevo a que se vulneren

---

58 Ibídem, p. 215. Para la edición original, vid. "The Right to Privacy", op. cit., pp. 214-218.
59 Ibídem, p. 226.
60 BRANDEIS, J. (juez). *OLMSTEAD V. UNITED STATES*, 277 U.S. 438, f.j. 478-479 (1928)

muchos derechos, entre ellos el de la intimidad, por lo que podemos afirmar que era un adelantado a su época.

Post Segunda Guerra Mundial, en el año 1948, la Declaración Universal de los Derechos Humanos reconoce el derecho a la intimidad y privacidad, o a la vida privada en su art. 12[61]. Además, otros pactos y convenios le han dado el reconocimiento de derecho fundamental pues se ha reflejado la creciente relevancia en las concepciones contemporáneas sobre la sociedad y el orden mundial. Tenemos así al Pacto Internacional de Derechos Civiles y Políticos, a la Convención Americana sobre Derechos Humanos, la Convención sobre los Derechos del Niño, la Convención Internacional sobre la Protección de los Derechos de todos los trabajadores migratorios y sus familiares, la Convención sobre los Derechos de las personas con Discapacidad, todos vinculantes para el Perú y de los cuales ahondaremos más adelante.

Ahora bien, surge una discusión en torno a los conceptos de vida privada e intimidad. Cabe señalar que vida privada e intimidad no son iguales. La "vida privada" puede entenderse como el conjunto de circunstancias y datos personales alejados del conocimiento del resto de los individuos salvo que haya autorización expresa del titular para exteriorizarlos, es un espacio propio de la esfera individual de la persona, en la que cada uno goza de "lo suyo", de sus opiniones. En tanto que el término "intimidad" debe emplearse para referirse a la esfera privada de cada persona y que incluso permanece fuera de su propio entorno familiar más cercano, se hace alusión "siempre a algo que es cercano al individuo, ya sea porque le es próximo o porque es algo propio, interno al mismo, que surge de él y que proyecta sobre su entorno. Suele hablarse, por ello, de la existencia de una esfera individual, de una vida privada, en la que sólo cada persona es quién para decidir lo que le afecta sin tener que tolerar ningún tipo de intromisiones"[62].

En efecto, la vida privada y, más aún, la intimidad, "aparecen como un reducto, un área reservada, donde el individuo se refugia, vive y actúa de forma independiente, donde puede realizar todo tipo de acciones y de actividades sin más regulación que la que él mismo se imponga"[63]. Es preciso indicar que nuestro Tribunal Constitucional ha señalado que "el derecho a la intimidad se encuentra materialmente reservado para lo más íntimo de la persona

---

61 Art. 12 de la Declaración Universal de los Derechos Humanos: "*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*".

62 MARTÍNEZ DE PISÓN CAVERO, J.M. Vida privada e intimidad. Implicaciones y perversiones. *Anuario de Filosofía del Derecho*, N° 13-14. 1997. p. 720. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=142345

63 Ibídem, p. 724.

y de la familia, para los datos más sensibles, entre los que podemos incluir, sin pretensiones de exhaustividad, a todos aquellos datos relativos a la salud, las preferencias sexuales, o los afectos y emociones de los seres más cercanos. El derecho a la vida privada, por su parte, como lo ha interpretado el Tribunal Constitucional, protege un círculo más amplio de actividades y relaciones que no pueden calificarse como íntimas, pero que merecen también protección frente a intromisiones externas"[64].

Para terminar, es importante recalcar que el contenido del derecho a la intimidad se basa en la autonomía del ser humano que comprende sus relaciones personales, familiares, laborales y todos los datos que en conjunto diferencian a cada persona. De modo que el derecho a la intimidad es la potestad que se le concede "a la persona sobre el conjunto de circunstancias personales que puede excluir ilícitamente del conocimiento de terceros"[65], es decir, la intimidad protege la esfera más personal de la persona y será ella quien tiene la libertad de decidir cuáles son los datos que debe limitar y que el derecho dará la correcta protección mediante sus leyes para evitar cualquier tipo de intromisión por parte de terceros a dicha información. En palabras del Tribunal Constitucional español, este derecho se funda en la necesidad de garantizar "la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (…)"[66].

2.2 El derecho a la intimidad en el entorno personal y familiar

Cuando se habla de derecho a la intimidad, necesariamente debemos referir no solo al ámbito personal, sino también al ámbito familiar de los sujetos pues es aquí donde las personas se desarrollan tanto física como emocionalmente, todos los hechos relevantes de la vida de las personas solo le importan a un minúsculo círculo de sujetos que conviven con él.

La vida privada se desenvuelve en infinitas gradaciones y matices que oscilan entre los dos polos de la absoluta publicidad, cuando la persona desaparece por completo bajo la vestidura social y la absoluta soledad, en donde la persona vive integra y absolutamente su vida auténtica y que el conjunto de la vida privada puede compararse con un cono donde la superficie de la base está todavía en contacto con el mundo de las relaciones públicas, pero a medida que los planos van acercándose al vértice y alejándose de la publicidad, van reduciéndose asimismo de extensión, hasta que, llegado al vértice, la vida privada se condensa

---

64 Expediente 03485-2012-PA/TC, f.j. 20.

65 CARMONA BRENIS, M. & VIGIL ZÁRATE, M. El derecho a la intimidad en las relaciones familiares. *Lumen*. Lima: Facultad de Derecho de la Universidad Femenina del Sagrado Corazón. N° 11, 2015. p.79. Disponible en: https://doi.org/10.33539/lumen.2015.n11.546

66 STC 77/2009, f. j. 2.

y concentra en un punto, en la soledad del yo viviente. A la que nadie más que uno mismo puede tener acceso[67]. La cúspide a la que se refiere el autor vendría a ser la intimidad y siguiendo la misma línea, hay que establecer cuál es la parte exenta de penetrar y cuándo está constitucional o legalmente permitido ingresar en la parte no exenta.

Existen dos supuestos en los que un tercero desconocido puede intervenir esa esfera privada: el primero es que la persona voluntariamente decida compartir su vida privada con terceros, es decir, tener una vida abierta al público; en tal caso la información que brinde podrá difundirse, pero con ciertos límites, por ejemplo, que no haya un menoscabo de su dignidad, que esta información sea veraz, que no sea trastocada, que no haya difamaciones que puedan afectar el honor del ciudadano. El segundo supuesto es cuando una persona ha alterado el orden público, haya afectado a terceros con su comportamiento, haya cometido una infracción o delito por el cual es necesario que la potestad pública le imponga una sanción o una pena, es en ese momento donde la fuerza pública está legitimada a averiguar todos los datos necesarios para resolver el conflicto que haya surgido entre sujetos privados.

Al ser un derecho fundamental, el Estado debe promover el reconocimiento y correcta regulación del bien humano intimidad, para permitirle a toda persona la posibilidad de reservar ciertos aspectos de su vida, sin que queden expuestos al conocimiento de los demás. La intimidad es protegida por la Constitución y diversas normas, por ello ni el Estado ni la comunidad en que reside, pueden entrometerse sin la voluntad del sujeto a menos que haya cometido un delito, pero incluso en esta situación se requerirá autorización judicial.

2.3 Contenido constitucional del derecho a la intimidad

2.3.1 *Metodologías sobre el contenido constitucional de los derechos*

Todos los derechos fundamentales tienen un contenido constitucional cuyo alcance es establecido por la Constitución y por las leyes y sentencias de desarrollo constitucional, así como por las normas de origen convencional. Es un contenido conformado por el conjunto de atribuciones que el derecho reconocido depara a su titular, de modo que la persona podrá invocar las pretensiones que vengan justificadas por las atribuciones que el derecho le otorga.

Los derechos fundamentales deben ser entendidos como bienes humanos “debidos a la persona humana por ser tal y es lo debido porque es lo que le corresponde por tener la naturaleza y dignidad humana, por eso se formulan como bienes jurídicos vinculantes. Y es que en la medida que se habla de título y deuda, se habla de derecho. Estos bienes humanos que corresponden a la persona humana (deuda) por tener naturaleza y dignidad humana

---

[67] GARCÍA MORENTE, M. *Ensayo sobre la vida privada*. Ensayos. Madrid. 1935. ISBN: 978-84-9920-106-1. pp. 163-169.

(título) son derechos humanos"[68]. Así definidos, los derechos fundamentales tienen a la dignidad humana como su fundamento. En palabras del Tribunal Constitucional, "la dignidad humana es el presupuesto jurídico de la existencia de todos los derechos fundamentales. La persona humana no puede ser concebida como un medio, sino como un fin en sí mismo; de ahí que su defensa constituya el fin supremo que debe inspirar todos los actos estatales, en particular, y los de la sociedad, en general"[69]. Con otras palabras, la dignidad humana es el "presupuesto ontológico para la existencia y defensa de sus derechos fundamentales"[70].

Esto significa que la dignidad humana, como valor constitucional supremo, influye en la delimitación del contenido constitucional de los derechos fundamentales. La dignidad humana siempre debe ser tomada en cuenta a la hora de determinar a qué da derecho un derecho fundamental. Y en esa delimitación deben ser empleados criterios de interpretación constitucional acordes precisamente con la dignidad humana. En particular, debe delimitarse de la mano de los principios de unidad (y sistematicidad) de la Constitución, así como del principio de concordancia práctica, los cuales nuestro Tribunal Constitucional los ha definido de la siguiente manera:

> (…) a) *El principio de unidad de la Constitución*: Conforme al cual la interpretación de la Constitución debe estar orientada a considerarla como un «todo» armónico y sistemático, a partir del cual se organiza el sistema jurídico en su conjunto. b) *El principio de concordancia práctica*: En virtud del cual toda aparente tensión entre las propias disposiciones constitucionales debe ser resuelta «optimizando» su interpretación, es decir, sin «sacrificar» ninguno de los valores, derechos o principios concernidos, y teniendo presente que, en última instancia, todo precepto constitucional, incluso aquellos pertenecientes a la denominada «Constitución orgánica» se encuentran reconducidos a la protección de los derechos fundamentales, como manifestaciones del principio-derecho de dignidad humana, cuya defensa y respeto es el fin supremo de la sociedad y el Estado (artículo 1 º de la Constitución)[71].

Así, se ha sostenido que la determinación del contenido constitucional "debe realizarse conforme a los alcances de los principios de unidad y concordancia práctica; vale decir, de un lado, resguardando la relación e interdependencia de los distintos elementos normativos con el conjunto de las decisiones básicas de la Constitución (ello obliga a no aceptar, en modo

---

68 CASTILLO CÓRDOVA, Luis. El significado del contenido esencial de los derechos fundamentales. Revista PUCP. *Foro Jurídico*, (13), 2014. p. 145. Disponible en: https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/13783

69 Expediente 00050-2004-AI/TC, f.j. 46.

70 Expediente 00010-2002-AI/TC, f.j. 217.

71 Expediente 5854-2005-PA/TC, f.j. 12.

alguno, la visión «insular» de una norma, sino a hacer imperativa la perspectiva del conjunto del texto); y del otro, garantizando que todos los derechos, valores y bienes constitucionales conserven en un grado razonable su identidad e indemnidad"[72]. El contenido de un derecho fundamental, no implica que se expande ilimitadamente, sino que tiene alcances razonables en razón del bien humano que es lo que da sentido al derecho fundamental. Por ello, en estricto, los conflictos entre derechos no son reales, lo que en realidad entra en conflicto son las pretensiones, para respetar un derecho fundamental se tiene que respetar su contenido constitucional y habrá que asegurarlo, cumplirlo, respetarlo y esto se logra tratando a la persona como fin supremo de la sociedad y del Estado.

El hecho de que exista un sacrificio por parte de un derecho por otro en caso de un conflicto, es lo que recoge la teoría conflictivista de los derechos fundamentales, esto se da cuando el titular de un derecho fundamental quiere ejercerlo, sin embargo, se encuentra frente a una postura distinta a la de ese ejercicio con el titular de otro derecho fundamental que también pretende ejercerlo. Para esta teoría, frente a una situación de conflicto los mecanismos de solución son la jerarquía y ponderación de derechos, que lo que busca es preferir un derecho por encima del otro. Es así que "en la jurisprudencia del Tribunal Constitucional español se suele afirmar que la libertad de información es jerárquicamente superior al derecho a la intimidad o al derecho al honor, en cuanto aquella libertad tiene una especial relevancia para el asentamiento democrático de una sociedad, valor que no se encuentra en derechos como el derecho a la intimidad o al derecho al honor"[73].

Las posiciones conflictivistas de los derechos fundamentales pueden legitimar situaciones que llegan a vulnerar el contenido constitucional de los derechos, afectando el principio de normatividad de la Constitución. Es grave que no se reconozca un derecho fundamental porque va en contra de la existencia digna del hombre del Estado de derecho e incluso del concepto de Constitución, por lo tanto, los derechos no prevalecen uno sobre otro, sino que deben vivir de una manera armoniosa y conjunta que garantice su plena vigencia.

En contra posición a la teoría conflictivista, está la teoría armonizadora de los derechos, la cual enuncia que el fundamento de los derechos es la naturaleza humana y la finalidad última es favorecer el completo desarrollo de la persona humana, tanto en el ámbito

---

72 GARCÍA TOMA, V. *La dignidad humana y los derechos fundamentales*. Revista Derecho & Sociedad, Perú: Asociación Civil de la Universidad Pontificia Universidad Católica del Perú. N° 51. 2018. p. 25. ISSN 2079-3634. Disponible en: https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/20855

73 CASTILLO CÓRDOVA, Luis. *¿Existen los llamados conflictos entre derechos fundamentales?* Cuestiones Constitucionales: Revista Mexicana de Derecho Constitucional, N°12, 2005. p. 103-104. Disponible en: https://doi.org/10.22201/iij.24484881e.2005.12.5726

individual y social, como en el espiritual y material. Entonces los derechos tienen su sentido en cuanto a su pleno ejercicio ayuda a la consecución de esa finalidad. La persona humana "es una realidad unitaria y coherente cuya plena realización rechaza cualquier tipo de contradicción interna. Es decir, si los derechos del hombre son desprendimientos o manifestaciones de una realidad unitaria y coherente como lo es su naturaleza humana, entonces no puede haber manera que los derechos puedan ser contradictorios entre sí, al punto que puedan entrar en conflicto"[74].

El modelo estatal actual en Perú se fundamenta en el Estado Constitucional de Derecho, donde la Constitución tiene la máxima autoridad en el sistema legal nacional y el Tribunal Constitucional desempeña un papel crucial como defensor de los derechos fundamentales; en ese sentido se ha pronuncia nuestro Tribunal en su jurisprudencia, en el Expediente N° 2839-2021-PHD/TC, fundamento jurídico 19: "Cabe recordar que un Estado Constitucional de Derecho, no es aquel en el que unos bienes jurídicos se priorizan por encima de otros so pretexto de circunstancias meramente coyunturales, sino aquel en el que se tiende a una correcta delimitación, pero también y con mucha mayor razón, una sensata armonización entre todos ellos".

En el mismo sentido se establece en el Expediente N° 3086-2021-PA/TC, fundamento jurídico 6 (voto singular del Magistrado Ochoa Cardich): "Finalmente estimo pertinente recalcar que, en un Estado Constitucional de Derecho, no corresponde una lectura aislada o unilateral de los bienes jurídicos sino una armonización integral de los mismos a efectos de que unos no terminen desvirtuando o vaciando de contenido a los otros. Así las cosas, el condicionar el razonamiento a lo que representan sólo unos derechos como si los mismos tuviesen una connotación absoluta o absolutista, no es lo que se espera de nuestro Colegiado ni desde luego de quienes como Magistrados lo representamos".

Todo esto es posible si al momento de interpretar la Constitución los "métodos de interpretación constitucional no se agoten en aquellos criterios clásicos de interpretación normativa (literal, teleológica, sistemático e histórico), sino que abarquen, entre otros elementos, una serie de principios que informan la labor hermenéutica del juez constitucional"[75], donde resaltan los principios de unidad de la Constitución y de concordancia práctica, anteriormente mencionados. Esto requiere examinar minuciosamente las circunstancias específicas de cada situación legal.

---

74 Ibídem, p. 110.

75 Expediente 5854-2005-PA/TC, f.j. 12.

En virtud de ello este método no permite la existencia de posiciones jurídicas contrarias entre sí, de manera que nos hace interpretar la Constitución de manera unitaria, sin generar contradicción, siendo que para esta teoría no existen conflictos, es decir, no habría ningún derecho fundamental que sacrificar, ni desplazar, puesto que los contenidos constitucionales están para cumplirse de manera eficaz; de modo que un juez que recoge esta teoría se preguntara al momento de resolver un caso concreto cuál de las dos partes (demandante o demandado), ha invocado y ejercido razonablemente su derecho, porque entiende que siendo ejercido el derecho de manera razonable por ambas partes no se configura controversia y si existiera, sería sobre las pretensiones y de ser el caso el juez utilizará una serie de herramientas, tales como la "interpretación sistemática o unitaria de la Constitución, el principio de normatividad de la Constitución, el principio de concordancia práctica, el principio teleológico, y el principio de razonabilidad en sus componentes de idoneidad y necesidad"[76], que le permitirán dar razones para delimitar cual es el alcance del contenido constitucional del derecho que está siendo invocado, en un caso en concreto, y una vez que logre determinarlo este deberá reconocerlo, exigirlo, cumplirlo y brindarle una protección eficaz, de modo que los contenidos constitucionales coexistan entre sí sin necesidad de sacrificar uno por otro, y si aparece alguna contradicción, no se resuelve ponderando, sino por medio de los criterios de justicia material (dignidad humana y derechos humanos).

En nuestro ordenamiento jurídico, cada operador jurídico usara la teoría que crea más conveniente para el caso concreto. El Tribunal Constitucional no puede imponer a instancias inferiores que metodología utilizar, pero lo que sí se debe tener en cuenta es que la metodología que se utilice se conozca a cabalidad y no sólo sea un uso nominal, y así evitar decir que se emplea una metodología cuando en realidad se resuelve con la otra.

2.3.2 *El contenido constitucional del derecho a la intimidad*

Dicho esto, el contenido constitucional del derecho a la intimidad está ligado estrechamente a la dignidad de la persona, pues es el ámbito mismo donde una persona puede desarrollarse y ejercer su libertad de manera plena. En reiterada jurisprudencia el Tribunal Constitucional menciona que "en ningún caso puede ser permitido desconocer la personalidad del individuo y, por ende, su dignidad. Ni aun cuando el sujeto se encuentre justificadamente privado de su libertad es posible dejar de reconocerle una serie de derechos o atribuciones que

---

[76] CASTILLO CÓRDOVA, Luis. *Las fuentes constitucionales sobre derechos fundamentales*. Lima: Centro de Investigaciones Judiciales. Colección: Cuadernos de Investigación. Serie: Derecho Constitucional n.° 2, Primera ed. Fondo Editorial del Poder Judicial. 2022. p. 86-87. ISBN: 978-612-4484-36-0. Disponible en: https://www.pj.gob.pe/wps/wcm/connect/695a7f804799c825ab5dbb2a87435a1f/web_Las+fuentes+constitucionales+-+Luis+Castillo.pdf?MOD=AJPERES&CACHEID=695a7f804799c825ab5dbb2a87435a1f

por su sola condición de ser humano le son consubstanciales. La dignidad, así, constituye un mínimo inalienable que todo ordenamiento debe respetar, defender y promover"[77].

Si bien la dignidad humana fundamenta el contenido constitucional del derecho que queremos proteger, debemos profundizar más en lo que respecta al objeto de protección del derecho a la intimidad, puesto que no podemos hablar de una garantía plena del derecho a la intimidad si no sabemos cuál es su ámbito de protección, sus alcances y los nuevos matices que ha alcanzado este derecho con el desarrollo tecnológico. De todo ello debemos tomar conocimiento, para que exista una mejor y mayor protección del derecho a la intimidad. Si queremos entender y buscar en qué ámbito de la persona se encuentra la intimidad, esta se refiere a la protección de las distintas áreas de la vida de las personas, por poner unos ejemplos podría ser la intimidad laboral, educativa, social, con respecto a su salud o simplemente su esfera de privacidad, estos ámbitos actualmente están protegidas por el ordenamiento jurídico a fin de evitar intromisiones frente a terceros.

Según el Tribunal Constitucional la "intimidad implica necesariamente la posibilidad de excluir a los demás en la medida que protege un ámbito estrictamente personal, y que, como tal, resulta indispensable para la realización del ser humano, a través del libre desarrollo de su personalidad"[78]. La persona únicamente podrá crear una identidad propia a través del reconocimiento de la misma y así salir a la sociedad cuando "aquel dato y espacio espiritual del cual goza se lo permita. La vida privada es un derecho fundamental en primordial relación con la intimidad. El último de ellos tiene una protección superlativa dado que configura un elemento infranqueable de la existencia de una persona; la vida privada, por su parte, la engloba y también incluye un ámbito que sí admite algunas intervenciones que habrán de ser consideradas como legítimas, vinculándose inclusive con otros derechos como la inviolabilidad de domicilio, prevista, en el artículo 2º, inciso 9 de la Norma Fundamental"[79].

Sobre el contenido constitucional del derecho a la intimidad, ha establecido el Tribunal Constitucional que el mandato constitucional "protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen"[80]. Asimismo, ha establecido que "el contenido esencial del derecho a la intimidad personal: a) la referencia al contenido esencial del derecho a la intimidad personal, reconocido por el articulo 2°7 de la Constitución,

---

77 Expediente 00010-2002-AI/TC, f.j. 218.
78 Expediente 00072-2004-AA/TC, f.j. 15.
79 Expediente 06712-2005-HC/TC, f.j. 38.
80 Expediente 01797-2002-HD/TC, f.j. 3.

hace alusión a aquel ámbito protegido del derecho cuya develación publica implica un grado de excesiva e irreparable aflicción psicológica en el individuo, lo que difícilmente puede predicarse en torno al componente económico del derecho"[81].

De los párrafos anteriores podemos afirmar que el contenido constitucional del derecho a la intimidad que se protege es el respeto de aquel espacio propio de la persona en el que puede realizar los actos que crea convenientes y que solo le competen a este, para su desarrollo o su plena realización; tendrá que ser una zona ajena al interés de los demás, donde el titular tiene el derecho a impedir, intromisiones de terceros. Ahora, con el tratamiento, la recolección, el almacenamiento de informaciones que antes sólo podía formar parte de la vida íntima de cada ser humano y que era conocido por un mínimo sector, ha ido variando paulatinamente su entorno y estructura.

Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados. Es por lo que el derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de acceso y control de sus informaciones personales, es decir, de toda aquella información relativa a su persona. Por tal motivo, "el uso y control sobre los datos concernientes a cada persona, debe serle reconocido ya no sólo como una mera prerrogativa, sino además como un derecho fundamentalmente protegido y garantizado por mecanismos de protección idóneos"[82]. Es menester indicar que ningún derecho es absoluto, en el sentido de que ningún derecho es ilimitado en su contenido, y el derecho a la intimidad no es la excepción: es un derecho que no puede ser ejercido extra limitadamente. Para conseguirlo es relevante saber identificar el alcance razonable del derecho en las concretas circunstancias de cada caso.

2.4 La interferencia de los Estados en la intimidad de las personas

El derecho nos garantiza libertad de desenvolvimiento de nuestra conducta en tanto esa conducta no vulnere el orden público, la moral y las buenas costumbres, ni tampoco perjudique el derecho de los demás. Las personas deben de tener la posibilidad de excluir hechos reservados para sí mismos del conocimiento de terceros y controlar cuáles aspectos pueden ser conocidos o no. La finalidad del derecho a la intimidad es garantizar esferas de libertad para su pleno ejercicio, sin la intromisión de terceros y se constituye como un espacio

---

81 Expediente 00011-2004-AI/TC, f.j. 37.

82 GARCÍA GONZÁLEZ, Aristeo. 2007. *La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.* Bol. Mex. Der. Comp. vol.40 no.120. Ciudad de México. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003

íntimo de exclusión para la autoridad y "se forja como un ámbito que no concierne al Estado, rasgo central para la definición de esfera privada. En consecuencia, lo privado es extensamente definido en oposición a lo público, así como en relación con la ausencia de interferencia o incumbencia estatal. Así, buena parte de la vida privada de las personas, incluida la vida familiar, íntima, de relación, crianza de la infancia, asistencia a las personas dependientes y otros, ha sido protegida primordialmente en términos de privacidad, es decir, como espacio libre de interferencia estatal, con vistas a garantizar un ámbito de mayor autonomía personal"[83].

La afectación del derecho a la intimidad se produce con la "sola intromisión, intrusión y divulgación de hechos, que perturba su reserva y privacidad y que se producen sin el consentimiento del titular. No se requiere que esta conducta conlleve ningún daño o perjuicio adicional a la mera molestia; incluso existirá violación del derecho (y obligación de reparación) si la difusión de la información genera un beneficio en la reputación o popularidad de la persona a que se refiere, en vez de una merma o menoscabo en ésta. Tampoco se admite que el autor de la agresión invoque la veracidad de la información difundida como eximente de responsabilidad, aunque ello sea realmente cierto, pues la *exceptio veritatis* no procede en un derecho cuya protección se refiere a una reserva o privacidad que resultan objetivamente vulneradas con la mera intromisión no autorizada"[84]. Sin embargo, hay que recalcar que el Estado interviene en la esfera privada de las personas para regular sus actuaciones, haciéndolo a través del derecho privado, mediante el cual ordena y pone límites a las actuaciones individuales.

Como ya hemos visto en el capítulo anterior, para la protección de los datos personales, cuya base es el derecho a la intimidad, el Estado interviene con la aprobación de una regulación jurídica que brinde protección al ámbito privado de las personas a fin de protegerlo de una posible injerencia no debida, ya sea por parte del mismo Estado o de terceros. Estableciendo razonables limitaciones, en particular cuando se trata de asuntos de seguridad nacional o motivos legítimos concretos, los cuales justifiquen una intervención, siempre razonable en el ámbito privado de las personas. La validez de tales limitaciones reclama que no sean abusivas o arbitrarias y se ajusten a los criterios y principios de interpretación de la Constitución, por lo que una idea de "autonomía basada solo en la no

---

83 ÁLVAREZ MEDINA, S. *La interferencia estatal en la vida privada y familiar*. Madrid: Universitat de Valencia. Cuadernos Electrónicos de Filosofía del Derecho, no. 42. 2020. ISSN: 1138-9877. Disponible en: https://doi.org/10.7203/CEFD.42.16609

84 EGUIGUREN PRAELI, F. 2000. La libertad de información. p. 61.

interferencia estatal en las acciones de las personas resulta una concepción pobre y distorsionada de la misma"[85].

2.5 Regulación del derecho a la intimidad en el Perú

Con el uso de las nuevas tecnologías, como las redes sociales, ponemos en riesgo también nuestro derecho a la intimidad ya que estamos disponiendo de nuestra privacidad, para ello solo basta con compartir una foto, puesto que posiblemente un tercero puede hacer mal uso de la información que compartamos. Dicho esto, es necesario estudiar las normas del sistema jurídico peruano que reconocen este derecho, las mismas que nos amparan frente a posibles arbitrariedades, pues la afectación a este derecho se va a producir, como ya hemos visto, con la sola intromisión, intrusión y divulgación de hechos que perturban la intimidad del titular. Recuerda el Tribunal Constitucional que:

> En la Constitución, como derecho-regla base se ha prescrito en el artículo 2°, inciso 7, que toda persona tiene derecho a la intimidad personal y familiar. Además, existen otros dispositivos que siguen refiriéndose a este tema dentro del mismo artículo 2°: el impedimento de que los servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar (inciso 6); la inviolabilidad de domicilio (inciso 9); el secreto e inviolabilidad de comunicaciones y documentos privados (inciso 10); entre otros. Y pese a que el desarrollo constitucional de la materia es disperso, lo cierto es que la Declaración Universal de Derechos Humanos le da cierta coherencia y unidad. Así, en el artículo 12º se sostiene que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, motivo por lo cual se expresa el derecho a la protección de la ley contra tales injerencias o ataques[86].
>
> Asimismo, señala:
>
> Que la intimidad personal implica el aislamiento de la intromisión de terceros de todos aquellos aspectos de la persona que forman parte de su desarrollo interno, entendido como el desarrollo de su personalidad física y espiritual que se encuentra reservada para sí misma, entre los que hallamos el desarrollo de los procesos de pensamiento y opinión, de la salud física y emocional, de la sexualidad humana (en todas sus expresiones), entre otros aspectos que únicamente son de interés de la persona. En tal sentido, la concepción de la intimidad humana se entiende que resulta personalísima, subjetiva, psicológica, pero también cultural y temporal, pues cada ser humano

---

85 ÁLVAREZ MEDINA, S. *La interferencia estatal en la vida privada y familiar*. no. 42.

86 Expediente 06712-2005-HC/TC, f.j. 37.

entiende de manera particular qué es aquello que para sí resulta íntimo en un espacio y tiempo histórico[87].

A parte de la normativa expuesta en la cita anterior debemos tener en cuenta que nuestro Código Civil también recoge normativa referente al derecho a la intimidad en su artículo 14[88]. Con respecto a esto, en la jurisprudencia del Tribunal Constitucional se ha señalado que lo que se protege no solo es lo recogido por el artículo 14 del Código Civil, sino también "que no se lleven a cabo intromisiones ilegítimas en dicha intimidad, aun cuando la información obtenida a partir de dicha intromisión no sea dada a conocer públicamente. Es decir, el derecho a la intimidad no solo protege el derecho a que no se difundan informaciones relativas a nuestra intimidad, sino el derecho a no ser objeto de intromisiones ilegítimas en nuestra vida íntima y familiar sin nuestro consentimiento, independientemente de la fuente de donde provengan dichos actos lesivos"[89]. Asimismo, se encuentra protegido en el Código Penal, a través del tipo penal de "violación de la intimidad"[90], que a su vez se encuentra dentro de los delitos contra la intimidad.

Otra norma que prevé la protección del derecho a la intimidad, pero referida directamente a los titulares de datos personales, los principios y las condiciones que se deben aplicar en su tratamiento es la Ley N° 29733, Ley de Protección de Datos Personales, la cual ya hemos abordado en el capítulo anterior, pero es necesario tenerla en cuenta en este recuento de normativa.

Del mismo modo, el Texto Único Ordenado del Código de los Niños y Adolescentes, protege la intimidad del menor en el artículo 77 señalando que "cuando un niño o adolescente se encuentre involucrado como autor o partícipe o testigo de una infracción no se hace pública su identidad. El Juez sanciona, por denuncia del Fiscal Especializado, a los que violan los secretos de las investigaciones relacionadas con los niños y adolescentes".

El Texto Único Ordenado del Código Tributario también protege la intimidad de las personas, a través de la salvaguarda de su información, por lo que en el artículo 85 establece que "tendrá carácter de información reservada, y únicamente podrá ser utilizada por la Administración Tributaria, para sus fines propios, la cuantía y la fuente de las rentas, los gastos, la base imponible o, cualesquiera otros datos relativos a ellos, cuando estén contenidos

---

87 Expediente 01929-2019-PHD/TC, f.j. 10.

88 Art. 14 del Código Civil: "*La intimidad de la vida personal y familiar no puede ser puesta de manifiesta sin el asentimiento de la persona, o si esta ha muerto, sin el de su cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en este orden*".

89 Expediente 03485-2012-PA/TC, f.j. 23.

90 Art. 154 del Código Penal: "*El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa no mayor de dos años […]"*

en las declaraciones e informaciones que obtenga por cualquier medio de los contribuyentes, responsables o terceros, así como la tramitación de las denuncias a que se refiere el Artículo 192° (…)".

La Ley del Procedimiento Administrativo General, Ley N° 27444, de igual manera protege la intimidad de las personas en el artículo 1.12: "Principio de participación. - Las entidades deben brindar las condiciones necesarias a todos los administrados para acceder a la información que administren, sin expresión de causa, salvo aquellas que afectan la intimidad personal, (…)". Del mismo modo lo hace en el artículo 160.1 donde señala que "los administrados, sus representantes o su abogado, tienen derecho de acceso al expediente en cualquier momento de su trámite, así como a sus documentos, antecedentes, estudios, informes y dictámenes, obtener certificaciones de su estado y recabar copias de las piezas que contiene, previo pago del costo de las mismas. Sólo se exceptúan aquellas actuaciones, diligencias, informes o dictámenes que contienen información cuyo conocimiento pueda afectar su derecho a la intimidad personal o familiar y las que expresamente se excluyan por ley o por razones de seguridad nacional de acuerdo a lo establecido en el inciso 5) del Artículo 20 de la Constitución Política. Adicionalmente se exceptúan las materias protegidas por el secreto bancario, tributario, comercial e industrial, así como todos aquellos documentos que impliquen un pronunciamiento previo por parte de la autoridad competente".

En este mismo marco la Defensoría del Pueblo ha reiterado en diversos comentarios y en concreto en uno de sus pronunciamientos lo siguiente:

> Que la difusión de imágenes, sin autorización, de personas heridas, así como de exámenes médicos o diligencias judiciales, constituye un delito, conforme lo señala el Artículo 154 del Código Penal, en la medida de que tal hecho lesiona de forma grave el derecho a la intimidad. La citada norma penal, en su Artículo 155, agrava la sanción (hasta los seis años de prisión) si en la comisión de este delito participan funcionarios o servidores públicos en razón de su función. Cabe mencionar que el inicio de la acción penal, en este caso, corresponde solo a los agraviados y no al Ministerio Público (Artículo 158 del Código Penal). Al margen del establecimiento de la responsabilidad penal, la Defensoría del Pueblo insiste en la necesidad de investigar y sancionar, a nivel administrativo, las filtraciones de imágenes que agravian la intimidad personal y familiar. En tal caso, las entidades públicas comprometidas están

obligadas a tomar acciones de oficio, sin esperar a que se formule denuncia de parte. La Defensoría del Pueblo supervisará si han cumplido o no con este deber[91].

El Estado está obligado a proteger estos derechos y exigencias, velando porque todos los poderes públicos establezcan mecanismos o protocolos que garanticen la intimidad de las personas. Es así que el ordenamiento jurídico peruano no ha sido ajeno a la actualización de la protección del derecho a la intimidad, ya que con el pasar de los años, este derecho se ha tornado un espacio donde la injerencia es mucho más factible debido a los constantes avances tecnológicos. Como hemos visto, la Constitución y diversas leyes han otorgado protección a este derecho, que ha tenido desarrollo normativo en los distintos códigos, que permiten regular las actuaciones de las personas en los distintos aspectos en los que desarrolla, permitiendo que desarrollen esa esfera personal libre de intromisiones.

2.6 Protección del derecho a la intimidad y a la vida privada en los tratados internacionales

La comunidad internacional se ha visto en la obligación de proteger la intimidad y esfera personal de las personas dada la aparición de nuevas tecnologías de la información, especialmente la internet, que hacen más propensas a las personas a sufrir injerencias no deseadas o consensuadas por parte de terceros, por lo que la comunidad internacional ha buscado reforzar la confianza sobre los medios de comunicación a través de la protección de la intimidad y de los datos personales.

Es así que la primera manifestación de positivización del derecho a la intimidad y privacidad la encontramos en la Declaración Americana de Derechos y Deberes del Hombre. A pesar de que no es un Tratado Internacional, es importante mencionarla, ya que, al momento de su adopción, en mayo de 1948, meses antes de la Declaración Universal de Derechos Humanos, los Estados acordaron que no era de cumplimiento obligatorio. Sin embargo, no podemos decir que su contenido no es vinculante, ya que desde su adopción los Estados Miembros de la Organización de Estados Americanos han acordado diversas decisiones que implican la obligatoriedad de esta Declaración, es decir, es costumbre internacional; y cuyo valor jurídico se vio fortalecido por el Pacto de San José de Costa Rica y por la base legal de la Comisión Interamericana de Derechos Humanos.

Es el primer instrumento del continente americano donde se establece un listado de todos los derechos que tienen las personas por el simple hecho de ser seres humanos y tuvo un

---

[91] DEFENSORÍA DEL PUEBLO. Pronunciamiento N° 014/DP/2019. 2019. Disponible en: https://www.defensoria.gob.pe/wp-content/uploads/2019/04/DEFENSOR%C3%8DA-DEL-PUEBLO-SE-PRONUNCIA-SOBRE-EL-DERECHO-A-LA-INTIMIDAD-PERSONAL-Y-FAMILIAR-4.pdf

rol muy importante en el mundo. Esta declaración incluye un total de 27 derechos, tanto derechos civiles y políticos como derechos económicos, culturales y sociales. Es así que el artículo 5 recoge lo siguiente: "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar". Asimismo, el artículo 9 señala: "Toda persona tiene el derecho a la inviolabilidad de su domicilio". Esta declaración es muy importante ya que es la primera que recoge de manera expresa el respeto a la vida privada y además su fundamento es el ser humano, su libertad y su dignidad.

La Declaración Universal de Derechos Humanos, suscrita meses después de la Declaración Americana de Derechos y Deberes del Hombre, en diciembre de 1948, fue aprobada por el Perú mediante Resolución Legislativa N° 13282, publicada el 24 de diciembre de 1959. Reconoce diversos derechos y brinda protección contra las injerencias arbitrarias en la vida privada y familiar, su domicilio o correspondencia. Es así, que en su artículo 12 establece: "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". Menos amplio es el reconocimiento mostrado en el artículo 5, que se restringe a señalar que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su vida privada y familiar".

El Pacto Internacional de Derechos Civiles y Políticos de 1966, aprobada en el Perú mediante Decreto Ley N° 22128 del 28 de marzo de 1978, reconoce en su artículo 17 lo siguiente: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". De un análisis de los artículos 12 de la Declaración Universal y 17 del Pacto Internacional, se llega a la conclusión que nadie podrá transgredir arbitraria o ilegalmente el derecho a la intimidad. Tampoco su honor o buena reputación serán objeto de ataques ilícitos.

En noviembre de 1969 se suscribió la Convención Americana de Derechos Humanos, aprobada en nuestro país el 11 de julio de 1979 mediante Decreto Ley N° 22231. La Convención recoge en su texto algo muy semejante a lo regulado en el Pacto Internacional, específicamente en su artículo 11: "Protección de la honra y de la dignidad: 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

De igual manera, la Convención sobre los Derechos del Niño, ratificada en 1989 y vigente en el país desde el 4 de octubre de 1990, aprobada mediante Resolución Legislativa N° 25278, estipula lo siguiente en su artículo 16: "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

La Convención Internacional sobre la Protección de los Derechos de todos los trabajadores migratorios y sus familiares de 1990, suscrita por el Perú en 2004, aprobada mediante Resolución Legislativa N° 28602 y ratificada por el Decreto Supremo N° 071-2005-RE. Sin embargo, debemos señalar, que, si bien es cierto que se publicó el 13 de setiembre de 2005, su entrada en vigencia no fue hasta el 1 de enero de 2006. Esta Convención señala en su artículo 14 que "ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques".

La Convención sobre los Derechos de las personas con Discapacidad, aprobado por la Asamblea General de las Naciones Unidas en 2006 y adoptada en nuestro país mediante Resolución Legislativa Nº 29127, publicada el 1 de noviembre de 2007 y ratificada por Decreto Supremo Nº 073-2007-RE, recoge en su artículo 22: "1. Ninguna persona con discapacidad, independientemente de cuál sea su lugar de residencia o su modalidad de convivencia, será objeto de injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia o cualquier otro tipo de comunicación, o de agresiones ilícitas contra su honor y su reputación. Las personas con discapacidad tendrán derecho a ser protegidas por la ley frente a dichas injerencias o agresiones. 2. Los Estados Partes protegerán la privacidad de la información personal y relativa a la salud y a la rehabilitación de las personas con discapacidad en igualdad de condiciones con las demás".

Al realizar un análisis de los tratados y convenios internacionales, podemos concluir que la protección al derecho a la intimidad está garantizada tanto convencionalmente como constitucionalmente, en razón a la aplicación de las nuevas formas de comunicación, como lo son las redes sociales y medios electrónicos. Esta protección no se dará solo a los sujetos privados sino también atañe a los órganos gubernamentales. Las distintas constituciones y sus normas de desarrollo, tienen la obligación de proteger el derecho a la intimidad. Asimismo, su protección abarca también un resguardo a la dignidad de la persona, que le permita desarrollar su propia personalidad, determinar su identidad y aspiraciones. Este espacio de libertad debe

estar exento de toda práctica o injerencia abusiva por parte de terceros o de la propia autoridad, y es el Estado quien tiene el deber de prevenir que se vulneren los bienes jurídicos protegidos que son propios de nuestra esfera personal.

Capítulo 3

La validez de la vigilancia masiva. Especial referencia a su constitucionalidad en el Perú

En el mundo digitalizado en el que nos encontramos, la vigilancia masiva se ha convertido en un tema de discusión fundamental. La proliferación de tecnologías de comunicación y el crecimiento exponencial de los datos han facilitado la capacidad de los gobiernos y entidades privadas para recopilar información sobre individuos en una escala sin precedentes. Este fenómeno plantea importantes interrogantes éticas, legales y constitucionales, cuya respuesta requiere un delicado equilibrio entre la seguridad nacional y los derechos fundamentales de las personas.

El avance tecnológico ha trasformado a los seres humanos y ha permitido un progreso sin precedentes. Esto se debe en gran medida a la interconectividad de los dispositivos que generan acceso a gran cantidad de información en un espacio y tiempo reducido. Uno de los más grandes inventos en el mundo tecnológico es la red Internet, que ha generado profundos cambios sociales, culturales, políticos y económicos. A través de la historia han ocurrido hechos relacionados con la vigilancia indiscriminada y arbitraria, sin embargo, se ha revelado la utilización de un nuevo tipo de vigilancia, la vigilancia masiva electrónica. A pesar de las grandes ventajas que nos pueden llegar a brindar estas nuevas tecnologías, también tiene sus desventajas que generan un temor y preocupación en la sociedad.

Es así, que los derechos de las personas se ven también afectados y vulnerados ante el desmesurado avance tecnológico. Uno de los más afectados es el derecho a la intimidad, que como ya hemos visto en el capítulo anterior es vulnerado por el uso arbitrario de las tecnologías, lo que ha generado que la protección de este derecho se actualice y adapte con el fin de darle una protección adecuada y así tenga una vigencia efectiva en la realidad.

La aparición de Internet supone un gran desafío para los operadores del derecho, ya que deben plantear leyes, directivas, reglamentos que regulen las actividades que se desarrollan en los entornos virtuales. Eric Schmidt, ex CEO de la empresa Google, dijo que "Internet es la primera cosa que la humanidad ha construido y que la humanidad no entiende, el experimento más grande de anarquía que hemos tenido"[92], por lo que los gobiernos tienen la tarea y obligación de asegurar una eficaz protección a los derechos fundamentales de las personas, la misma que debe adaptarse a los cambios propios del mundo interconectado y globalizado en el que nos encontramos.

---

[92] REIGOSA, Carlos G. La verdad en Internet. *La Voz de Galicia*. 2019. Disponible en: https://www.lavozdegalicia.es/noticia/opinion/2019/10/14/verdad-internet/0003_201910G14P14992.htm

Dicho esto, surge la necesidad de explorar la constitucionalidad de la vigilancia masiva en el Perú. En particular, conviene responder a preguntas como, ¿hasta qué punto es legítima la recolección indiscriminada de datos en aras de la seguridad nacional? ¿Qué implicaciones tiene para los derechos fundamentales de los ciudadanos peruanos? ¿Cuál es el papel de las leyes y las instituciones gubernamentales en garantizar un equilibrio justo entre la protección de la intimidad y la prevención de amenazas a la seguridad nacional?

3.1 Uso indebido de la vigilancia masiva. Interceptación y manipulación de información para fines ilegítimos

Como hemos visto, la figura de la vigilancia masiva es usada con el fin de garantizar la seguridad nacional, siempre y cuando se respeten los derechos y libertades de las personas que consolidan una sociedad democrática. Permitir amplias excepciones a esta figura (al no regularla de manera correcta) para que se use de manera arbitraria y desproporcionada, puede llevar a que se afecte el día a día de las personas sin que estas se den cuenta, ya que en la era digital en la que nos encontramos y con las nuevas herramientas tecnológicas, la vigilancia se está haciendo más común a través de estos medios (cámaras de video vigilancia, redes sociales, aparatos móviles, entre otros).

Después de las revelaciones realizadas por Edward Snowden, los países han procurado reforzar sus leyes y ser más cautos con el uso de la vigilancia masiva, con el fin de garantizar la intimidad y no intromisión por parte del Estado, empresas, corporaciones u otras personas (sean naturales o jurídicas) en la esfera de reserva de las personas. Sin embargo, han sido muchos los casos donde se ha vulnerado la misma a través de la vigilancia masiva, esto debido a motivaciones políticas, personales o de cualquier otra índole, que quedan lejos de su verdadera naturaleza que es el de garantizar la seguridad nacional.

Un caso de estos y que tomó gran atención por parte de las personas fue el de Facebook Inc.- Cambridge *Analytica,* dado a conocer a mediados de marzo del año 2018. Una investigación llevada a cabo por *The New York Times*, *Channel* 4 y *The Guardian* reveló como una empresa privada se dedicaba a recopilar datos y utilizar información privada de más de cincuenta millones de personas a través de Facebook Inc. para manipularla con fines electorales, y así hacerles llegar información de manera más eficiente que influya de manera favorable en los clientes que la contrataban. Es así que influyó en la campaña presidencial de Donald Trump en 2016, en el proceso político del sí al Brexit y del no en el referéndum en Colombia por la paz ocurridos también el mismo año. Esta empresa privada es Cambridge *Analytica*, consultora británica que usa data para estudiar el comportamiento de los votantes,

pero no siempre de la manera más transparente, y muchas veces actuando como mecanismo de propaganda política.

Para tener el panorama más claro debemos remontarnos al año 2013 cuando Christopher Wylie, exempleado de Cambridge *Analytica* y pieza importante para que el caso sea de conocimiento público, estaba muy interesado en la idea de analizar datos psicológicos que las personas ponen en la red y así manipular dicha información. Es así que se contactó con Grupo *Strategic Communication Laboratories*-SCL Elections, una división dentro de una empresa especializada en materia de defensa y política. En esta empresa Wylie conoce a Alexander Nix, quien en ese entonces era director de SCL *Elections*, y pactaron continuas reuniones con Steve Bannon, quien en un futuro sería director de campaña de Donald Trump y estratega de la Casa Blanca, para hacerse de los servicios.

Cambridge *Analytica* fue contratada por Steve Bannon para favorecer la campaña de Trump en 2016 y tenía un plan perfecto para persuadir a los votantes, pero le faltaba lo más importante: la data. Es así que acudieron a Aleksandr Kogan, psicólogo social e investigador de la Universidad de Cambridge, quien fundó la empresa Global Science Research, mediante la cual se recopilaron datos y perfiles de usuarios de Facebook Inc. Kogan desarrolló un test de personalidad en 2014 basado en la psicometría, la cual señalaba que "la personalidad de un usuario podía predecirse fácilmente a través de los datos públicos que se extraían de sus rutinas de navegación (páginas web, redes sociales, etc.)"[93], muy vinculado a las emociones democráticas que influyan al momento de votar, y consiguió acceso a la información de más de 87 millones de usuarios de Facebook Inc. en 10 países.

Kogan vendió esta base de datos (desde fotos de perfil, edades, lugares de residencia e incluso mensajes privados) a Cambridge *Analytica* sin el permiso de Facebook Inc. Sin embargo, debemos advertir que "este incidente no fue una anomalía, fue la consecuencia inevitable de un sistema basado en recopilar y monetizar nuestra información: el modelo empresarial que la académica Shoshana Zuboff denomina «**capitalismo de vigilancia**». Los pilares fundamentales del modelo son: recopilar enormes cantidades de datos sobre personas, utilizarlos para deducir perfiles increíblemente detallados de su vida y su comportamiento, y monetizarlos vendiendo esas predicciones a otras partes, por ejemplo, anunciantes. Cambridge *Analytica* se limitó a utilizar ese mismo modelo básico para dirigirse a votantes,

---

93 VERCELLI, A. H., 2021. El extractivismo de grandes datos (personales) y las tensiones Jurídico-Políticas y tecnológicas vinculadas al voto secreto. *THEMIS Revista de Derecho*. Lima. 2021, no. 79, p. 116. ISSN: 2410-9592. Disponible en: https://doi.org/10.18800/themis.202101.006

en lugar de a consumidores"[94]. Wylie comentó que la principal fuente de Cambridge Analytica y por la que gastó cerca de un millón de euros en adquirirla fue la data de Facebook Inc. que les proporcionó Aleksandr Kogan.

Es así que Cambridge Analytica organizó y ejecutó una de las operaciones de mercadeo político más sofisticadas de la historia y además usó data y algoritmos para persuadir votantes de muchos países en el mundo como Nigeria, Brasil, Kenia, Reino Unido, etc. El 2 de mayo de 2018 la empresa anunció su cierre definitivo[95] debido a los altos costos que tuvo que pagar en materia legal para ejercer su defensa y por la masiva pérdida de clientes.

Otro caso que generó (y sigue generando) mucha repercusión es el "caso Pegasus". El programa Pegasus es un software espía invisible que cuenta con una instalación remota y automática, capaz de acceder a casi toda la totalidad de un dispositivo móvil que ha sido infectado por el mismo, logrando extraer mensajes de texto, fotografías, contactos, correos electrónicos, así como tener la ubicación histórica y en tiempo real del objetivo e incluso puede escuchar conversaciones de los propietarios activando en secreto sus cámaras o micrófonos, siendo considerado el software espía más completo y sofisticado de todos los tiempos. Una de las razones de peligrosidad de este programa "es que no requiere acción alguna de parte del propietario de un celular para que el aparato sea hackeado por el programa de espionaje. La mayoría de los virus en los aparatos celulares se activa cuando una persona hace funcionar el enlace que se le ha enviado, o cuando va a un sitio e ingresa con un clic"[96]. Es decir, el programa se instala sin que el propietario del teléfono lo sepa, pasando totalmente desapercibido para la víctima evadiendo medidas de protección de cualquier aplicación de su celular.

Pegasus fue descubierto en agosto de 2016 luego de una fallida instalación en un teléfono de una activista árabe de derechos humanos. Investigaciones llevadas a cabo por The New York Times y The Times of Israel informaron que Emiratos Árabes Unidos probablemente usó este programa desde el 2013. Tras unas demandas legales, se descubrió que quien estaba detrás de Pegasus era la firma cibernética israelí NSO Group, empresa que dota de tecnología a "las agencias gubernamentales para prevenir e investigar delitos de

---

94 AMNISTÍA INTERNACIONAL. *El gran hackeo: Cambridge Analytica es sólo la punta del iceberg*. Londres: Amnistía Internacional. 2019. Disponible en: https://www.amnesty.org/es/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/

95 Se transformó en otra empresa llamada Emerdata.

96 MUÑOZ V., H., Democracias en peligro. Regresión democrática en Latinoamérica y propuestas de futuro. Primera edición. Santiago, Chile: Editorial Catalonia. 2023. ISBN: 978-956-415-079-6. Disponible en: https://books.google.com.pe/books?id=zb31EAAAQBAJ&pg=PT87&hl=es&source=gbs_toc_r&cad=1#v=onepage&q&f=false

terrorismo, organización criminal y delitos graves"[97], que confirmó la existencia del programa. Sin embargo, NSO Group se defiende diciendo que Pegasus está destinado a la lucha contra el terrorismo y que sólo es vendido a agencias gubernamentales con el fin de garantizar su seguridad nacional.

El 18 de julio de 2021 se dio a conocer el Proyecto Pegasus, el mayor estudio realizado sobre el alcance de este software espía. Es una investigación llevada a cabo por un consorcio de periodistas pertenecientes a 17 grupos mediáticos (entre los que destacan The Guardian, The Washington Post, Frontline, Le Monde, entre otros) de diferentes países del mundo, bajo la coordinación de Forbidden Stories[98] y con el apoyo técnico de Amnistía Internacional[99]. Se descubrió también que el programa había sido utilizado en más de 50 000 números de teléfonos fijados, entre 2016 y 2021, por varios gobiernos como objetivo para ser espiados y vigilados por este software israelí, entre lo que se incluyen teléfonos de al menos 600 políticos y 180 periodistas[100]. Asimismo, la investigación señala que el programa ha sido utilizado como arma por gobiernos represivos para perseguir y vigilar sin control alguno a periodistas, empresarios, opositores a los gobiernos de turno, activistas políticos, etc.; lo que afecta en gran medida "el derecho a la intimidad y puede violar también los derechos a la libertad de expresión, de opinión, de asociación y de reunión pacífica"[101]. El 18 de enero del 2022 salió a la luz que la policía de Israel utilizaba Pegasus para espiar a sus ciudadanos. Entre las víctimas están alcaldes, activistas políticos, así como antiguos empleados gubernamentales, que fueron espiados sin ninguna orden de registro o escucha que autorizara su vigilancia[102]; al igual que jefes de Estado o de Gobierno, destacando el presidente de Francia Emmanuel Macron, el ex primer ministro del Reino Unido Boris Johnson y el presidente del Gobierno de España Pedro Sánchez; y entre los clientes de Pegasus aparecen

---

97 DUEÑAS CHÁVEZ, G. M. y SEÑA MANGUINURY, J. E., *Fortalecimiento de la capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet* Trabajo tesis de maestría. Pontificia Universidad Católica del Perú, Gobierno y Políticas Públicas. 2023. Disponible en: http://hdl.handle.net/20.500.12404/26812

98 Forbidden Stories es una red de periodistas que se encargan de proteger y publicar trabajos de periodistas que han visto vulnerados sus derechos y libertades, debido a diversas situaciones como amenazas, extorsiones, chantajes, etc.

99 Amnistía Internacional es un movimiento global que tiene como misión velar por los derechos humanos, realizando labores de investigación para evitar e impedir agresiones contra los mismos.

100 VISUALPOLITIK. *PEGASUS: El sistema espía de Israel que ha escandalizado al mundo* [video]. *YouTube*. 09 de febrero de 2022. Disponible en: https://www.youtube.com/watch?v=XE7JptwDPec

101 AMNISTÍA INTERNACIONAL. *Proyecto Pegasus: Un año después, la crisis de los programas espía continúa, mientras el sector de la vigilancia sigue sin estar sometido a control*. 2022. Londres: Amnistía Internacional. Disponible en: https://www.amnesty.org/es/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/

102 El MUNDO. La Policía israelí espió a sus ciudadanos a través de Pegasus. Israel. 2022. Disponible en: https://www.elmundo.es/internacional/2022/01/18/61e6f71521efa0621e8b456f.html

los gobiernos de 11 países, entre los que destacan Hungría, India, México, Ruanda, Marruecos y Arabia Saudita, incluso ha llegado a ser utilizado por los países de El Salvador y Polonia.

Pegasus tomó gran relevancia en España debido a un escándalo de espionaje virtual en 2022 realizado con este programa. El 22 de marzo de 2022 Citizen Lab, un proyecto de ciberseguridad de la Universidad de Toronto que busca garantizar la seguridad global y los derechos humanos cuando se hace uso de tecnologías de información y comunicación (TIC), publicó un informe[103] que identificaba a decenas de políticos independentistas y activistas catalanes de las más altas esferas (al menos 65 personas) cuyos celulares habían sido atacados por Pegasus entre 2017 y 2020. A esto se le conoció como el Catalangate, por lo cual el congreso español aprobó en diciembre del 2023 la creación de una comisión de investigación para el mismo.

En mayo del 2022, en medio del escándalo suscitado por el informe de Citizen Lab, el Centro Criptológico Nacional[104] descubrió indicios de que el presidente del gobierno español Pedro Sánchez, la ministra de Defensa Margarita Robles, el ministro de Agricultura Luis Planas y el ministro del Interior Fernando Grande-Marlaska, habían sido víctimas de un ataque externo con el programa Pegasus.

El Gobierno presentó una denuncia a la Audiencia Nacional, que recayó en el titular del Juzgado Central de Instrucción Cuatro, el juez José Luis Calama, que inició una investigación en secreto el 3 de mayo del 2022. El magistrado archivó provisionalmente la investigación en julio del 2023 debido a la nula cooperación jurídica por parte de Israel (lugar del domicilio de NSO Group). Sin embargo, el 23 de abril del 2024 el juez decidió reabrir el caso "tras recibir una Orden Europea de Investigación (OEI) emitida por las autoridades judiciales de Francia que incorpora una investigación llevada a cabo en 2021 por múltiples infecciones de teléfonos de periodistas, abogados, personalidades públicas y asociaciones gubernamentales y no gubernamentales, así como miembros de gobierno francés, ministros y diputados, con el software Pegasus"[105]. Como hemos podido observar, Pegasus es utilizado

---

103 THE CITIZEN LAB. ¿Harías clic? Munk school. University Toronto. 2022. Disponible en: https://catalonia.citizenlab.ca/es/

104 Organismo español adscrito al Centro Nacional de Inteligencia (CNI), creado el año 2004 mediante Real Decreto 421/2004, encargado de garantizar la seguridad de las tecnologías de la información y comunicaciones (TIC), de material criptológico y de información clasificada, con el fin de contribuir a la ciberseguridad española y responder de manera eficaz a ciberataques y ciberamenazas; utilizando y desarrollando para ello políticas, procedimientos y tecnologías que ayuden a conseguir un ciberespacio más seguro libre de amenazas y de injerencias no deseadas.

105 COMUNICACIÓN PODER JUDICIAL. *Audiencia Nacional reabre la causa Pegasus ante nuevos datos aportado por Francia*. 2024. España: Disponible en: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-reabre-la-causa-Pegasus-ante-nuevos-datos-aportados-por-Francia

con fines específicos, es decir, no busca espiar la información de ciudadanos comunes y corrientes, sino de altos cargos gubernamentales u otros relacionados con un objetivo predeterminado (que incluye a periodistas, activistas, empresarios, entre otros).

Después de observar estos ejemplos donde la tecnología ha sido utilizada de manera ilegal, vulnerando derechos y libertades de las personas para conseguir fines individuales transgrediendo barreras legales, es menester señalar que el Perú no ha sido ajeno a este tipo de acciones. Es por ello que veremos algunos casos ocurridos en territorio peruano, en los que se busca perjudicar a selectos grupos de personas a través de la utilización de la vigilancia masiva para obtener diversas finalidades sin respetar los derechos y libertades de las personas.

3.2 Vigilancia masiva en Perú: Riesgos de interceptación y uso ilícito de información

3.2.1 *La implicancia de la vigilancia masiva en la época del terrorismo*

Después de haber advertido que gobiernos como Estados Unidos, España, Reino Unido, Israel, Colombia (por nombrar a algunos), optan por hacer uso de la vigilancia masiva que incluye interceptación de comunicaciones, rastreo de equipos, cámaras de video vigilancia, geolocalización, entre otros; en aras de conseguir una protección de su soberanía, seguridad nacional o ya sea simplemente por intereses políticos, es necesario rememorar en qué época de nuestra historia reciente el Perú ha sido también víctima de dichas injerencias.

Comenzamos con la década del 80, una época que marcó uno de los periodos más oscuros y violentos en el país; la insurgencia de grupos armados como Sendero Luminoso y el MRTA (Movimiento Revolucionario Túpac Amaru), desataron una ola de violencia indiscriminada, atentados y enfrentamientos armados con el objetivo de desestabilizar el país y promover sus ideales políticos, los cuales dejaron miles de víctimas y un profundo impacto en la sociedad peruana.

Durante esta época, las fuerzas del orden, en especial el Ejército y la Policía Nacional, llevaron a cabo operaciones militares y policiales para combatir a estos grupos insurgentes, lo que generaría un escenario propicio para el desarrollo de las actividades de vigilancia masiva a los ciudadanos por parte del Estado, teniendo como fundamento la seguridad nacional. Y es que el terrorismo tenía múltiples objetivos que "pueden mencionarse como actos dirigidos a subvertir total o parcialmente el orden político constituido y ponerlo en peligro, destruir el orden constitucional, alterar la seguridad y el orden público con fines políticos y sociales"[106].

---

[106] TRAMONTANA CUBAS, D. *La violencia terrorista en el Perú, Sendero Luminoso, y la protección internacional de los derechos humanos.* Revista Persona No.25 Argentina. 2004. Disponible en: https://www.revistapersona.com.ar/Persona25/25Tramontana1.htm

En la época del terrorismo la vigilancia era ejercida únicamente por los servicios de inteligencia del Estado y que en cierto sentido se podría encontrar sustento a dichas prácticas teniendo en cuenta el momento convulsionado por el que pasaba el país. Sin embargo, con el ingreso de Alberto Fujimori a la presidencia y con él su asesor Vladimiro Montesinos, se empezaría a utilizar los aparatos del sistema de inteligencia para fines personales y políticos, ya sea para interceptar comunicaciones de congresistas de oposición, seguir a militares que no iban acorde con sus lineamientos o investigar y perseguir a civiles.

Es importante resaltar el caso de la vigilancia estatal realizada en el gobierno fujimorista por la figura de Vladimiro Montesinos, encargado de dirigir las labores del Sistema de Inteligencia Nacional[107] (en adelante SIN), tema que él certificaría más adelante[108]. La posición de dominio que tuvo sobre el SIN y la cantidad de información recogida a través de prácticas[109] de vigilancia como interceptaciones telefónicas, seguimiento y grabaciones, permitieron al régimen un control efectivo sobre el país y sobre la clase política. De esta manera, el gobierno influía en las decisiones políticas y militares del país.

Para asegurarse el control sobre sus aliados y oponentes, Montesinos grababa en secreto las reuniones y transacciones en las que participaba; a estas grabaciones se les denominó "los Vladivideos", donde se documentan sobornos, manipulación de medios de comunicación, compra de congresistas, extorsión y otros actos ilícitos. En estos videos, se puede ver a Montesinos entregando grandes sumas de dinero a diversos individuos a cambio de lealtad política o favores. Los más notorios son los videos donde se evidencia la compra de congresistas de la oposición para que se pasen al partido oficialista, facilitando así el control del Congreso por parte del gobierno de Fujimori.

Durante la década de los noventa, Montesinos "llevó, golpe de Estado mediante, al SIN de la insignificancia al desarrollo y de ahí al control real del Estado y el Gobierno, todo eso sin haber sido jamás el jefe formal del SIN"[110]. Terminado el gobierno en el año 2000 y revelados ya los actos de corrupción y mal manejo del SIN, éste último sería desactivado en el año 2001, mediante Ley N° 27351, siendo sustituido por el Consejo Nacional de Inteligencia (CNI) y por la Dirección Nacional de Inteligencia Estratégica (DINIE). En el año 2006 se establecería con la Ley N° 28664 el Sistema de Inteligencia Nacional (en adelante SINA) y la

---

107 La cual se vio fortalecido con la promulgación del Decreto Ley 25635, en donde se le daba rango ministerial y dependía del Presidente de la República.

108 En concreto durante el proceso penal que se le siguió por el delito de usurpación de funciones, el cual aceptó y fue condenado a 9 años y 4 meses de prisión efectiva en 2002. Recopilado de: https://elcomercio.pe/politica/justicia/principales-condenas-vladimiro-montesinos-interactivo-399150

109 Se excluye la vigilancia informática propiamente dicha por las limitaciones tecnológicas de la época.

110 GORRITI, G., 2015. *Espías*. España. El País. Disponible en: https://www.idl-reporteros.pe/espias/

Dirección Nacional de Inteligencia (en adelante DINI); esta última seria protagonista de un nuevo escándalo, que se abordara en el siguiente acápite.

Las prácticas documentadas durante el gobierno de Fujimori, que involucraron el uso del SIN para fines personales y políticos, muestran un claro ejemplo de cómo estos órganos de inteligencia y seguridad que históricamente han tenido como función principal la recolección y análisis de información para la protección del Estado, pueden ser desviados de sus propósitos originales. Estas prácticas no solo han perdurado a lo largo del tiempo, sino que en algunos casos se han intensificado, pues, aunque "los políticos peruanos ya han visto las consecuencias de la vigilancia se les sale de las manos; pero parece que la tentación de otorgar mayores poderes sin supervisión permanece"[111].

La consolidación de la vigilancia estatal con fines políticos en la década de los noventa marcó un precedente significativo en la historia reciente del Perú. Los eventos de ese periodo estuvieron caracterizados por la utilización de mecanismos de inteligencia para controlar y coaccionar a opositores y ciudadanos. Este contexto se ha perpetuado en la memoria colectiva y en la percepción pública, sirviendo como un parámetro comparativo para evaluar las acciones del Estado en materia de derechos civiles y libertades individuales. Aunque la existencia de órganos de inteligencia, por sí sola, no implica automáticamente una vigilancia invasiva y masiva, su utilización en antaño con fines políticos ha generado (y genera) la sospecha y el temor de la sociedad hacia estas instituciones.

Aunque el terrorismo disminuyó y con ello algunos de los justificativos más extremos para la vigilancia, la herencia de la década de los noventa sigue influyendo en la manera cómo se perciben y se ejecutan las políticas de seguridad y vigilancia en el Perú. A lo largo del tiempo, la percepción de una vigilancia estatal no ha disminuido, y a pesar de las reformas y cambios en las instituciones de inteligencia, persiste una desconfianza hacia estas, especialmente en contextos políticos tensos. En este sentido, la vigilancia, en muchos casos, continúa siendo vista como una amenaza a la intimidad y a los derechos fundamentales, lo que evidencia la necesidad de un equilibrio entre la seguridad nacional y la protección de las libertades individuales.

Por ello, este apartado pretende evidenciar los primeros indicios de la vigilancia masiva en el Perú; aun cuando no se utilizaban tecnologías digitales avanzadas como en la vigilancia masiva contemporánea. El Estado peruano implementó estrategias de vigilancia intensiva y control social que, en algunos casos, se alejaron de la legalidad y respeto a los

---

111 CARLSON, K. *La triste historia del Perú con la vigilancia, y cómo solucionarla*. 2016. Disponible en: https://www.eff.org/es/deeplinks/2016/10/la-triste-historia-del-peru-con-la-vigilancia-y-como-solucionarla

derechos civiles. Es importante recordar que las lecciones del pasado deben guiarnos hacia una sociedad democrática, en donde haya un equilibrio entre la seguridad con el respeto a los derechos humanos, para así evitar los abusos de poder.

3.2.2 *Vigilancia estatal. Caso de la Dirección Nacional de Inteligencia*

En el año 2006, el Congreso de la República del Perú estableció el SINA y reguló el funcionamiento de la DINI a través de la Ley N° 28664, la cual fue derogada por el Decreto Legislativo N° 1141. Esta ley tiene como objetivos principales: "1. Producir el conocimiento útil para el proceso de toma de decisiones en materia de seguridad nacional, 2. Proteger las capacidades nacionales frente a acciones de inteligencia u otras encubiertas provenientes de actores que representan amenazas a la seguridad nacional; y, 3. Realizar actividades destinadas a alcanzar la seguridad digital en materia de seguridad nacional"[112].

El SINA es "el conjunto de principios, normas, procedimientos, técnicas e instrumentos del Estado peruano, funcionalmente vinculados, que provee de inteligencia estratégica, militar y policial al país"[113]. Por tanto, su misión incluye identificar y evaluar amenazas a la seguridad nacional, así como proponer políticas y medidas para enfrentarlas de manera efectiva. Por otro lado, la DINI "es el órgano rector del sistema de inteligencia nacional y la organización más importante en materia de inteligencia del Perú"[114], constituyendo el órgano central del SINA, y tiene la responsabilidad de dirigir, coordinar y supervisar las actividades de inteligencia en el ámbito nacional.

El Decreto Legislativo N° 1141, en su artículo 3, establece los principios rectores que deben regir las actividades de inteligencia, destacando la legalidad, la legitimidad, el respeto a los derechos humanos, la pertinencia, confidencialidad de la información obtenida por la inteligencia y la exclusividad de las actividades de inteligencia a los componentes del SINA. Esto proporciona un marco normativo que equilibra la necesidad de una sólida inteligencia estatal con la protección de los derechos fundamentales de los ciudadanos. Además, la ley establece mecanismos de control y supervisión para garantizar el cumplimiento de la normativa y prevenir posibles abusos. Tales mecanismos son, en primer lugar, el control judicial (artículo 32), según el cual las operaciones especiales de obtención de información son ejecutadas exclusivamente por el SINA y requieren autorización judicial previa por

---

112 GOBIERNO DEL PERÚ. *"Dirección Nacional de Inteligencia"*. En: gob.pe, s.f., párr. 14. Disponible en: https://www.gob.pe/institucion/dini/organizacion

113 GOBIERNO DEL PERÚ. *"Sistema de Inteligencia Nacional (SINA)"*. En: gob.pe, s.f., párr. 2. Disponible en: https://www.gob.pe/27632-sistema-de-inteligencia-nacional-sina

114 ARIAS ARÓSTEGUI, E. A., *Un caso de transferencia de política: entre el éxito y el fracaso, la reforma de inteligencia durante el gobierno de Alejandro Toledo*. Trabajo tesis de licenciatura. Pontificia Universidad Católica del Perú, Ciencia Política y Gobierno. 2017. Disponible en: http://hdl.handle.net/20.500.12404/8972

cualquiera de los dos jueces superiores Ad Hoc del Poder Judicial. Este requisito asegura una supervisión independiente y una revisión judicial de las acciones planificadas, proporcionando una capa adicional de control para prevenir posibles abusos de poder.

En segundo lugar, el control legislativo (artículo 36), que implica que la Comisión de Inteligencia del Congreso de la República está facultada para fiscalizar las actividades del SINA. Esta comisión puede solicitar información clasificada y no clasificada, investigar de oficio y requerir informes anuales sobre las actividades de inteligencia. Este mecanismo legislativo de supervisión garantiza la transparencia y la rendición de cuentas de las operaciones de inteligencia, fortaleciendo el control democrático sobre estos organismos.

Estos mecanismos de control refuerzan la estructura normativa del Decreto Legislativo N° 1141, asegurando que las actividades de inteligencia del Estado se realicen de manera responsable y respetuosa de los derechos humanos. Pese a lo mencionado anteriormente, la DINI ha sido cuestionada por su papel en presuntas actividades de espionaje político y seguimiento ilegal a periodistas, políticos y ciudadanos en general. Se han denunciado casos de interceptación de comunicaciones y seguimientos sin autorización judicial, lo que ha generado preocupación sobre el respeto a la intimidad y los derechos individuales. En el año 2015, la DINI estuvo envuelta en un escándalo de vigilancia estatal, realizando más de cien mil quinientas búsquedas ilegales, reglajes y seguimientos a personalidades clave de la política y de la prensa nacional de ese entonces, como Marisol Espinoza, quien ejercía el cargo de vicepresidenta de la República; Alan García, expresidente; Yhony Lescano, congresista de la República; Jorge del Castillo, dirigente del APRA; y Fernando Rospigliosi, periodista, entre otros[115]. Todos estos hechos fueron los que llevaron a la censura de la primera ministra del gobierno de Ollanta Humala, Ana Jara.

La censura se sostuvo en varios argumentos, de los que destacan los siguientes:

> (…) la Dirección Nacional de Inteligencia (DINI) al espiar y armar expedientes de varios miles de ciudadanos peruanos -muchos de los cuales pertenecen a partidos de oposición- y sus familiares, referidos al patrimonio personal y que se encuentra registrado en SUNARP. (…) Que este gravísimo suceso no hace sino confirmar la nefasta utilización que se está haciendo de los elementos de la inteligencia nacional. [Y teniendo en cuenta] que la DINI, asimismo, acorde al Decreto Legislativo N°1141, es un organismo público ejecutor del Sistema Nacional de Inteligencia (SINA), depende funcionalmente del presidente de la República y se encuentra adscrita a la

115 AYMA, D. *"El trabajo de la revista Correo Semanal y del diario Correo: La DINI al desnudo".* En: Diario Correo. 2015. Disponible en: https://diariocorreo.pe/politica/la-dini-al-desnudo-576539/

> Presidencia del Consejo de ministros, por lo que la señora Ana Jara Velásquez, presidenta del Consejo de ministros, resulta siendo la directa responsable política de estos lamentables hechos. (…) [Por tal motivo], CENSURAR a la presidenta del Consejo de ministros, señora Ana Jara Velásquez, por su confirmada incapacidad para seguir desempeñando el cargo[116].

La censura de Ana Jara se produjo en medio de un escándalo de espionaje. La DINI había sido acusada de espiar y realizar reglaje a políticos, periodistas, empresarios y otras figuras públicas sin autorización. Estas actividades se habrían llevado a cabo durante varios años y, aunque comenzaron antes de su gestión, la responsabilidad recayó sobre Jara, dado que el escándalo estalló durante su mandato como presidenta del Consejo de ministros. Fue pues este hecho el que motivo al gobierno a anunciar la desactivación de la DINI por 180 días para iniciar un proceso de reestructuración, indicativo de que la política adoptada para dirigir el sistema de inteligencia estatal no era la adecuada, pues en menos de 15 años se había reacomodado dos veces la organización del sistema de inteligencia.

3.2.3 *Dirección antidrogas de la Policía Nacional del Perú y su vínculo con las interceptaciones telefónicas*

Otra institución pública del Perú que ha enfrentado duras críticas por su posible participación en casos de interceptaciones telefónicas ilegales ha sido la Dirección Antidrogas de la Policía Nacional del Perú (en adelante DIRANDRO). La DIRANDRO, creada en 1991 mediante el Decreto Legislativo N° 744, es una división especializada encargada de investigar y combatir el tráfico ilícito de drogas y delitos conexos en el país. Para realizar esta función, la DIRANDRO colabora estrechamente con otras instituciones del Estado, organismos internacionales y la sociedad civil en la lucha integral contra las drogas, vinculándose estratégicamente con las direcciones especializadas para combatir el terrorismo y el lavado de activos, estableciendo vínculos de estrategia funcional; y, coordina con gobiernos y entidades internacionales la persecución de la criminalidad organizada, siendo reconocida a nivel internacional la eficiencia y alta calificación profesional del policía antidrogas[117]. Sin embargo, esta institución no ha estado exenta de escándalos.

---

116 DEPARTAMENTO DE INVESTIGACIÓN Y DOCUMENTACIÓN. Mociones de censura. Periodo Parlamentario 2011-2016 (27julio de 2011 al 26 julio de 2016). *Reporte de Antecedentes Parlamentarios*. 2015. Congreso de la República. Número de moción 12623, ítem 10, párr. I-II-IV-V). Disponible en: https://www2.congreso.gob.pe/Sicr/TraDocEstProc/InfSiste_2013.nsf/C8CE491805E736C405257AF700743CC6/15C87144714CAA8505257C0D005BA5C5?OpenDocument

117 DIRECCIÓN ANTIDROGAS. *Trabajando por el Perú y el Mundo*. Lima: vol. nº 1, 2022. Disponible en: https://dirandro.policia.gob.pe/publicaciones/revista1.pdf

En el año 2011 fue acusada de mantener una sala de interceptación telefónica ubicada en el sexto piso de su oficina central, donde se trabajaba en un proyecto llamado "Programa Constelación", que dirigía el Ministerio Público y permitía interceptar 300 líneas de teléfono celular a la vez[118]. Ante esta acusación, el congresista Daniel Abugattás se dirigió a la DIRANDRO para investigar si este lugar se utilizaba para llevar a cabo interceptaciones telefónicas ilegales de políticos nacionalistas (del partido Gana Perú), señalando que había "una mafia al más puro estilo montesinista que ya comenzó a hacer estas escuchas. El chuponeo está comprobado, las conversaciones son reales"[119].

El jefe de la DIRANDRO de aquel entonces, Carlos Morán y el fiscal superior Jorge Chávez Cotrina, en una conferencia de prensa negaron dichas acciones con las siguientes declaraciones: "En la DIRANDRO no se practican interceptaciones telefónicas ilegales. Éstas tienen que contar con una autorización judicial motivada y tramitada previamente por el fiscal del caso"[120] y recalcaron "que la ley sólo otorga la facultad de escucha al fiscal, en especial en casos de delitos graves, entiéndase terrorismo, tráfico ilícito de drogas, secuestros, tráfico de personas, corrupción, etc.; y para ello es necesario que la compañía operadora de telefonía tenga que abrir su base de datos y el fiscal es la única persona que puede programar los números que son el blanco objetivo"[121.]

Este incidente generó un llamado a una mayor transparencia y rendición de cuentas por parte de la institución para garantizar el respeto irrestricto de los derechos fundamentales, sobre todo del derecho a la intimidad, que sería el mayormente afectado. En definitiva, es crucial que se realicen investigaciones imparciales y se tomen medidas para asegurar que la DIRANDRO actúe dentro del marco legal establecido. La rendición de cuentas, la transparencia y el fortalecimiento de los mecanismos de control son fundamentales para restaurar la confianza en las instituciones y preservar el Estado de derecho en el país.

3.2.4 *Proyecto Pisco. Sistema electrónico de interceptación*

A fines del año 2012, la DINI realizó la compra de un equipo de interceptación telefónica valorizado en 55 millones de soles a la empresa israelí de inteligencia electrónica

---

118 CASTILLA, O. *Así funciona Constelación, el sistema de escucha telefónica de la Dirandro*. En: Diario El Comercio. 2011. Disponible en: https://elcomercio.pe/sociedad/lima/asi-funciona-constelacion-sistema-escucha-telefonica-dirandro-noticia-1341509/

119 PANAMERICANA. *Congresista Daniel Abugattás denunció interceptación telefónica desde sede policial*. 24 horas edición central. Redacción Panamericana, 2011. Disponible en: https://panamericana.pe/24horas/elecciones2011/86301

120 MINISTERIO DEL INTERIOR. *Dirandro no realiza Interceptaciones Ilegales***.** Oficina de Comunicación Social**.** 2011. Disponible en: https://www.mininter.gob.pe/content/dirandro-no-realiza-interceptaciones-ilegales

121 Ibídem.

Verint Systems Ltd. al que se le denominó Proyecto Pisco. Este sistema electrónico consistía en un plan de rastreo de comunicaciones a gran escala conformado por un conjunto de redes, softwares y computadoras que estaría a cargo de la Policía Nacional del Perú para luchar contra el crimen organizado y el narcotráfico.

Asimismo, tiene la capacidad de interceptar hasta tres mil líneas telefónicas simultáneamente y "puede intervenir cualquier tipo de comunicación a través de telefonía fija, telefonía celular, y cualquier otro servicio sobre Internet (chat, *webmail*, VoIP, y navegación por Internet). Además, ofrece la posibilidad de brindar alertas sobre la ubicación o la proximidad de los equipos interceptados gracias a la geolocalización. Para su funcionamiento no es necesario que intervengan las empresas de telecomunicaciones dado que la interceptación se produce directamente"[122]. Esto pone en peligro las comunicaciones privadas de millones de peruanos, lo que puede llegar a causar una sensación de temor y preocupación por parte de los ciudadanos.

La adquisición de este programa fue realizada de manera irregular debido a que no se siguieron los procedimientos establecidos para la compra de bienes o servicios por parte del Estado peruano. Se encontró que la compra se efectuó sin un proceso de licitación y sin sustentar la necesidad de por qué se requería el equipo, es decir, no se siguieron los procedimientos y requisitos básicos para realizar esta compra. Todo esto llevó a que esta adquisición sea investigada por la Contraloría y por la Comisión de Inteligencia del Congreso de la República[123].

Si bien es cierto que el equipo tuvo un costo de 55 millones de soles como mencionamos al inicio, a esto hay que sumarle un adicional de 10 millones de soles relativos a la infraestructura para la instalación de dicho equipo, por lo que el Proyecto Pisco costó unos 65 millones de soles. Fue un pedido expreso del entonces presidente Ollanta Humala, información que se supo gracias a un documento suscrito por el ex jefe de la DINI, Víctor Gómez Rodríguez.

El proceso de adquisición empezó en octubre del 2012 y culminó en abril del 2013, esto tras una lista de cotizaciones realizadas por el entonces jefe del gabinete de asesores de la DINI, Iván Kamisaki Sotomayor, a "seis empresas: Digitro, de Brasil; Penlink y Frost & Sullivan, de Estados Unidos, Utimaco, de Alemania; y Nice Systems y Verint Systems, de

---

122 MORACHIMO, M. El sistema de espionaje de las comunicaciones que dejó Humala. *Hiperderecho*. 2016. Disponible en: https://hiperderecho.org/2016/08/proyecto-pisco-skylock-peru-verint/#

123 América Noticias. *DINI compró millonario equipo de "chuponeo" a pedido del presidente Humala* [video]. *YouTube*. 09 de agosto de 2015. Disponible en: https://www.youtube.com/watch?v=PxP59hHEDjE&t=27s

Israel"[124]. Después de realizado esto, Kamisaki presentó un informe de cotizaciones de equipos y precios a Víctor Gómez, dando inicio así al proceso de adquisición. Ante esto, el Primer Despacho de la Fiscalía Provincial Corporativa Especializada en Delitos de Corrupción de Funcionarios de Lima Sur presentó, en octubre del 2023, una acusación fiscal por la comisión del delito de colusión agravada en perjuicio del Estado, solicitando diez años y cuatro meses de prisión contra el expresidente Ollanta Humala Tasso, el ex jefe de la DINI Víctor Gómez Rodríguez, el exjefe del gabinete de asesores de la DINI Iván Kamisaki Sotomayor y el representante en el Perú de la empresa Verint Systems Ltd., el señor Shafrir Paz[125].

3.3 Decreto Legislativo N° 1182. Ley Stalker

En nuestro país la seguridad se ha convertido en un tema de máxima importancia en la agenda política peruana desde hace varios años. Es así que en julio del 2015 se aprobó el Decreto Legislativo N° 1182 o también llamado "Ley Stalker", que busca principalmente combatir la delincuencia y el crimen organizado. Esta norma plantea fortalecer al cuerpo policial peruano, permitiéndole que acceda sin orden judicial a la ubicación de cualquier dispositivo conectado a la red celular (teléfonos móviles, *tablets* o cualquier otro dispositivo).

El artículo 2 de este decreto establece que su finalidad es "(…) regular el acceso de la unidad especializada de la Policía Nacional del Perú, en casos de flagrancia delictiva, a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar". En otras palabras, la ley pretende establecer normativas o procedimientos específicos para controlar y limitar el acceso de una unidad especializada de la Policía Nacional del Perú a la localización o geolocalización de teléfonos móviles u otros dispositivos electrónicos similares en situaciones donde se está cometiendo un delito flagrante.

En lo que se refiere al objeto de la norma, según su artículo 1° es "(…) fortalecer las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, a través del uso de tecnologías de la información y comunicaciones por parte de la Policía Nacional del Perú". En otras palabras, la ley establece un marco legal que permite a la misma utilizar herramientas digitales para recopilar y analizar información, para actuar de manera más eficaz en la detención y persecución de delitos, asegurando que el acceso a estos

---

124 YOVERA, D. DINI adquirió sistema Pisco por orden de Ollanta Humala. *El Comercio*. 2015. Disponible en: https://elcomercio.pe/politica/gobierno/dini-adquirio-sistema-pisco-orden-ollanta-humala-192136-noticia/?ref=ecr

125 MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN. Fiscalía Anticorrupción presenta acusación y pie 10 años de prisión contra el expresidente Ollanta Humala. Gob. Pe. 12 octubre 2023. Disponible en: https://www.gob.pe/institucion/mpfn/noticias/848836-fiscalia-anticorrupcion-presenta-acusacion-y-pide-10-anos-de-prision-contra-el-expresidente-ollanta-humala

datos se realice de manera controlada y específica; así como para mejorar la coordinación y la comunicación entre las diferentes unidades policiales.

No obstante, con esta ley el Estado trata de tutelar la seguridad ciudadana permitiendo a las fuerzas policiales requerir a las compañías de telecomunicaciones los datos de ubicación o geolocalización de dispositivos móviles y electrónicos, sin necesidad de obtener previamente la autorización de un juez o fiscal. Es por ello que este decreto ha sido objeto de críticas, pues ha cambiado "la vigilancia de los registros de comunicaciones basada en la sospecha individualizada, al registro masivo de comunicaciones para la vigilancia de personas comunes sin sospecha"[126].

El Decreto Legislativo N° 1182 señala que deben concurrir los siguientes supuestos para su aplicación, según lo establecido en su artículo 3: 1. Cuando se tratara de un delito flagrante; 2. Cuando la sanción por el delito fuera mayor a 4 años de pena privativa de la libertad; y, 3. Cuando el acceso a esta información fuera necesario para la investigación. Sin embargo, el 16 de julio de 2021, se modificó este decreto por la Ley N° 31284, mediante la cual "los supuestos para habilitar a la policía a solicitar los datos de geolocalización han sido ampliados para incorporar a las investigaciones preliminares por delitos contra la vida, el cuerpo y la salud; delitos contra la libertad; delitos contra el patrimonio; delitos contra la administración pública; delitos de lavado de activos; delitos de trata de personas; delitos de tráfico ilícito de drogas; delitos de minería ilegal; más aquellos delitos comprendidos en la Ley 30077, ley contra el crimen organizado"[127]. Asimismo, se modificó el artículo 4 correspondiente al procedimiento donde "señala que la entrega de los datos de localización o geolocalización o rastreo a la Policía debe darse en un plazo máximo de 24 horas de solicitada la información y durante las 24 horas del día de los 365 días del año"[128].

Consideramos importante hacer un comentario sobre este decreto pues aun cuando no se haya visto involucrado en problemas como tal en su aplicación, la geolocalización es una forma de manifestación de la vigilancia masiva, tema que abarca nuestra tesis. Es así que, al revisar el tenor de esta ley, no se descarta que, pese a que existen presupuestos para su aplicación, siempre pueden surgir arbitrariedades en su materialización, por lo que es importante fijarnos en el procedimiento que sigue este decreto para que en su ejercicio no exista una extralimitación y en caso exista, esta sea justificada razonablemente. Para

---

126 RODRIGUEZ, K., *Ley Stalker, o cómo el gobierno legalizó la vigilancia masiva a peruanos inocentes*. En: Electronic Frontier Foundation, párr. 3. 2015. Disponible en: https://www.eff.org/es/deeplinks/2015/08/stalker-law-como-gobierno-peru-legalizo-vigilancia-ciudadanos

127 ESCOBEDO, C.,2021. *Modificaciones a la «Ley Stalker» en Perú*. En: iapp, párr. 4-5. Disponible en: https://iapp.org/news/a/modificaciones-a-la-ley-stalker-en-peru-2

128 Ibídem.

garantizar que la obtención de la información solicitada se realice de manera justa y dentro de los límites legales, evitando posibles abusos o violaciones a la intimidad de los ciudadanos, es necesario que se encuentre un equilibrio entre la necesidad de aplicar la ley con el respeto a los derechos individuales y la protección de la intimidad.

Como se ha visto hasta el momento, la mala aplicación de la vigilancia masiva en sus distintas manifestaciones puede representar una amenaza significativa al derecho a la intimidad, es por ello que es necesario evaluar en el siguiente apartado la constitucionalidad e implicancia de la vigilancia masiva en el tratamiento de los datos personales y cómo esta afecta al derecho a la intimidad.

3.4 La constitucionalidad de la vigilancia masiva como medida para garantizar la seguridad nacional según la teoría armonizadora

La creciente dependencia de la tecnología en nuestra vida diaria ha planteado importantes cuestiones sobre cómo equilibrar la seguridad nacional con la protección de la intimidad. Es por ello que los Estados se han visto en la ardua tarea de buscar medidas de la mano de la tecnología para atenuar los índices de criminalidad. Una de estas medidas es la recopilación y análisis de datos personales, que se utilizan como estrategia para garantizar la integridad y la soberanía de un país.

Sin embargo, esta estrategia plantea interrogantes fundamentales sobre la constitucionalidad y las implicancias éticas de la vigilancia masiva en el tratamiento de los datos personales. La primera cuestión que nos planteamos es como este fenómeno impacta directamente en el derecho fundamental a la intimidad. Para ello debemos tener en cuenta los desafíos legales y morales asociados con la vigilancia masiva, siempre teniendo en cuenta la capacidad que tiene esta medida para erosionar en la esfera privada de los de los individuos y socavar los pilares de las sociedades democráticas.

Reconocemos la complejidad y divergencia que existe en cada caso concreto, es por ello que debemos buscar soluciones equilibradas que se ajusten a la realidad y que principalmente protejan los intereses de los particulares tanto como sea posible. En ocasiones, estas situaciones pueden implicar la implementación de límites razonables en el ejercicio de los derechos para prevenir interferencias arbitrarias en el contenido esencial de otros derechos. De esta manera la teoría armonizadora emerge como un enfoque crucial para abordar estos dilemas, proponiendo que no es necesario sacrificar un derecho en beneficio de otro, sino que se debe buscar un equilibrio que permita la coexistencia de todos los intereses en juego a partir del ejercicio razonable de los derechos fundamentales, así como de la justificación, también razonable, de las medidas que los limiten. Este enfoque requiere un

análisis detallado de cada situación específica para determinar cómo se pueden implementar prácticas que respeten adecuadamente el derecho a la privacidad de los individuos y, al mismo tiempo, no comprometan la seguridad nacional.

Para ello debemos recordar lo dicho en el segundo capítulo donde se explica, que, en un Estado Constitucional de Derecho, es fundamental reconocer el papel central que desempeña el Tribunal Constitucional en la protección de los derechos fundamentales y en la interpretación de la Constitución. Esto implica la aplicación meticulosa de principios de interpretación constitucional, tales como los principios de unidad de la Constitución y concordancia práctica, los cuales son cruciales para asegurar una interpretación coherente y no contradictoria de los derechos constitucionales. En este marco la teoría armonizadora de los derechos plantea la inexistencia de los llamados conflictos de contenidos constitucionales de derechos fundamentales, o de estos con bienes jurídico constitucionales, pues en lugar de tratar de eliminar uno de los derechos en "colisión" en favor del otro, se debe buscar una solución que permita su coexistencia en la medida mayor de lo posible.

Para iniciar un análisis bajo esta teoría debemos entender a los derechos fundamentales como "derechos humanos constitucionalizados. Los derechos humanos, por su parte, pueden ser definidos como el conjunto de bienes humanos esenciales debidos a la persona por ser lo que es y valer lo que vale, y cuyo goce o adquisición le depara grados de realización"[129]. En otras palabras, los derechos humanos existen antes de ser reconocidos por el legislador, ya que son inherentes a la persona, la cual vale como fin supremo y es por ello que está ordenado promover su máxima realización posible. Una mayor vigencia de los derechos fundamentales implica una mayor realización de la persona.

Como se explicó en el apartado 2.3 de este trabajo, es la naturaleza y dignidad humana lo que permiten reconocer que a la persona se le adeudan por su sola naturaleza y valor, unos esenciales bienes humanos. Estos bienes tienen un alcance razonable que reclaman su cumplimiento efectivo y descartan su sacrificio. Los derechos fundamentales no son simples "mandatos de optimización que están caracterizados por el hecho que pueden ser cumplidos en diferente grado y que la medida debida de su cumplimiento no sólo depende de las posibilidades reales sino también de las jurídicas"[130], es decir, no son realidades que tienden a expandirse ilimitadamente hasta que una choca contra otra y surge la necesidad de sacrificar una de ellas.

---

129 CASTILLO CÓRDOVA, Luis. 2022. *Las fuentes constitucionales sobre derechos fundamentales*. 1a ed. p. 25.

130 ALEXY, Robert. *Teoría de los Derechos Fundamentales*. Madrid: Centro de Estudios Constitucionales, 1993. p. 86. Disponible en: https://www.pensamientopenal.com.ar/system/files/2014/12/doctrina37294.pdf

Esto reclama el ámbito material y formal de cada derecho. El ámbito material está referido a la cobertura general o teórica de un derecho, este ámbito necesita ser concretado (de manera doctrinal, legal y jurisprudencial) y esas concreciones determinan cuales acciones dentro de este ámbito son legítimas; mientras que el ámbito formal de un derecho establece su legítimo alcance y ejercicio razonable, como se regula dentro del marco normativo. Así habrá acciones que están materialmente incluidas en un derecho y que, al pasar por el tamiz de la razonabilidad y la justicia, se formalizarán y serán verdaderamente amparadas[131]. En otras palabras, el ámbito material de un derecho hace referencia a las acciones que no están protegidas o reconocidas por el derecho, pero que son posibles bajo ese derecho en un sentido amplio. En cambio, el ámbito formal se refiere a las acciones que están formalmente legitimadas y protegidas dentro de los límites del derecho, es decir, las acciones legítimas que el derecho permite.

De esta manera el ámbito material se enfoca en las libertades y capacidades concretas que un derecho protege, incluso aquellas que no están formalmente reconocidas pero que son concebibles dentro de ese derecho en un sentido amplio; haciendo referencia a como los derechos se expresan y se entienden en la vida cotidiana. Por otro lado, el ámbito formal alude a la regulación y estructura de un derecho dentro del marco legal, las normas que el Estado establece para asegurar su ejercicio y las condiciones bajo las cuales puede ser restringido de manera legítima, siempre respetando la esencia del derecho. Estos dos ámbitos son importantes para la protección efectiva de los derechos fundamentales.

Llevando esta distinción a lo que nos atañe, en el acápite 1.4 de nuestra investigación hicimos mención del tratamiento de los datos personales y la protección de estos, que se encuentra recogido en el artículo 2.6 de nuestra Constitución, al recordar el tenor de este artículo, podemos deducir a primera vista que los servicios informativos no pueden afectar nuestra intimidad personal, ni familiar; asimismo el articulo 2.7 busca salvaguardar la dignidad, la intimidad y la seguridad de las personas en el ámbito personal y familiar. Por otro lado, el artículo 163 de nuestro ordenamiento indica que “el Estado garantiza la seguridad de la Nación mediante el Sistema de Defensa Nacional”.

Siguiendo el razonamiento de Fernando Toller, en primer lugar, identificamos los derechos y el bien jurídico que están en un aparente conflicto, así tendríamos: Derecho a la

---

131 TOLLER, Fernando M., 2014. Metodologías para tomar decisiones en litigios y procesos legislativos sobre derechos fundamentales. En: RIVERA (H), Julio César; ELIAS, José Sebastián; GROSMAN, Lucas Sebastián y LEGARRE, Santiago, directores. *Tratado de los Derechos Constitucionales.* 1ª ed. Ciudad Autónoma de Buenos Aires: Abeledo Perrot. pp. 107-199. Disponible en: https://es.scribd.com/document/350080847/Toller-Fernando-M-Metodologias-Para-Tomar-Decisiones-en-Litigios-y-Procesos-Legislativos-Sobre-Derechos-Fundamentales

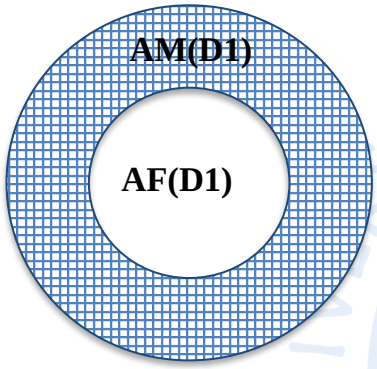
protección de datos personales y derecho a la intimidad; y seguridad nacional como bien jurídico protegido.

A. Derecho a la protección de datos personales (D1)

A su vez lo definimos como el derecho que le va a permitir al ciudadano tener una visión sobre sus datos y el tratamiento de estos, decidiendo sobre su recopilación, la razón de porque se recopilaron y la manera en la que se están transmitiendo y de esto puede resultar la siguiente premisa de protección de datos personales (P1): **Proteger los datos personales para que el ciudadano pueda ejercer control sobre su información.**

Tabla 2

Protección de datos personales (D1)



Ámbito Material (AM): los aspectos tangibles y concretos de la vida privada y personal que están protegidos por el derecho a la autodeterminación informativa.

Ámbito Formal (AF): Hará referencia a las normas, procedimientos legales y mecanismos institucionales que garantizan y protegen el derecho a la autodeterminación informativa. Este ámbito incluye las leyes, regulaciones y entidades encargadas de supervisar y hacer cumplir este derecho.

Ejemplos de ámbito material:

1. Protección de información sensible como el estado de salud, datos biométricos, orientación sexual y antecedentes penales.
2. Protección de la información financiera personal, como cuentas bancarias, historial de crédito y transacciones financieras.
3. Protección de la información sobre las actividades en línea de una persona, como historiales de búsqueda, visitas a sitios web y datos de redes sociales.
4. Protección de datos como números de teléfono, direcciones de correo electrónico y domicilios.

Ejemplos de ámbito formal:

1. Ley de Protección de Datos Personales (Ley N° 29733).
2. Reglamento de la Ley de Protección de Datos Personales: El Decreto Supremo N° 003-2013-JUS, que desarrolla las disposiciones de la Ley N° 29733, especificando cómo deben aplicarse y cumplirse las normativas de protección de datos.

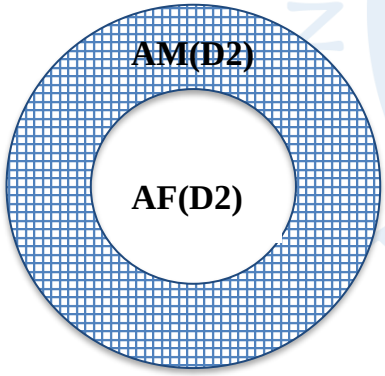
3. Autoridad Nacional de Protección de Datos Personales: Esta entidad supervisa el cumplimiento de la Ley de Protección de Datos Personales y sus reglamentos, y tiene la autoridad para imponer sanciones en caso de infracción.
4. Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO): Mecanismos legales que permiten a los individuos acceder a sus datos personales, solicitar la corrección de datos inexactos, solicitar la eliminación de datos innecesarios y oponerse al tratamiento de sus datos en ciertas circunstancias.
5. Garantía constitucional: Habeas data, recogida en el artículo 200 inciso 3[132], de la Constitución.

B. Derecho a la intimidad (D2)

Si le damos una definición es aquel derecho que protege la esfera privada de las personas contra injerencias arbitrarias y de esto puede resultar la siguiente premisa de protección de la esfera de intimidad (P2): **Garantizar que los Estados no invadan de manera irrazonable la intimidad de los individuos.**

Tabla 3

Derecho a la intimidad (D2)



Ámbito Material (AM): Se refiere a los aspectos sustantivos y concretos de la vida privada de una persona. Este ámbito abarca las acciones y conductas que ocurren en la esfera personal y que no deben ser objeto de intervención o vigilancia sin justificación adecuada.

Ámbito Formal (AF): Se refiere a las garantías procesales y normativas que aseguran la protección del ámbito material de la intimidad. Este ámbito incluye las leyes, reglamentos y procedimientos que establecen cómo debe protegerse la intimidad y cuáles son los límites para su protección.

Ejemplos de ámbito material

1. La protección del contenido de cartas, correos electrónicos y comunicaciones privadas contra la apertura o vigilancia sin consentimiento.
2. El derecho a la intimidad en el hogar, que incluye la protección contra registros domiciliarios sin una orden judicial adecuada.

---

[132] Artículo 200.3: *"La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución"*.

3. La protección de datos personales, como la información médica, financiera o cualquier otro dato sensible que no debe ser divulgada sin el consentimiento del individuo.

Ejemplos ámbito formal:

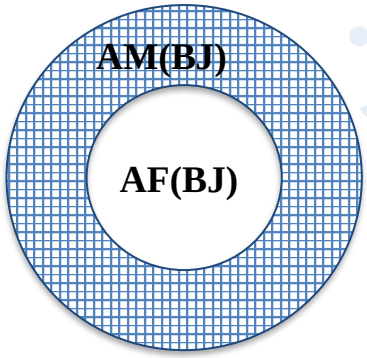
1. Regulación de la Intervención Telefónica: Leyes que establecen bajo qué circunstancias y mediante qué procedimientos una autoridad puede intervenir una llamada telefónica (por ejemplo, la Ley N°27697, que otorga facultad al Fiscal para la Intervención y Control de Comunicaciones y Documentos Privados en caso excepcional, modificada por la Ley N°30096).
2. Procedimientos Judiciales: Garantías constitucionales (por ejemplo, acción de amparo; recogida en el artículo 200 inciso 2[133] de la Constitución) en los juicios que protegen la intimidad del acusado, así como la posibilidad de declarar ciertos procedimientos como confidenciales o la protección de testigos.

C. Seguridad nacional como bien jurídico protegido

Por otro lado, tenemos la seguridad nacional, abordada en nuestro primer capítulo, reconocida como un bien jurídico por el Tribunal Constitucional en el expediente 005-2001-AI/TC. En ese sentido en la tabla 4 quedaría de la siguiente manera:

Tabla 4

Bien jurídico protegido (BJ)



Ámbito Material: Implica la protección de la soberanía, la integridad territorial y la estabilidad del Estado Peruano, frente a amenazas internas y externas.

Ámbito Formal: Hará referencia al marco teórico, leyes que regulan las políticas y estrategias de defensa y seguridad nacional.

Si le damos una definición, la seguridad nacional será un conjunto de medidas, políticas y acciones que los Estados adoptan para proteger y preservar su integridad, soberanía, independencia y estabilidad frente a amenazas internas y externas, además implicara la protección de sus ciudadanos, territorio, infraestructuras críticas y valores

[133] Artículo 200.2: *"La Acción de Amparo, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los demás derechos reconocidos por la Constitución, con excepción de los señalados en el inciso siguiente. No procede contra normas legales ni contra Resoluciones Judiciales emanadas de procedimiento regular".*

fundamentales, de esa manera podemos tener como resultado la siguiente premisa (P3): **Es obligación del Estado brindar mecanismos para asegurar la seguridad nacional de su territorio**

Ejemplos ámbito material:

1. Un ambiente seguro para los ciudadanos, libre de amenazas que incluirá políticas de defensa inteligencia, ciberseguridad y respuesta a emergencias y desastres naturales.
2. Medidas que garanticen la seguridad, respetando al mismo tiempo los derechos humanos y las libertades fundamentales.

Ejemplos ámbito formal:

1. Constitución Política del Perú: Los artículos 163, 165 y 166 establecen las bases para la seguridad nacional, incluyendo la organización y funciones de las fuerzas armadas y la policía nacional.
2. La Ley del Sistema de Defensa Nacional (Ley N° 28478) regula las políticas y estrategias de defensa y seguridad nacional.

A partir del análisis desarrollado líneas arriba tendríamos el siguiente esquema:

- P1: Proteger los datos personales para que el ciudadano pueda ejercer control sobre su información personal.
- P2: Garantizar que los Estados no invadan de manera irrazonable la intimidad de los individuos.
- P3: Es obligación del Estado brindar mecanismos para asegurar la seguridad nacional de su territorio.

Teniendo finalmente como pretensión:

"**La vigilancia masiva como mecanismo que utilizan los Estados para la seguridad nacional**".

Aplicaremos la teoría armonizadora a estas premisas para dilucidar cual sería el resultado de este análisis, en relación con la pretensión de hacer uso de la vigilancia masiva como mecanismo para la seguridad nacional.

A. Proteger los datos personales para que el ciudadano pueda ejercer control sobre su información personal (P1)

El razonamiento que resultaría es el siguiente: si se implementa la vigilancia masiva, serán los ciudadanos quienes deben tener el control sobre quién accede a su información y cómo se utiliza. Ello se logrará dando leyes y previendo políticas que aseguren la protección de los datos personales.

B. Garantizar que el Estado no invada de manera irrazonable la intimidad de los individuos (P2)

En caso de que se implemente la vigilancia masiva esta debe ser razonable y no excesiva, y bajo ciertos presupuestos, eso se lograra implementando mecanismos de supervisión para asegurar que las prácticas de vigilancia se encuentren debidamente justificadas en razones de interés público.

C. Es obligación del Estado brindar políticas para asegurar la seguridad nacional de su territorio. (P3)

La seguridad nacional es crucial y puede justificar medidas de vigilancia masiva, pero estas medidas deben ser bajo ciertos supuestos y equilibradas con el respeto a los derechos individuales, lo que se conseguirá a través de una justificación especialmente cualificada en razones de interés general.

De este análisis es posible formular la siguiente conclusión: el Estado, puede recurrir a mecanismos que promuevan la seguridad, como lo es la vigilancia masiva, siempre y cuando existan garantías para el respeto de los derechos individuales, en particular el derecho a la intimidad de las personas, lo cual se consigue a través de una justificación que se construya de modo cualificado desde razones de interés público. Es importante señalar en este punto la relación entre el derecho a la intimidad y el derecho a la protección de datos personales, ya que esta radica en que el respeto a la autodeterminación informativa contribuye a preservar la intimidad de las personas, así cuando los individuos tienen control sobre su información personal, se fortalece su capacidad para mantener su esfera privada y proteger su intimidad. Asimismo, la vulneración del derecho a la autodeterminación informativa puede tener implicaciones directas en la vulneración del derecho a la intimidad, ya que la divulgación no autorizada de datos personales puede afectar aspectos íntimos de la vida de una persona.

En situaciones donde la recopilación y uso de datos personales pueden afectar la intimidad de una persona, como lo es en casos de vigilancia masiva o recopilación de datos sin consentimiento, la autodeterminación informativa actúa como un mecanismo de defensa, permitiendo a los individuos proteger su derecho a la intimidad al controlar su información. En conclusión, el derecho a la intimidad y a la autodeterminación informativa son complementarios. Ambos buscan proteger la esfera privada de las personas, asegurando que estas tengan el control sobre su vida privada y su información personal. Jurídicamente, se reconocen como derechos fundamentales y están protegidos por una serie de garantías y normas que buscan prevenir abusos y asegurar el respeto a la dignidad humana

Si se graficase se obtendría la figura 1:

Figura 1

Gráfico de protección de datos, intimidad y seguridad

El triángulo representa el equilibrio entre ambos derechos fundamentales y el bien jurídico constitucional, permitiendo así una coexistencia razonable con la pretensión de los gobiernos por implementar medidas como lo es la vigilancia masiva. Se destaca la importancia de encontrar un punto medio que permita respetar y proteger cada uno de ellos sin comprometer los otros. Para lograr dicho equilibrio, el Estado debe reconocer que las acciones que ha venido realizando (programa Pisco, interceptaciones, espionaje, entre otras) son manifestaciones de la vigilancia masiva y que si aspiramos a este mecanismo se debe realizar la Integración de Salvaguardias Legales, que implicaría incorporar supuestos, medidas y mecanismos legales para proteger los derechos, libertades y garantías de las personas. Estas salvaguardias legales pueden incluir la adopción de leyes, regulaciones y políticas cuyo tenor sea claro, preciso en cuanto a los límites sobre la recolección, almacenamiento, acceso y uso de información personal o sensible, así como procedimientos para garantizar la transparencia, la rendición de cuentas y el respeto a los derechos humanos, de esta manera se acreditará que los datos recolectados son únicamente para los fines específicos de seguridad nacional.

Alguno de estos supuestos que proponemos son:

Amenazas graves a la Seguridad Nacional.– La vigilancia masiva puede ser utilizada en casos como terrorismo, donde los gobiernos podrán detectar, identificar patrones sospechosos y prevenir ataques que causarían un daño significativo.

Prevenir delitos graves.– La vigilancia masiva puede ayudar a prevenir delitos como el tráfico de drogas, extorsiones o secuestros, ya que al monitorizar grandes volúmenes de datos y comunicaciones la autoridad puede identificar y desarticular redes criminales.

Control efectivo en las fronteras.– La vigilancia masiva puede ayudar a gestionar el control del tránsito en las fronteras, ya que en base a un sistema interconectado con otras instituciones que manejen base de datos podría verificar la identidad de los viajeros de manera más eficiente y precisa, ya que se permitiría el cruce de datos en tiempo real, identificando posibles alertas.

Crisis sanitarias.– Este mecanismo puede aportar una correcta gestión durante crisis sanitarias, pues permitiría identificar focos de infección y patrones de propagación, se podrá tener visión clara de las áreas más afectadas permitiendo así que las autoridades puedan asignar recursos de manera más eficiente, como equipos médicos y suministros. Asimismo. el uso de tecnologías de seguimiento puede verificar si los individuos están respetando las restricciones impuestas.

En conclusión, la vigilancia masiva no es, per se, una violación a la intimidad de las personas. Si entendemos la vigilancia como la atención o cuidado hacia una determinada cosa o algo en particular, y a masiva como lo dirigido a un gran grupo de personas, la mera existencia de órganos de vigilancia no implica necesariamente una vigilancia masiva invasiva. Sin embargo, el mal uso de este mecanismo puede resultar en un menoscabo de nuestra intimidad, especialmente si los gobiernos lo emplean con fines políticos o particulares. En estos casos, estaremos ante un uso excesivo y arbitrario. Por ello, la implementación o supervisión de la vigilancia masiva debe estar justificada por el interés general, acompañada de rendición de cuentas y respeto a los derechos humanos. Solo así se garantizará que los datos recolectados se utilicen exclusivamente para el bien común.

Conclusiones

Primera. La vigilancia masiva tiene un impacto profundo en el derecho a la intimidad y la autodeterminación informativa. La recopilación indiscriminada de datos personales sin una causa legítima o justificada socava la confianza de los individuos en las instituciones y limita su capacidad de control sobre su propia información. Es así que cuando los datos personales son recogidos y analizados sin el consentimiento explícito o informado de los individuos, se ve comprometida su libertad para decidir qué información compartir y con quién. Este invasivo monitoreo puede llevar a una erosión significativa de la intimidad, creando un ambiente en el que las personas se sienten constantemente observadas y vulnerables. Por tanto, es crucial implementar mecanismos que aseguren su protección y garanticen que la intimidad de los individuos sea respetada y protegida, para mantener la libertad y la dignidad en un entorno de creciente vigilancia.

Segunda. Es inconstitucional hacer uso de la vigilancia masiva sin fundamentarse en indicios razonables y estar estrictamente limitadas a lo necesario para alcanzar objetivos legítimos. Es esencial que la implementación de medidas de vigilancia se base en evidencia concreta que justifique su necesidad y posterior aplicación. Esta base razonable asegura que la vigilancia no se convierta en un instrumento de intrusión indiscriminada, sino que se utilice únicamente cuando esté claramente justificada por una amenaza. Además, es crucial que las prácticas de vigilancia estén cuidadosamente delimitadas para evitar que se extiendan más allá de lo requerido para cumplir con su propósito legítimo. Esto implica establecer limitaciones razonables y claras sobre el alcance y la duración de la vigilancia, así como mecanismos de supervisión y rendición de cuentas para garantizar que se mantenga dentro de los límites autorizados.

Tercera. El Estado debe prever un nivel de protección excepcional a los datos personales, pues son estos los que tienen la capacidad de afectar profundamente la intimidad de las personas (salud, orientación sexual, creencias religiosas, entre otros) pues en caso de que se divulguen o se manejen de manera inapropiada, podrían tener implicaciones significativas. Es por ello que las leyes y las regulaciones deben ser explícitas y rigurosas en cuanto a su manejo y protección. Las normativas deben definir claramente qué constituye información sensible, establecer los principios para su recolección, almacenamiento y uso, y asegurar que se implementen medidas de seguridad adecuadas para prevenir accesos no autorizados y filtraciones.

Cuarta. Otro punto importante es la transparencia en la implementación de la vigilancia masiva para con ello garantizar la confianza pública y la protección de los derechos

individuales. Los ciudadanos deben estar claramente informados sobre los siguientes aspectos: Qué datos se recopilan, es así que las personas deben saber qué tipo de información personal está siendo recolectada. Esto incluye especificar las categorías de datos y los métodos utilizados para su recolección. Cómo se utilizan estos datos, es decir cómo se procesan. Se debe detallar los propósitos específicos para los cuales se emplean estos datos, así como las posibles implicaciones de su uso. Por último, que existan mecanismos de supervisión y control. Esto evitara abusos y garantizara una vigilancia responsable siendo legal y ética.

Quinta. Para abordar problemas relacionados con los derechos fundamentales, el operador jurídico puede adoptar una metodología conflictivista, que considera los derechos como principios que tienden a expandirse ilimitadamente y que por ello chocan y entran en conflicto, conflictos que se solucionan con el sacrificio de uno de los derechos y la prevalencia del otro. Este enfoque puede llevar a aceptar situaciones que vulneran el contenido constitucional de los derechos y afecta el principio de normatividad de la Constitución. En contraste, la metodología armonizadora asume un conflicto que se queda en las pretensiones y mantiene la visión de los derechos como bienes humanos debidos a la persona por ser lo que es y valer lo que vale con un alcance razonable, por lo que no aceptan contenidos sacrificables. Al usar esta metodología, se aplican mecanismos interpretativos (literal, teleológico, concordancia práctica, cláusula interpretativa, razonabilidad) dirigidos a responder a la pregunta ¿a qué da derecho el derecho fundamental invocado en las circunstancias de un caso concreto? Si alguna pretensión excediese el ejercicio razonable permitido, no formará parte del contenido constitucionalmente protegido del derecho fundamental. Ambas metodologías tienen fundamentos doctrinales diferentes y el operador jurídico debe elegir una u otra, evitando mezclar estos enfoques.

Sexta. La teoría armonizadora es esencial para lograr un equilibrio justo entre la seguridad nacional y los derechos individuales. En lugar de ver estos aspectos como irreconciliablemente opuestos, esta teoría propone que es posible alcanzar una coexistencia razonable sin tener que sacrificar un derecho en detrimento de otro. Cabe recalcar que los verdaderos conflictos no son entre derechos sino entre las pretensiones y el alcance de un derecho fundamental no es ilimitado, sino que debe ser razonable en relación con el bien humano que sustenta el derecho. Para respetar un derecho fundamental es esencial mantener su contenido constitucional y garantizar que se cumpla, respetando a la persona como el fin supremo de la sociedad y del Estado. Este enfoque busca integrar las necesidades de seguridad con la protección de los derechos fundamentales de manera que ambos puedan

coexistir de forma armoniosa. Al aplicar la teoría armonizadora, se pretende diseñar políticas y marcos legales que permitan garantizar la seguridad pública sin comprometer las libertades individuales. Esto implica encontrar soluciones que respeten los derechos humanos mientras se abordan eficazmente las amenazas a la seguridad. La clave está en implementar medidas que sean adecuadamente reguladas, de modo que se salvaguarden los valores que están comprometidos.

Sétima. La adopción de instrumentos normativos internacionales, como el Convenio 108 del Consejo de Europa y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, es crucial para armonizar las normativas de protección de datos y garantizar un nivel adecuado de protección a nivel global. Estos instrumentos internacionales establecen estándares elevados para la gestión y protección de datos personales, proporcionando un marco sólido que promueve la transparencia, la responsabilidad y la seguridad en el tratamiento de la información. Su implementación no solo facilita la cooperación internacional y el intercambio seguro de datos, sino que también asegura que las leyes nacionales estén alineadas con las mejores prácticas globales en materia de privacidad. Esto es especialmente importante en un contexto de creciente globalización y digitalización, donde la protección de datos transnacionales es fundamental para salvaguardar los derechos de los ciudadanos en un entorno interconectado. De esta manera el Perú puede mejorar sus sistemas de protección de datos, fortalecer la confianza pública y asegurar un estándar global de privacidad que beneficie a los individuos.

Octava. En la era digital, el derecho a la intimidad se ha expandido para abarcar el control sobre la información personal en línea, un aspecto crucial en un entorno donde los datos digitales son constantemente recopilados, compartidos y utilizados. Las regulaciones deben evolucionar de manera continua para enfrentar los desafíos emergentes de las tecnologías digitales y asegurar la protección efectiva de todos los derechos fundamentales, en particular el derecho a la intimidad. Esto incluye la actualización de leyes para abordar nuevas formas de vigilancia, el uso de algoritmos y la recolección de datos a gran escala, así como la implementación de medidas que garanticen la privacidad en plataformas digitales y redes sociales. De esta manera se podrá proteger adecuadamente la intimidad en un mundo digital en constante cambio y garantizar que este derecho fundamental se respete y se preserve frente a las innovaciones tecnológicas.

Novena. Es crucial que tanto el Estado como las empresas colaboren estrechamente para salvaguardar la protección de los datos personales. El Estado debe garantizar que no se exija a las empresas la entrega de datos sin una justificación adecuada. Esto implica establecer

normas claras que definan las condiciones bajo las cuales la información puede ser solicitada y procesada, asegurando que tales demandas estén siempre respaldadas por razones legítimas y específicas. La colaboración efectiva entre el Estado y las empresas también debe incluir la implementación de prácticas transparentes y mecanismos de control que prevengan el uso indebido de datos. A través de esta cooperación equilibrada, se puede proteger la privacidad de los ciudadanos y mantener la integridad de la gestión de datos personales, respetando tanto la necesidad de seguridad como los derechos individuales.

Décima. En el contexto peruano, lograr un equilibrio adecuado entre la seguridad nacional y el derecho a la intimidad constituye un desafío complejo y multifacético. La seguridad nacional es crucial para resguardar al país de amenazas tanto internas como externas, garantizando la estabilidad, el orden público y el bienestar general de la sociedad. Sin embargo, es igualmente indispensable proteger el derecho a la intimidad, que representa un pilar fundamental de la dignidad y libertad individual. Este derecho asegura que los ciudadanos puedan disfrutar de su vida personal sin temor a invasiones injustificadas o intrusiones en su privacidad. La clave para lograr una coexistencia armónica entre seguridad y privacidad reside en un compromiso continuo con la protección de los derechos individuales, al tiempo que se asegura la estabilidad y la seguridad del país. De esta manera es fundamental adoptar un enfoque equilibrado y responsable que permita resguardar los derechos fundamentales de los ciudadanos sin comprometer la capacidad del Estado para cumplir con sus deberes de seguridad. Solo mediante la implementación de políticas que integren ambos aspectos de manera equitativa y transparente se podrá garantizar un entorno donde la protección de la privacidad no se vea sacrificada en favor de la seguridad, y viceversa. Esta armonía es esencial para preservar la confianza pública y la integridad de nuestras instituciones, asegurando que la protección de los derechos y la seguridad nacional se refuercen mutuamente en beneficio de una sociedad justa y segura.

Referencias

ALEXY, Robert. 1993. *Teoría de los Derechos Fundamentales.* Madrid: Centro de Estudios Constitucionales. https://www.pensamientopenal.com.ar/system/files/2014/12/doctrina37294.pdf.

ÁLVAREZ MEDINA, Silvina. 2020. «La interferencia estatal en la vida privada y familiar.» *Cuadernos Electrónicos de Filosofía del Derecho* (Universitat de Valencia) (42). doi:10.7203/CEFD.42.16609.

AMÉRICA NOTICIAS. 2015. «DINI compró millonario equipo de "chuponeo" a pedido del presidente Humala.» *Youtube.* 9 de agosto. https://www.youtube.com/watch?v=PxP59hHEDjE&t=27s.

AMINISTÍA INTERNACIONAL. 2022. *Proyecto Pegasus: Un año después, la crisis de los programas espía continúa, mientras el sector de la vigilancia sigue sin estar sometido a control.* https://www.amnesty.org/es/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/.

AMNISTÍA INTERNACIONAL. 2019. «El gran hackeo: Cambridge Analytica es sólo la punta del iceberg.» *Amnistía Internacional.* 24 de julio. https://www.amnesty.org/es/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/.

ARIAS ARÓSTEGUI, Enrique Alfredo. 2017. «Un caso de transferencia de política: entre el éxito y el fracaso, la reforma de inteligencia durante el gobierno de Alejandro Toledo.» Tesis de licenciatura en Ciencia Política, Facultad de Ciencias Sociales, Pontificia Universidad Católica del Perú, Lima, 123. http://hdl.handle.net/20.500.12404/8972.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (APDP). 2013. *Directiva de seguridad.* Ministerio de Justicia y Derechos Humanos, Lima: Editora Diskcopy S.A.C. https://cdn.www.gob.pe/uploads/document/file/1401560/Directiva%20de%20seguridad.pdf.

AYMA, Diego. 2015. «El trabajo de la revista Correo Semanal y del diario Correo: La DINI al desnudo.» *Diario Correo.* https://diariocorreo.pe/politica/la-dini-al-desnudo-576539/.

BERTONI, Eduardo, Edison LANZA, y Mariana y TORRES, Natalia MAS. 2012. «Seguridad Nacional y Acceso a la Información en América Latina: Estado de

situación y desafíos.» Documento, Centro de Archivos y Acceso a la Información Pública (CAinfo) con la asistencia técnica del Centro de Estudios para la Libertad de Expresión y Acceso a la información (CELE), Facultad de Derecho. Universidad de Palermo, Argentina. https://www.palermo.edu/cele/noticias/acceso-informacion-seguridad-nacional.html.

BONIFAZ, Rafael. 2017. «Vigilancia masiva y privacidad en Internet. La NSA según las Revelaciones de Snowden.» Trabajo final de posgrado, Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería, Universidad de Buenos Aires, Buenos Aires. http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-0938_BonifazR.

BRU CUADRADA, Elisenda. 2007. «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad.» *IDP. Revista de Internet, Derecho y Política* (Universitat Oberta de Catalunya) (5): 78-92. https://www.redalyc.org/articulo.oa?id=78812861008.

CARLSON, Kimberly. 2016. «La triste historia del Perú con la vigilancia, y cómo solucionarla.» *Effecting Change.* 24 de Octubre. https://www.eff.org/es/deeplinks/2016/10/la-triste-historia-del-peru-con-la-vigilancia-y-como-solucionarla.

CARMONA BRENIS, Marco y VIGIL ZÁRATE, Martha. 2015. «El derecho a la intimidad en las relaciones familiares.» *Lumen: Revista de la facultad de Derecho de la Universidad Femenina del Sagrado Corazón* (11): 77-84. doi:https://doi.org/10.33539/lumen.2015.n11.546.

CASTILLA, ÓSCAR. 2011. «Así funciona Constelación, el sistema de escucha telefónica de la Dirandro.» *El Comercio.* https://elcomercio.pe/sociedad/lima/asi-funciona-constelacion-sistema-escucha-telefonica-dirandro-noticia-1341509/.

CASTILLO CORDOVA, L. 2014. «El significado del contenido esencial de los derechos fundamentales.» *Revista PUCP. Foro jurídico* (13): pp. 143-154. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/13783.

CASTILLO CÓRDOVA, Luis. 2005. «¿Existen los llamados conflictos entre derechos fundamentales? Cuestiones Constitucionales.» *Revista Mexicana de Derecho Constitucional* (12): pp. 99-129.

—. 2012. «La finalidad del derecho de autodeterminación informativa y su afianzamiento a través del hábeas.» *Transparencia, información pública, datos personales.* 31 de julio. https://sumaciudadana.wordpress.com/2012/07/31/la-finalidad-del-derecho-de-autodeterminacion-informativa-y-su-afianzamiento-a-traves-del-habeas-data/.

CASTILLO CÓRDOVA, Luis. 2022. «Las fuentes constitucionales sobre derechos fundamentales.» *Centro de Investigaciones Judiciales* (Fondo Editorial del Poder Judicial del Perú. Primera ed.) (2): pp. 97. ISBN: 978-612-4484-36-0. https://www.pj.gob.pe/wps/wcm/connect/695a7f804799c825ab5dbb2a87435a1f/web_Las+fuentes+constitucionales+-+Luis+Castillo.pdf?MOD=AJPERES&CACHEID=695a7f804799c825ab5dbb2a87435a1f.

COMUNICACIÓN PODER JUDICIAL. 2024. *La Audiencia Nacional reabre la causa Pegasus ante nuevos datos aportados por Francia.* 23 de abril. https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-reabre-la-causa-Pegasus-ante-nuevos-datos-aportados-por-Francia.

CONGRESO CONSTITUYENTE DEMOCRÁTICO. 1998. *Debate Constitucional Pleno 1993.* Vol. I. Lima: Congreso de la República. https://spij.minjus.gob.pe/Textos-PDF/Constitucion_1993/DebConst-Pleno93/DebConst-Pleno93TOMO1.pdf.

CONSEJO DE EUROPA. OFICINA DE TRATADOS. 1981. «Convenio para la Protección de las Personas con respecto al Procesamiento Automatizado de Datos Personales (ETS No. 108).» Detalles del Tratado N° 108, Estrasburgo. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

CONSEJO DE EUROPA. OFICINA DE TRATADOS. 2021. «Protocolo Adicional al Convenio para la Protección de las Personas en lo que respecta al Tratamiento Automatizado de Datos Personales, en relación con las autoridades de control y los flujos transfronterizos de datos (STE n.º 181).» Detalles del Tratado N° 181, Estrasburgo. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181.

DEFENSORÍA DEL PUEBLO. 2019. *Pronunciamiento N° 014/DP/2019. Sobre el derecho a la intimidad personal y familiar.* https://www.defensoria.gob.pe/wp-content/uploads/2019/04/DEFENSOR%C3%8DA-DEL-PUEBLO-SE-PRONUNCIA-SOBRE-EL-DERECHO-A-LA-INTIMIDAD-PERSONAL-Y-FAMILIAR-4.pdf.

DEPARTAMENTO DE DERECHO INTERNACIONAL. 2022. «Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.» Secretaría de Asuntos Jurídicos, Organización de Estados Americanos (OEA), Washington.

DEPARTAMENTO DE INVESTIGACIÓN Y DOCUMENTACIÓN PARLAMENTARIA. 2015. *Mociones de Censura. Periodo Parlamentario 2011-2016 (del 27 de julio del 2011 al 26 de julio del 2016).* Congreso de la República. 20 de marzo. https://www2.congreso.gob.pe/Sicr/TraDocEstProc/InfSiste_2013.nsf/C8CE491805E736C405257AF700743CC6/15C87144714CAA8505257C0D005BA5C5?OpenDocument.

DIRECCIÓN ANTIDROGAS. 2022. «Trabajando por el Perú y el Mundo.» Vol. I. nº 1. Lima. https://dirandro.policia.gob.pe/publicaciones/revista1.pdf.

DUEÑAS CHAVEZ, Gian Marco y SEÑA MANGUINURY, Jonathan Enrique. 2023. «Fortalecimiento de la capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet.» Trabajo de Tesis de maestría, Gobierno y Políticas Públicas, Pontificia Universidad Católica del Perú, Lima. http://hdl.handle.net/20.500.12404/26812.

EGUIGUREN PRAELI, Francisco. 2000. «La libertad de información y su relación con los derechos a la intimidad y al honor en el caso peruano.» *Ius Et Veritas* (Pontificia Universidad Católica del Perú) (20). https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15924.

EL MUNDO. 2022. «La Policía israeli espió a sus ciudadanos a través de Pegasus.» https://www.elmundo.es/internacional/2022/01/18/61e6f71521efa0621e8b456f.html.

ENRÍQUEZ ÁLVAREZ, Luis. 2020. «La visión de América Latina sobre el Reglamento General de Protección de Datos.» *Comentario Internacional* (19): 99-112. doi:10.32719/26312549.2019.19.4.

ESCOBEDO, Catalina. 2021. «Modificaciones a la "Ley Stalker" en Perú.» *iapp.* 3 de agosto. https://iapp.org/news/a/modificaciones-a-la-ley-stalker-en-peru-2.

ESPINOSA, Pablo. 2023. «Vigilancia masiva: Conflicto entre seguridad nacional, derecho a la protección de datos personales y vida privada.» *REVISTA CÁLAMO* (13): 123-137. https://doi.org/10.61243/calamo.13.167.

FIGUEROA FRANCISCO, Javiera Montserrat. 2022. «Inteligencia artificial, big data y derecho sanitario: reflexiones a la luz de los derechos fundamentales.» Tesis fin de grado en Derecho, Facultad de Derecho, Universidad de Cantabria, Santander.

https://repositorio.unican.es/xmlui/bitstream/handle/10902/26234/FIGUEROAFRANCISCOJAVIERAMONTSERRAT.pf?sequence=1.

GARCÍA GONZÁLEZ, Aristeo. 2007. «La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.» *Scielo. Boletín mexicano de derecho comparado* 40 (120). https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003.

GARCÍA MORENTE, Manuel. 1935. *Ensayo sobre la vida privada.* Madrid.

GARCÍA TOMA, Víctor. 2018. «La dignidad humana y los derechos fundamentales.» *Derecho & sociedad* (Asociación Civil de la Universidad Pontificia Universidad Católica del Perú) (51): 13-31.

GASCÓN MACÉN, Ana. 2021. «El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea.» *Cuadernos de Derecho Transnacional* XIII (2): 209-232. doi:https://doi.org/10.20318/cdt.2021.6256.

GOBIERNO DEL PERÚ. s.f. *Dirección Nacional de Inteligencia.* https://www.gob.pe/institucion/dini/organizacion.

—. 2024. *Sistema de Inteligencia Nacional.* 14 de enero. https://www.gob.pe/27632-sistema-de-inteligencia-nacional-sina.

GONZÁLEZ PORRAS, Andrés José. 2016. «Privacidad en internet: los derechos fundamentales de privacidad e intimidad en Internet y su regulación jurídica. La vigilancia masiva.» Tesis doctoral, Departamento de Ciencia Jurídica y Derecho Público, Universidad de Castilla- La Mancha. https://hdl.handle.net/10578/10092.

GORRITI, Gustavo. 2015. *Espías.* 26 de marzo. https://www.idl-reporteros.pe/espias/.

GREENWALD, Glenn. 2014. *Sin un lugar donde esconderse: Edward Snowden, la NSA y el estado de vigilancia de EE. UU.* Barcelona: Ediciones B. https://www.proglocode.unam.mx/sites/proglocode.unam.mx/files/Greenwald,%20G.%20(2014)%20Edward%20Snowden%20(red)....pdf.

GUEVARA SANMATEO, Mar. 2018. «El impacto del Big Data en la protección de datos personales.» Tesis fin de grado, Departamento de Derecho Público, Universitat Jaume I. http://hdl.handle.net/10234/175806.

LUCENA CID, Isabel Victoria. 2012. «La protección de la intimidad en la era tecnológica: hacia una reconceptualización.» *Revista Internacional de Pensamiento Político* VII: 117-144. https://www.upo.es/revistas/index.php/ripp/article/view/3683.

MARTÍNEZ DE PISÓN CAVERO, José María. 1997. «Vida privada e intimidad. Implicaciones y perversiones.» *Anuario de Filosofía del Derecho* (13-14): 717-738. https://dialnet.unirioja.es/servlet/articulo?codigo=142345.

MARTÍNEZ DEVIA, Andrea. 2019. «La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales?» *Revista La Propiedad Inmaterial* (Universidad Externado de Colombia) (27): 5-23. https://revistas.uexternado.edu.co/index.php/propin/article/view/6071.

MAYER-SCHÖNBERGER, Viktor, y Kenneth CUKIER. 2013. *Big Data. A Revolution That Will Transform How We Live, Work, and Think.* Primera edición. Traducido por Antonio Iriarte. Madrid: Turner Publicaciones S.L. http://catedradatos.com.ar/media/3.-Big-data.-La-revolucion-de-los-datos-masivos-Noema-Spanish-Edition-Viktor-Mayer-Schonberger-Kenneth-Cukier.pdf.

MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN. 2023. «Fiscalía Anticorrupción presenta acusación y pie 10 años de prisión contra el expresidente Ollanta Humala.» *Gob. Pe.* 12 de otubre. https://www.gob.pe/institucion/mpfn/noticias/848836-fiscalia-anticorrupcion-presenta-acusacion-y-pide-10-anos-de-prision-contra-el-expediente-ollanta-humala.

MISHIMA, Miya. 2023. «Multas por infracciones en materia de protección de datos personales pueden ascender hasta S/ 495,000.00.» *EY Building a better working world.* 1 de febrero. https://www.ey.com/es_pe/news/2023/02/multas-infracciones-proteccion-datos-personales.

MNIISTERIO DEL INTERIOR. 2011. *Dirandro no realiza Interceptaciones Ilegales.* 03 de junio. https://www.mininter.gob.pe/content/dirandro-no-realiza-interceptaciones-ilegales.

MORACHIMO, Miguel. 2016. *El sistema de espionaje de las comunicaciones que dejó Humala.* 07 de agosto. https://hiperderecho.org/2016/08/proyecto-pisco-skylock-peru-verint/# .

MUÑOZ PETERSEN, Bárbara Alejandra. 2005. «La corrupción como amenaza a la seguridad nacional tras la transición democrática en México.» Tesis de licenciatura en Relaciones Internacionales, Departamento de Relaciones Internacionales e Historia. Escuela de Ciencias Sociales, Universidad de las Américas Puebla, Puebla. http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/.

MUÑOZ V., Heraldo. 2023. *Democracias en peligro. Regresión democrática en Latinoamérica y propuestas de futuro.* Primera edición. Santiago de Chile: Editorial

Catalonia. https://books.google.com.pe/books?id=zb31EAAAQBAJ&pg=PT87&hl=es&source=gbs_toc_r&cad=1#v=onepage&q&f=false.

NIEVES SALDAÑA, María. 2012. «The right to privacy»: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis.» *WARREN, S. D. Y BRANDEIS, L. D. (1995). El derecho a la intimidad, págs. 26 y 27. Para la edición original, vid. «The Right to Privacy», op. cit., pág. 196.* nº 85. 195-239. doi:https://doi.org/10.5944/rdp.85.2012.10723.

Olmstead V. The United States. 1928. US 438 (Corte Suprema de Estados Unidos, fj. 478-479).

ORTEGA Y GASSET, José. 1980. «El hombre y la gente.» *Revista de Occidente en Alianza Editorial* (Alianza Editorial). http://manuelosses.cl/VU/El%20Hombre%20y%20la%20gente.%20O.Gasset.pdf.

PALOMO GARRIDO, Aleksandro. 2016. «La lucha antiterrorista y el nuevo sistema de seguridad internacional tras el 11 de septiembre: ¿una consecuencia lógica?» *Foro Internacional* (El Colegio de México) vol. LVI (4 (226)). https://doi.org/10.24201/fi.v56i4.2379.

PANAMERICANA. 2011. *Congresista Daniel Abugattás denunció interceptación telefónica desde sede policial.* Redacción Panamericana. 03 de junio. https://panamericana.pe/24horas/elecciones2011/86301.

PAVÓN PÉREZ, Juan Antonio. 2001. «La protección de datos personales en el consejo de Europa.» *Anuario de la Facultad de Derecho* (Universidad de Extremadura) (19): 235-252. https://dialnet.unirioja.es/servlet/articulo?codigo=831270 .

PÉREZ LUÑO, ANTONIO ENRIQUE. 1998. «Impactos sociales y jurídicos de Internet. Argumentos de razón técnica.» *Revista Española de Ciencia, Tecnología y Sociedad, y Filosofía de la Tecnología* (1): 33-48. http://hdl.handle.net/11441/57678.

RALLO LOMBARTE, A. 2014. *El derecho al olvido en Internet: Google versus España.* Primera edición. Madrid: Centro de Estudios Políticos y Constitucionales.

REAL ACADEMIA ESPAÑOLA. 1992. *Diccionario de la Lengua Española.* Madrid: Editorial Espasa Calpe.

REIGOSA, Carlos G. 2019. «La verdad en Internet.» *La Voz de Galicia.* 14 de octubre. https://www.lavozdegalicia.es/noticia/opinion/2019/10/14/verdad-internet/0003_201910G14P14992.htm.

RIBAS, J. 1996. «Aspectos legislativos de las autopistas de la información: Delitos en Internet.» *Jornadas Profesionales Informat-96.*

RODRIGUEZ, Katitza. 2015. «Ley Stalker, o cómo el gobierno legalizó la vigilancia masiva a peruanos inocentes.» *Electronic Frontier Foundation.* 2 de Agosto. https://www.eff.org/es/deeplinks/2015/08/stalker-law-como-gobierno-peru-legalizo-vigilancia-ciudadanos.

SECRETARÍA DE SEGURIDAD Y DEFENSA NACIONAL (SEDENA). 2015. *Doctrina de seguridad y defensa nacional.* https://www.esup.edu.pe/wp-content/uploads/2021/01/8.%20Doctrina%20de%20Seguridad%20y%20Defensa%20Nacional%202015.pdf.

SUÁREZ GONZALO, SARA. 2019. «Big data, poder y libertad. Sobre el impacto social y político de la vigilancia masiva.» Tesis doctoral, Departamento de Comunicación, Universidad Pompeu Fabra. http://hdl.handle.net/10803/668235.

TENE, Omar. 2015. «Reforming data protection in Europe and beyond: a critical assessment of the second wave of global privacy laws.» *En: RALLO LOMBARTE A. y GARCÍA MAHAMUT, R. coord. Hacia un nuevo derecho europeo de protección de datos.* Vaencia: Tirant lo Blanch.

THE CITIZEN LAB. 2022. «¿Harías clic? Munk school.» *University Toronto.* https://catalonia.citizenlab.ca/es/.

TOLLER, Fernando M. 2014. «Metodologías para tomar decisiones en litigios y procesos legislativos sobre derechos fundamentales.» En *Tratado de los Derechos Constitucionales*, de Julio César Rivera (H), José Sebastián Elias y Lucas Sebastián y Legarre, Santiago Grosman. Buenos Aires: Abeledo Perrot. https://es.scribd.com/document/350080847/Toller-Fernando-M-Metodologias-Para-Tomar-Decisiones-en-Litigios-y-Procesos-Legislativos-Sobre-Derechos-Fundamentales.

TRAMONTANA CUBAS, Dora. 2004. «La violencia terrorista en el Perú, Sendero Luminoso, y la protección internacional de los derechos humanos.» *Revista Persona* (25). https://www.revistapersona.com.ar/Persona25/25Tramontana1.htm.

UNITED STATES SENATE. 1976. «Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities.» *Internet Archive.* https://archive.org/details/finalreportofsel01unit.

UNITED STATES TRADE REPRESENTATIVE. 2021. *National Trade Estimate Report on Foreign Trade Barriers.* https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

VASOLI, Maria Josefina. 2002. «Seguridad Nacional o Defensa Nacional: La implicancia de la tecnología en el planeamiento del Sistema de Defensa Nacional.» *Red de Seguridad de Defensa de América Latina - RESDAL*. 1 de octubre. Último acceso: mayo de 2024. https://www.resdal.org/Archivo/d0000271.htm.

VERCELLI, Ariel Hernán. 2021. «El extractivismo de grandes datos (personales) y las tensiones Jurídico-Políticas y tecnológicas vinculadas al voto secreto.» *Themis. Revista de Derecho* (79). doi:https://doi.org/10.18800/themis.202101.006.

VISUALPOLITIK. 2020. *NSA: la agencia que espiaba a Merkel (y a otros muchos líderes mundiales)*. 27 de mayo. https://www.youtube.com/watch?v=cn7TwjiH4DQ.

—. 2022. «PEGASUS: El sistema espía de Israel que ha escandalizado al mundo.» *Youtube*. 9 de febrero. https://www.youtube.com/watch?v=XE7JptwDPec.

YOVERA, Daniel. 2015. «DINI adquirió sistema Pisco por orden de Ollanta Humala.» *El Comercio*. 09 de agosto. https://elcomercio.pe/politica/gobierno/dini-adquirio-sistema-pisco-orden-ollanta-humala-192136-noticia/?ref=ecr.

Jurisprudencia

Primera Sala del Tribunal Constitucional Alemán (Ley del Censo), sentencia del 15 de diciembre de 1983.

Tribunal Constitucional Español, sentencia 292/2000 del 30 de noviembre del 2000.

Tribunal Constitucional Español, sentencia STC 77/2009 del 23 de marzo del 2009.

TC. Expediente N° 005–2001–AI/TC, sentencia del 15 de noviembre del 2001.

TC. Expediente N° 0905–2001–AA/TC, sentencia del 14 de agosto del 2002.

TC. Expediente N° 4739-2007-PHD/TC, sentencia del 15 de octubre del 2007.

TC. Expediente N° 00473-2022-PHD/TC, sentencia del 08 de julio del 2022.

TC. Expediente N° 2839-2021-PHD/TC, sentencia del 22 de agosto del 2022.

TC. Expediente N° 3086-2021-PA/TC, sentencia del 13 de febrero de 2024.

TC. Expediente N° 03485-2012-PA/TC, sentencia del 10 de marzo del 2016.

TC. Expediente N° 00050-2004-AI/TC, sentencia del 03 de junio del 2005.

TC. Expediente N° 00010-2002-AI/TC, sentencia del 03 de enero del 2002.

TC. Expediente N° 5854-2005-PA/TC, sentencia del 08 de noviembre del 2005.

TC. Expediente N° 00072-2004-AA/TC, sentencia del 07 de abril del 2005.

TC. Expediente N° 06712-2005-HC/TC, sentencia del 17 de octubre del 2005.

TC. Expediente N° 01797-2002-HD/TC, sentencia del 29 de enero del 2003.

TC. Expediente N° 00011-2004-AI/TC, sentencia del 21 de setiembre del 2004.