FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de **DERECHO Y CIENCIAS POLÍTICAS**

“LA PROBLEMÁTICA DE LA REGULACION DE LOS MACRODATOS EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES”

Tesis para obtener el título profesional de:

Abogado

Autor:

Gerardo Joel Rengifo Ynfanzon

Asesor:

Dr. Guisseppi Paul Morales Cauti
https://orcid.org/0000-0002-6550-0722

Lima - Perú

2022

JURADO EVALUADOR

Jurado 1 Presidente(a)	**Dra. Patricia Malena Cepeda Gamio**	**08144095**
	Nombre y Apellidos	Nº DNI

Jurado 2	**Dr. Emilio José Balarezo Reyes**	**40343109**
	Nombre y Apellidos	Nº DNI

Jurado 3	**Dr. Michael Lincol Trujillo Pajuelo**	**44953968**
	Nombre y Apellidos	Nº DNI

RESUMEN DEL REPORTE DE SIMILITUD

Document Information

Analyzed document	Tesis Final Gerardo Rengifo.docx (D157680465)
Submitted	2023-02-02 20:30:00
Submitted by	
Submitter email	guisseppi.morales@upn.edu.pe
Similarity	13%
Analysis address	guisseppi.morales.delnor@analysis.urkund.com

Sources included in the report

SA	**TESIS FINAL - 100% CORREGIDA.docx** Document TESIS FINAL - 100% CORREGIDA.docx (D87626232)	3
SA	**Universidad Privada del Norte / 2017Gonzales Cabrera Monica Lizette.pdf** Document 2017Gonzales Cabrera Monica Lizette.pdf (D139694429) Submitted by: karen.galvez@upn.edu.pe Receiver: karen.galvez.delnor@analysis.urkund.com	2
W	URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf Fetched: 2021-12-20 04:33:43	1
W	URL: http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-rcdp.i65.2022.3834 Fetched: 2023-01-21 20:17:32	1
W	URL: https://agnitio.pe/articulo/el-big-data-y-sus-implicancias-legales-en-la-proteccion-de-datos-p... Fetched: 2021-11-13 00:27:05	4
W	URL: https://www.aepd.es/sites/default/files/2019-10/big-data.pdf Fetched: 2020-01-03 00:47:52	2
W	URL: https://repositorio.umsa.bo/bitstream/handle/123456789/10689/T.3225.pdf?sequence=1&isAllowed=y Fetched: 2020-07-24 09:29:05	1
W	URL: https://boe.es/buscar/act.php?id=BOE-A-2018-16673 Fetched: 2020-01-17 23:52:11	1
W	URL: https://hiperderecho.org/wp-content/uploads/2019/04/Ley_PDP.pdf Fetched: 2021-07-10 06:35:20	5
SA	**Universidad Privada del Norte / EF_TALLER DE TESIS 2_LAM TRIGOSO CHRISTIAN CHRISTOPHER.docx** Document EF_TALLER DE TESIS 2_LAM TRIGOSO CHRISTIAN CHRISTOPHER.docx (D151962475) Submitted by: Ramiro.Rondon@upn.edu.pe Receiver: ramiro.rondon.tamayo.delnor@analysis.urkund.com	19

DEDICATORIA

A Dios, por guiarme y mantener todas las opciones posibles de continuar estudiando.

A mi familia, especialmente mis padres quienes me brindaron su apoyo incondicional, siendo partícipes del proceso.

A mi asesor, por guiarme en el proceso y acoplarse a la disponibilidad en este contexto en particular

AGRADECIMIENTO

A Dios, el que en todo momento está conmigo ayudándome a aprender de mis errores y a no cometerlos otra vez.

A mis padres por ser los principales motores de mis sueños.

A mis abuelos, a quienes los llevo en mi mente y corazón todos los días de mi vida.

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo de la presente investigación fue determinar los efectos de la regulación jurídica del Big Data en la ley Nº29733 que garantice la protección de datos personales. La metodología usada fue de tipo cualitativa, con un nivel de investigación descriptivo y de tipo básica. En cuanto a la población se consideró finita por cuanto se conocía el número exacto de los elementos a analizar y la muestra fue no probabilista puesto que se escogió los elementos más idóneos y no se aplicaron técnicas estadísticas. Las unidades de análisis escogidas fueron artículos científicos, trabajos de investigación, normas jurídicas vigentes y sentencias de los tribunales nacionales e internacionales especializados. La técnica usada para la recolección de datos fue el análisis documental y el instrumento la ficha de análisis documental. Analizada las fuentes primarias se concluyó que la ley vigente en materia de protección de datos personales no contempla mecanismos de protección en cuanto al uso y manipulación de datos masivos a través de tecnologías Big Data, poniendo en gran riesgo la seguridad jurídica a las personas que tienen información personal y profesional en plataformas tecnológicas que se encuentra en el Internet o redes empresariales masivas, las cuales se encuentran grandes cantidades de datos en tecnologías donde se manipulan sin ningún control jurídico y sin seguimiento por parte de los usuarios.

PALABRAS CLAVES: Big Data, Protección de Datos Personales.

ABSTRACT

The objective of this research was to determine the effects of the legal regulation of Big Data in Law No. 29733 that guarantees the protection of personal data. The methodology used was qualitative, with a descriptive and basic research level. Regarding the population, it was considered finite because the exact number of elements to be analyzed was known and the sample was non-probabilistic since the most suitable elements were chosen and statistical techniques were not applied. The units of analysis chosen were scientific articles, research papers, current legal regulations and judgments of specialized national and international courts. The technique used for data collection was the documentary analysis and the instrument the document analysis sheet. Analyzing the primary sources, it was concluded that the current law on the protection of personal data does not include protection mechanisms regarding the use and manipulation of massive data through Big Data technologies, putting at great risk the legal security of people who have Personal and professional information on technological platforms found on the Internet or massive business networks, which are large amounts of data in technologies where they are manipulated without any legal control and without monitoring by users.

KEY WORDS: Big Data, Personal Data Protection.

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

A nivel mundial, la era de las tecnologías de información y comunicación ha marcado pautas en el desarrollo de la vida cotidiana de las personas, ya que, desde la explosión de la informática hasta la actualidad, se han creado aproximadamente, cinco exabytes de información que se encuentran en bases datos públicos y privadas. Actualmente, esa misma cantidad se produce cada dos días en virtud de la evolución de estas tecnologías en recabar grandes cantidades de datos y que son almacenados en servidores en diferentes partes del mundo. En ese sentido, la manipulación de bases de datos tan extensas ha propiciado el nacimiento del Big Data, cuyo desarrollo está siendo objeto de reflexión profunda acerca de sus consecuencias y su posible impacto en el mundo del derecho.

La existencia de un mundo digitalizado, en el cual el uso del internet está al alcance de cada persona, ha contribuido a que la manipulación de datos personales pueda estar al alcance de terceras personas, incluso se encuentran registros de hechos pasados que quedan almacenados en formato digital, pero se mantienen en la internet en diferentes aplicaciones en la web. (Olivos, 2020), en consecuencia, el derecho como ciencia, tiene como finalidad la regulación de las relaciones que se generan en la sociedad y debe establecer mecanismos con el fin de proteger los intereses de las personas en cuanto a la protección de los datos personales que se manipulan por cualquier medio electrónico.

En este orden de ideas, la privacidad y la protección de los datos de las personas se ha visto alterada en los últimos años por el surgimiento de las tecnologías de la información y principalmente internet, las normativas jurídicas vigentes especializadas en la materia a nivel mundial intentan controlar ese vacío jurídico que ha existido en estos últimos años entre una normativa desfasada frente a una tecnología que avanza cada año de maneras diversas,

"ahora este déficit se ha intentado ajustar con una normativa homogénea a nivel global que permita a la mayoría de los Estados adecuar el ordenamiento jurídico interno con estas nuevas directrices." (Aguad, 2018, p. 29)

En cuanto a la evolución normativa con respecto al tema, la regulación acerca de la protección de datos personales, se presenta en primer término en la Declaración Universal de los Derechos Humanos (1948), en cuyo artículo 12 reconoce que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia" (p. 10) esta misma idea es recogida por el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos (1966). Estos instrumentos son la base que ha permitido a los diferentes Estados a crear mecanismos normativos con la intención de proteger la privacidad de los ciudadanos impidiendo cualquier intromisión a los datos personales y a la privacidad.

Asimismo, a nivel jurisprudencial, un Tribunal Constitucional alemán, trajo a colación la importancia del control de la información de los datos de las personas. En esta sentencia se plateó en primer término, la necesidad de crear mecanismos jurídicos de protección de datos personales en razón de la manipulación de la información que se hacía en medio públicos y privados, por el peligro inminente que pueda producir en el uso de estos datos en la vulneración de los derechos de la privacidad de cada persona. (Herrán, 1998)

El derecho a la protección de datos personales como derecho autónomo ha tenido un desarrollo sustancial tanto a nivel doctrinal como jurisprudencial a nivel latinoamericano, donde se fundamenta en dos conceptos: intimidad y privacidad (Hernández, 2013), esta denominación es utilizada en diversos normas de rango constitucional y legal a nivel latinoamericano y en algunos casos, se ha considerado como una nueva categoría jurídica, autónomo de otros derechos de similar naturaleza, diferenciándolo del derecho a la intimidad. (Isaca, 2009).

La evolución normativa y jurisprudencial del derecho a la protección de datos personales ha tenido un largo recorrido en el Perú. Desde la década de los 90 este derecho fue reconocido como un derecho fundamental en la Constitución Política establecido en el artículo 2.6 de la mencionada norma, el cual otorga el derecho a la persona a tener plena disposición sobre los datos personales que se encuentren almacenado en cualquier medio, de modo que, previo consentimiento de la persona, estos medios pueden disponer de estos datos.

En este orden de ideas, el Tribunal Constitucional interpreta a través de diversas sentencias en razón de lo establecido en el artículo 61.2 del Código Procesal Constitucional, lo que se denomina en la actualidad como el derecho a la autodeterminación informativa, el cual consiste en aquellas facultades que tiene toda persona de ejercer el uso y control sobre la información personal que le es concerniente, que pueden encontrarse en registros públicos o privados, a fin de controlar posibles abusos y mal uso de estos datos.

El 3 de julio del 2011, el Estado Peruano promulga la Ley Nº 29733, Ley de Protección de Datos Personales y el 22 de marzo del 2013 mediante Decreto Supremo Nº 003- 2013 se aprobó el Reglamento. Esta norma desarrolla las garantías e instituciones encargadas de hacer cumplir el derecho de protección de datos personales y a la intimidad del individuo.

Los derechos y las obligaciones contenidas, tanto de la ley como en el reglamento, son particularmente complejas, ya que ante el abuso indiscriminado que se hacían de los datos personales de los ciudadanos, ahora se crearon, bajo parámetros estrictos, el control sobre esta información, mediante la autorización de la Autoridad de Protección de Datos Personales (APDP), actualmente adscrita a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIP), lo que ha permitido presenciar un gran avance en el ejercicio de este derecho.

Desde entonces, el impulso que se le ha dado a este instrumento jurídico, ha sido relevante, pero la legislación peruana aun presenta limitaciones frente a la evolución tecnológica, como la presencia de las tecnologías del Big Data. Schmarzo (2013) afirma que el consentimiento con todas las características requeridas por ley es uno de esos límites. En efecto, el procesamiento de grandes cantidades de datos hace imposible prever todas las finalidades para las cuales se utilizarán dichos datos; o determinar quiénes se beneficiarán de los mismos, entre otros aspectos importantes.

Un gran reto de la sociedad es la de actualizar constante y oportunamente la legislación para que acompañe a la innovación tecnológica y así mejorar las garantías que el Estado brinda sobre el derecho a la privacidad y a la protección de datos personales, es por ello que esta investigación se plantea una discusión, en torno a la implicación de las nuevas tecnologías de almacenamiento de datos masivos conocido como Big Data en la interpretación y ejecución de las normas jurídicas vigentes relacionadas con la protección de datos personales, con el objetivo de brindar aportes significativos a la investigación científica en torno a este derecho fundamental.

1.2 **Antecedentes de la Investigación**

Antecedentes Internacionales

Martínez (2017) en la investigación realizada en la ciudad de Valencia, España y titulada “Big data, investigación en salud y protección de datos personales ¿Un falso debate?” concluye que el uso de Big data ha producido cambios profundos en el ámbito de la salud, haciendo cambios de paradigma para la investigación y en la gestión sanitaria, pero presenta ciertas dificultades con respecto a la regulación en cuanto a la protección de datos de pacientes y personal de salud, la cual debe ser regulada e implementada por la legislación vigente en materia de protección de datos.

Navas (2015) en su artículo de investigación realizado en la ciudad de Barcelona, España y que lleva el título "Computación en la nube: Big Data y protección de datos personales" afirma que las tecnologías adaptadas a almacenar grandes cantidades de datos en la nube representan una ventaja para implementar la "Privacy by design". Esta herramienta consiste en que el titular de los datos tenga un mayor control sobre la información almacenada, en cuanto al uso y las medidas de seguridad que se puedan adoptar, prohibiendo el acceso sin un consentimiento previo y expreso y a la cancelación automática de datos, cuando ya no sea utilizada con el mismo propósito con los que sea había contratado.

González, Ruiz y Pollo (2016) realizaron una investigación en la ciudad Buenos Aires, Argentina, la cual fue titulada "Buenas prácticas para la protección de datos personales en ambientes de Big Data" donde determinaron que la capacidad de almacenar cantidades considerable de datos puede generar beneficios para la sociedad. Sin embargo, puede vulnerar la forma como se maneja el uso de los datos en las personas y la privacidad de la información y el derecho a la auto determinación informativa, es por ello que existen elementos que contribuyen a la seguridad de las organizaciones dedicadas al tratamiento de datos personales masivos, entre ellos está la aplicación de los principios de la privacidad desde el diseño, el cual le concede al titular de los datos mantener mayor control sobre los datos, en cuanto al uso que se les da y las medidas de seguridad que se aplican.

Gayo (2017) en su investigación titulada "Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas" la cual fue realizada en la ciudad de Santiago en Chile concluye que en el caso del tratamiento analítico de los datos masivos, el riesgo para la persona respecto a su privacidad y la protección de sus datos personales no está tanto en la obtención o el tratamiento, sino en el uso que se dé al resultado de dicho tratamiento y las consecuencias que este pueda tener para dicha persona. Es por

ello que en la medida en que la privacidad y la protección de datos personales convergen en el control de la persona sobre sus datos personales, son necesarias la transparencia y la responsabilidad aumentadas y seguramente el alcance de los conceptos de privacidad y protección de datos personales cambiarán en un futuro próximo, para evolucionar y seguir siendo un elemento esencial en materia de confianza y control de datos personales.

Guevara (2018) en su trabajo de grado realizado en la ciudad de Madrid, España y titulado "El impacto del Big Data en la protección de datos personales" observó la gran importancia de una regulación en materia de protección de datos unificada en todos los Estados miembros de la UE y que conociendo la tecnología del big data, se estableció que es una herramienta muy útil para el nuevo modelo de las empresas, donde se intenta estudiar cada paso que da el consumidor para poder ofrecer los mejores productos. Este aspecto que es muy positivo para las empresas, pone en tela de juicio hasta qué punto los interesados están dispuestos a este seguimiento y monitorización, exponiendo los datos más personales y desdibujando la diferencia entre vida privada, pública e intimidad.

Antecedentes Nacionales

Olivos (2020) en su artículo de investigación titulado "El derecho a la protección de datos personales en el Perú: 27 años desde su incorporación en la Constitución Política de 1993" establece que, a nivel de derecho comparado, El Perú, aun con el tiempo transcurrido, todavía tiene un pobre desarrollo en cuanto a la manipulación y protección de datos masivos. Los modelos de regulación tomados del sistema europeo el cual inspira el esquema regulatorio peruano, han pasado por importantes reformas como la entrada en vigencia en el 2016 del Reglamento General de Protección de Datos, el cual cambió el régimen aplicable sobre este tema en los países de la Unión Europea. La norma entró en vigor el 25 de mayo

de 2018, y partía de la concepción de que el tratamiento de datos personales debe estar concebido para proteger a la humanidad.

Aguad (2018) con su investigación "El Internet, el Big Data y el tratamiento de datos personales" concluye que en la mayoría de los casos, las políticas de privacidad y protección de datos personales ofrecidas a los usuarios son unilaterales y de difícil comprensión, las cuales pocas veces son leídas, es por ello que las nuevas herramientas que nos abordan día a día, como la geolocalización, el internet de las cosas, cloud computing y más, así como el acelerado avance en las técnicas de procesamiento de grandes cantidades de datos como el Big Data, son tan evidentes como los múltiples beneficios económicos y sociales que podríamos obtener de sus resultados. Es por eso que se tienen que encontrar soluciones aceptables a los problemas de privacidad que se generan con el desarrollo del Big Data en relación a la protección de datos personales, buscando mitigar los riesgos sin renunciar a los beneficios que esta proporcione.

Miyagusuku y León (2019) en su artículo de investigación titulado "Algoritmos laborales: big data e inteligencia artificial" concluyen que es innegable que las nuevas tecnologías, en especial la big data y la Inteligencia Artificial estarán cada vez más presentes en las relaciones de trabajo y las organizaciones podrán otorgarles la relevancia que estimen conveniente, pero para que dichas decisiones permitan una armoniosa convivencia entre el mundo laboral y la tecnología, tienen que ir acompañadas de un control normativo que permita monitorear las decisiones automatizadas de los algoritmos. Al final, en la ponderación entre la frialdad digital y la valoración humana debe privilegiarse esto último.

Alvarado (2016) en su investigación titulada "La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales" establece que el interés por la protección de datos personales es consecuencia del aumento progresivo de la

pérdida de confidencialidad e integridad debido al mal uso que se ha hecho de esta información de manera automatizada. En el Perú, con la promulgación de ley que regula la materia se incorpora el principio de seguridad que obliga a los titulares de las bases de datos y a los encargados de manipular la data, documentar todas las medidas de seguridad implementadas, tanto para la información digital como el almacenamiento de documentación no automatizada con el objetivo de evitar el riesgo de adulterar o alterar la información en beneficio de un tercero o la pérdida de información y cualquier tratamiento ilegal.

Valdivia (2019) concluye en su investigación titulada "La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información" que el modelo normativo construido para garantizar el respeto de este derecho fundamental ha sido fuertemente impactado por el Internet y las distintas expresiones que de forma global presenta la digitalización, por lo que se hace necesario cambiar el paradigma en el enfoque de la privacidad y de los derechos vinculados a ella para adaptarlo a las circunstancia actuales. La respuesta desde la normativa peruana de protección de datos frente al reto que plantean los factores de cambio, debe ser el de superar el modelo de gestión de datos para insertarse en un esquema de responsabilidad proactiva que contemporice con el fenómeno del Internet, con el Big Data, las redes sociales y, en general con todas aquellas nuevas formas de tratar datos personales para relacionarse o hacer de negocios, sin que por ello tenga que afectarse el núcleo esencial del derecho fundamental a la protección de datos como es la capacidad de control por parte del titular de la información.

1.3 **Bases Teóricas**

Big Data

Es el conjunto de tecnologías que permiten procesar cantidades masivas de información y datos personales a través del uso de algoritmos, con el propósito de darles utilidad en plataformas digitales y para la publicidad en línea (Guevara, 2018). Estas tecnologías pueden manejar datos cuyo volumen, variabilidad y velocidad de crecimiento sean complejos para capturarlos, procesarlos o analizarlos por parte de tecnologías convencionales.

El big data se aplica en dos fases: la primera fase consiste en un proceso que toma los datos, los inserta en los algoritmos y construye modelos que permiten realizar inferencias. Es importante saber que los datos recopilados han sido asociados de manera correcta. La segunda fase es en la que el nuevo conocimiento se puede utilizar para tomar decisiones. Fase donde puede surgir un mayor riesgo para la privacidad de las personas. (Hernández, C, 2019)

Tipos de Datos en Big Data

Para el análisis y procesamiento de datos con Big Data, se maneja tres tipos de datos, estructurados, no estructurados y semiestructurados.

Datos estructurados: este tipo de datos según la Escuela Superior Politécnica del Litoral ESPAE (2017) “son aquellos que se almacenan en campos de tablas de bases de datos relacionales donde su longitud, denominación y formato han sido predefinidos” (p. 6) La organización, estructura, el tipo, su posición y las posibles relaciones entre ellos, es conocida previamente La información se representa por datos elementales, no compuestos por otras estructuras.

Datos no estructurados: en este tipo de datos se almacenan en el formato en el que ha sido creados y no tienen una estructura definida, ni están almacenados en una tabla, por lo que de acuerdo a ESPAE (2017) la información no está compuesta por datos relacionales, sino por una composición de unidades estructurales de nivel superior.

Datos semiestructurados: ESPAE (2017) define a los datos semiestructurados como datos elementales, no tienen estructura fija a pesar de que tienen algún tipo de estructura implícita o autodefinida que se encuentran encapsulados en ficheros semiestructurados. Es el caso de documentos escritos con lenguaje HTML, XML o SGML.

Ciclo de análisis de Big Data

El objetivo principal de Big Data es mejorar la toma de decisiones en las organizaciones, en la ejecución de proyectos y en la ejecución de decisiones, tomando en cuenta que la toma de decisiones informada es un componente esencial para una organización. Para ello es importante realizar un análisis exhaustivo de la información previo a la toma de decisiones operativas y estratégicas. (Tabesh, Mousavidin y Hasani, 2019) para conseguir estos resultados se deben ejecutar cuatro fases que, según Hernández, C (2019) son las siguientes:

Fase 1: Es amplia y diversa, en esta fase generalmente se recopilan los datos no estructurados de fuentes internas, externas, fuentes procesadas es decir datos analizados utilizando herramientas analíticas avanzadas y diversos algoritmos para la generación de ideas.

Fase 2: Todo lo percibido en la fase 1 se transforma en decisiones, esto lo suelen hacer los gerentes, ellos generan ideas a partir de los datos analizados, además suelen asignar un significado especifico según amerite el caso.

Fase 3: Las decisiones generadas en la fase 2 se transforman en acciones operativas específicas. En este punto las decisiones se ejecutan.

Fase 4: Las decisiones que se ejecutan se transforman en acciones que generan resultados, el conjunto de datos resultante sirve para retroalimentar al proceso con el fin de mejorar la toma de decisiones futuras.

Inconvenientes del big data

Debido a la gran cantidad de interacciones diarias en la red y debido al uso que de la información intercambiada realizan las compañías y los Estados, se plantean nuevos retos en el ámbito de la infracción a los derechos fundamentales. Guevara (2018) afirma que no todo son ventajas en la implantación del uso del big data, principalmente hay tres aspectos que considera el autor que pueden ser negativos a la aplicación de estas tecnologías las cuales son: 1. el riesgo de incurrir en conclusiones erróneas que una persona no revise, ya que estamos expuestos a encontrar relaciones entre información que no tienen ningún tipo de relación que puede ser debido a la casualidad o al puro azar. 2. El riesgo que para las personas pueda tener tomar decisiones automatizadas sin una supervisión humana **y** 3. El riesgo para la privacidad de las personas y la violación de los datos personales. El empleo de los macrodatos implica en muchas ocasiones una intrusión en nuestro derecho fundamental a la protección de datos personales que deriva directamente de la Constitución y que se encuentra regulado en las leyes vigentes que tratan al respecto; además de una seria intrusión en el derecho a la privacidad. Con la expansión de Internet, se ha ampliado la amenaza al derecho a estos derechos, ya que, a través de las cookies o programas de rastreo, se posibilita el funcionamiento de las denominadas “redes de seguimiento”

Dato Personal

Es toda información que posea una persona para identificarlo o para que sea identificable, es decir, cuya identidad pueda determinarse por cualquier medio confiable mediante un identificador, como por ejemplo un número de identificación o elementos propios de persona que pueden ser fisiológicos, genéticos o sociales. (Rosales, 2019)

Derecho a la protección de datos personales

El artículo 8.1 de la carta de los Derechos Fundamentales de la UE, y en el artículo 16.1 del Tratado de Funcionamiento de la UE, establecen que toda persona física esta facultada para controlar los datos almacenados de carácter personal que estén ubicados en cualquier base de datos, así como dar su autorización para ser manipulados por terceros.

Siguiendo este orden de ideas, el Tribunal Constitucional del Perú (04739-2007-PHD/TC) incorpora el llamado derecho a la autodeterminación informativa, el cual consiste en la facultad que tiene toda persona de controlar la información personal que le sea pertinente a sus intereses, que puedan estar en registros públicos y privados de carácter informático, a fin de proteger intereses particulares ante un eventual abuso en el uso de información confidencial o personal.

Principios que regulan a la protección de datos personales

Principio del consentimiento: El art. 5 de la LPDP y art. 7 de su reglamento reconocen el derecho que tiene toda persona de poder autorizar de manera formal el uso y tratamiento de datos personales, es decir, cuando la persona que es dueña de la información presta su consentimiento de manera libre, expresa e inequívoca.

Principio de finalidad: los datos personales deben ser usados con el propósito que ha sido asignado por la persona que ha prestado su consentimiento de manera explícita y lícita. (Olivos, 2019)

Principio de proporcionalidad: toda manipulación de los datos personales debe ser adecuada y no debe excederse de la finalidad para la que estos fueron recogidos. (Olivos, 2019)

Principio de calidad: los datos ser manipulados de manera veraz y precisos, además deben ser adecuados respecto a la función para la que fueron recabados. (Olivos, 2019)

Principio de legalidad: los datos personales deben adecuarse a la norma jurídica vigente, por consiguiente, está prohibida la recopilación de los datos personales por medios fraudulentos e ilícitos. (Olivos, 2019)

Principio de seguridad: el responsable del banco de datos donde esta almacenada la información debe adoptar medidas estrictas en cuanto a los requerimientos técnicos necesarios para garantizar la seguridad de la información. (Olivos, 2019)

1.4 Formulación del problema

Ante todo, lo anteriormente planteado cabe preguntarse:

1.4.1 Problema general:

¿De qué manera la regulación jurídica del Big Data en la ley Nº29733 garantiza la protección de datos personales?

1.4.2 Problemas específicos:

¿Cuáles son los mecanismos de protección de datos personales contemplados en la Ley Nª29733?

¿Qué aspectos contempla las sentencias de tribunales naciones e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data?

1.5 Objetivos.

1.5.1 Objetivo general:

Determinar los efectos de la regulación jurídica del Big Data en la ley Nº 29733 que garantice la protección de datos personales.

1.5.2 Objetivos específicos:

O.E1 Analizar los mecanismos de protección de datos personales contemplados en la Ley N° 29733

O.E2 Analizar las sentencias de los tribunales nacionales e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data.

1.6 Hipótesis

La presente investigación no contiene hipótesis a demostrar, ya que, al tratarse de una investigación de enfoque cualitativo perteneciente a la hermenéutica jurídica, lo que busca el investigador es revelar el significado que tienen los fenómenos investigados en el pensamiento colectivo. “Estos datos son subjetivos, no se pueden pesar, medir ni contar, por consiguiente, la hipótesis se usa como una herramienta orientadora de la precisión matemática en investigaciones de tipo cuantitativas.” (Millán, 2008 p. 25). Sí puede ser usada como una orientación general para reforzar la dirección que tiene que seguir una investigación, pero no es una obligación metodológica usarla y se puede prescindir de ella sin problemas porque en las investigaciones cualitativas no existen suposiciones por adelantado.

1.7 Justificación del problema

La presente investigación plantea la noción de analizar las circunstancias en las que se están manipulando grandes cantidades de datos con las tecnologías del Big Data en el contexto de la pandemia del COVID-19 la cual ha afectado a miles de personas en todo el planeta. Además, se abordará la necesidad de determinar el equilibrio debe existir entre la protección de datos personales y la evolución que ha generado la tecnología, cuyo derecho a la privacidad de estos datos conjuntamente con la innovación permite generar la confianza necesaria en el ciudadano. Para Carrasco (2006) toda persona al momento de justificar la investigación debe exponer, argumentar o sustentar los motivos por los cuales se realiza dicha búsqueda con el objetivo principal de responder la pregunta de la investigación. Al respecto, se presentan tres dimensiones:

- Una justificación teórica, ya que esta investigación determinará, a través de las definiciones de los diferentes doctrinarios, las decisiones de los tribunales nacionales e internacionales y las normas jurídicas vigentes, la conceptualización y características fundamentales de las tecnologías del Big Data, asi como los efectos que producen en la manipulación de datos personales masivos y su regulación en instrumentos normativos internacionales, haciendo énfasis en la necesidad de incorporar estas directrices a la normativa nacional vigente; esto aportará la formulación de nuevos criterios jurisdiccionales en el ámbito del derecho civil en materia de protección de datos personales y enriquecerá la doctrina nacional vinculante al tema objeto de estudio.
- Una justificación práctica, ya que el estudio aportará soluciones ante la ausencia de regulación de orden constitucional en cuanto a la protección de datos personales cuando se hacen uso de estos en medios electrónicos donde se manipulan grandes

cantidades de información, vulnerando el derecho a la privacidad y confidencialidad que tiene toda persona sobre sus datos; también busca orientar al legislador nacional para la regulación de las tecnologías del Big Data e incorporarlas a una futura reforma de la ley Nº 29733 para la protección de datos ; estos aspectos serán profundizados en la investigación a través del desarrollo y análisis que se le hará a la doctrina, la ley y la jurisprudencia en cuanto a la necesidad de regular la manipulación de datos personales a través de las tecnologías del Big Data.

- Una justificación metodológica, porque cumple con el rigor de una investigación científica, partiendo de la observación de un problema o fenómeno de estudio, que permitirá crear conocimiento confiable a través del desarrollo de varias etapas del proceso investigativo con base al análisis de fuentes bibliográficas, tales como artículos científicos, trabajos de investigación, leyes vigentes, jurisprudencia nacional e internacional y la opinión de abogados especialistas que contribuirá al abordaje de la problemática descrita, con el fin de desarrollar los objetivos propuestos y responder a la pregunta de investigación planteada, a través de un proceso metodológico ordenado y sistematizado, empleando técnicas de investigación cualitativas, como el análisis documental y la entrevista, además los instrumentos que se diseñaran serán aporte significativo para investigaciones futuras.

CAPÍTULO II: METODOLOGÍA

2.1. Tipo de investigación

Esta investigación según su enfoque es de tipo cualitativo por cuanto propone la interpretación y evaluación de la información lograda mediante técnicas, con la finalidad de indagar en su significado. La investigación de corte cualitativo es la que produce datos descriptivos, con la opinión de expertos de forma verbal o escrita y la observación de conductas, constituida por un conjunto de técnicas de recolección de datos validas y confiables. (López y Sandoval, 2012)

En cuanto al alcance de la investigación, ésta es de tipo correlacional, la cual es definida como un tipo de estudio que tiene como propósito evaluar la relación que exista entre dos o más conceptos, categorías o variables. Hernández et al (2014) señalan que el propósito principal de este tipo de estudios es conocer el comportamiento de un concepto o variable comparándola con el comportamiento de otras variables relacionadas. Es por ello que en la presente investigación se busca determinar la relación entre la variable "Big Data" y la variable "protección de datos personales"

Según el propósito, la presente investigación es de tipo básica, ya que su razón de ser se centra en explicar las características del problema o fenómeno que se presenta en un determinado lugar de la sociedad. (López y Sandoval, 2012)

El diseño de esta investigación es no experimental ya que no se van a manipular las variables de manera intencional. Para Hernández et al (2014) en la investigación no experimental la variable independiente no debe ser manipulada, ya que es un hecho que se ha manifestado en la realidad y el investigador no tiene control para modificar dicho fenómeno ni sus efectos.

Al ser una investigación de corte no experimental, se considera a la misma de forma transversal ya que los datos se tomarán en un solo momento, es decir, se analiza la incidencia e interrelación en un momento determinado (Hernández, Fernández y Batista, 2014).

2.2. Población y muestra

La población se define como el "cumulo finito o infinito de componentes que poseen características comunes para los cuales se hacen extensivos los resultados obtenidos en una investigación." (Arias, 2016 p. 18). En la presente investigación la población se establece como finita, por cuanto se conoce el número exacto de elementos que contribuirán a lograr los objetivos propuestos en la investigación. Las unidades de análisis estarán comprendidas por:

- 5 artículos científicos nacionales e internacionales y 5 trabajos de investigación comprendidos entre el periodo de 2010 a 2020 en idioma español y que hayan sido publicados en revistas indexadas o repositorios universitarios.
- 3 normas jurídicas nacionales vigentes, que su contenido pueda ser descargadas directamente de la base de datos del órgano legislativo correspondiente y que su aplicación sea de carácter general
- 10 sentencias de los tribunales especializados, tanto nacionales como internacionales, que estipulen controversias relacionadas con recursos de casación, apelación o agravio constitucional relacionadas con las variables "big data" y "protección de datos personales" o algunas de sus dimensiones.
- 4 entrevistas realizadas a 2 expertos en el área de la protección de datos personales y 2 abogados especialistas en derecho informático, con 5 años de experiencia en el área.

En cuanto a la muestra, ésta será de tipo no probabilístico, ya que la población está comprendida por un número específico de elementos y no se empleará ningún procedimiento de muestreo, porque se tomará la totalidad de la población. (García, 2017)

Para esta investigación, la muestra fue seleccionada en razón de las características que el investigador considera pertinentes para recoger los datos necesarios con el fin de dar respuestas a los planteamientos de la investigación, los cuales se describen a continuación:

Tabla 1

Características de los artículos científicos

Año de publicación	Autor/es	Título de la publicación	País de publicación	Base de Datos extraído
2015	Ojeda Bello	El derecho a la protección de datos personales desde un análisis histórico-doctrinal	México	Proquest
2017	Vélez, C.	La explotación de los datos personales por los gigantes de internet	Colombia	Google Académico
2017	Gómez & Martínez	Política antes que regulación: La protección de la información personal en la era del big data	España	Google Académico
2019	Martínez Devia	La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales?	España	Redalyc
2019	Urueña R.	Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del "big data"? (2018)	Colombia	Scielo

Fuente: Elaboración propia

Tabla 2

Características de los trabajos de investigación

Año de publicación	Autor/es	Título de la publicación	País de publicación	Base de Datos extraído
2015	Gil González	Big data, privacidad y protección de datos	España	Google Académico
2017	García Chumioque	El derecho a la protección de datos personales y los motores de búsqueda en el Perú	Perú	Google Académico
2012	Cerna Figueroa	Análisis del objeto de la ley de protección de datos personales en la constitución	Perú	Google Académico
2019	Franco y Quintanilla	La protección de datos personales y el derecho al olvido en Perú. Sobre el propósito de los estándares internacionales del Sistema Interamericano de Derechos Humanos	Perú	Redalyc
2019	Álvarez Valenzuela	La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa	Chile	Google Académico

Fuente: Elaboración propia

Tabla 3

Características de las normas jurídicas

Año de promulgación	Órgano legislador	Título de la norma
1993	Congreso Constituyente Democrático	Constitución Política del Perú
2011	Congreso de la Republica	Ley de protección de datos personales Ley Nª 29733
2013	Congreso de la Republica	Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales

Fuente: Elaboración propia

Tabla 4

Características de las sentencias

N° de Sentencia	Organismo o Tribunal	Recurso interpuesto
SSTC 11/1998, FJ 5, 94/1998	Tribunal Constitucional Español Nº 292/000	Recurso de Nulidad derecho de control sobre los datos relativos a la propia persona
EXPTE. N° 5.528/2010	La Corte Suprema de Justicia de la Nación (Argentina)	Recurso de Apelación. Acceso a bases de datos sin autorización previa
Sentencia C-1011/08	La Sala Plena de la Corte Constitucional	Revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

EXP N ° 04027 2013-PIID/TC	Tribunal Constitucional	Recurso de agravio constitucional. Habeas Data y la protección de datos personales
EXP. N.° 05484-2015-PHD/TC	Tribunal Constitucional	Recurso de agravio constitucional. Derecho a la autodeterminación de los datos
Nº 73-624-40-89-002-2003-053-00	Juzgado Segundo Promiscuo Municipal Rovira Tolima (Colombia)	Acción de tutela por la violación al derecho constitucional de habeas data, autodeterminación informática y la intimidad mediante spam
Nº 09- 009434-0007-CO	Sala Constitucional de la Corte Suprema de Justicia (Costa Rica)	Recurso de amparo. Derecho a la autodeterminación de la información
Nº 08- 011774-0007-CO	Sala Constitucional de la Corte Suprema de Justicia (Costa Rica)	Recurso de amparo. Violación del derecho a la intimidad y la autodeterminación de la información
Nº 1356-2006	Corte de Constitucionalidad (Guatemala)	Amparo provisional. Violación a la intimidad y a la protección de datos personales
Tribunal de Apelaciones en lo Civil de 5º Turno Nº 12 Sentencia Nº 12	Tribunal de Apelaciones en lo Civil de 5º Turno Nº 12	Acción de protección de datos personales en el marco de la nueva Ley Nº 18.331

Fuente: Elaboración propia

2.3 **Técnicas e instrumentos de recolección y análisis de datos**

Según Bernal (2016) las técnicas de recolección de datos comprenden una serie de procedimientos que permiten al investigador obtener información necesaria para responder la pregunta planteada como parte de la realidad problemática objeto de estudio. Para la investigación se tomarán como técnica, el análisis documental.

Esta técnica es definida como un conjunto de pasos intelectuales que buscan describir los documentos de forma sistemática para su mejor comprensión. “Comprende el

procesamiento analítico- sintético que, a su vez, incluye la descripción bibliográfica y general de la fuente, la clasificación, indización, anotación, extracción, traducción y la confección de reseñas." (García, 2002 p. 89).

En cuanto a los instrumentos de recolección de datos, Bernal (2016) los define como aquellos medios materiales que se utilizar para almacenar la información, entre los más usados están las fichas, los cuestionarios, guías de entrevista, escala de actitudes u opinión y la lista de cotejos.

El instrumento que se utilizó para la recolección de datos en la presente investigación es la ficha de análisis documental la cual sirvió para examinar la información encontrada en las fuentes bibliográficas y jurídicas manipuladas en esta investigación, a través de resúmenes que aporten indicios suficientes en cuanto a la problemática generada, lo cual será detallado de acuerdo al análisis que se realice en función de los objetivos a alcanzar. (Dulzaides y Molina, 2004)

Para el proceso de recolección de datos se procedió a realizarlo en varias fases con el fin de realizar la discusión de los resultados, donde se ha empleado el método inductivo, ya que la investigación se va a desarrollar según las categorías y sub categorías, de lo particular a lo general, y no se clasificará la información, sino que debe contener un producto intelectual (Glaser,1978); dichas etapas se mencionan a continuación:

- El estudio se inició seleccionando las referencias bibliográficas que avalaran los conceptos y teorías utilizadas; para la selección de los artículos de investigación científica y trabajos de investigación se extrajeron de bases de datos confiables como: Scielo.org, Google académico (https://scholar.google.es), Redalyc.org, Proquest.org y Dialnet.es

- En el caso de la recolección de las jurisprudencias, se tomó como base de datos confiable, la página web de la Corte Superior de Justicia (https://www.pj.gob.pe) y base de datos de las paginas web de los órganos judiciales de Guatemala, Colombia, España y Uruguay, organizando por fecha, tipo de recurso y la resolutoria de cada una de las sentencias, que dan respuesta a los objetivos planteados
- Luego de haber obtenido todas las fuentes documentales, se procedió a escoger la información relevante de cada uno, clasificándola por cada objetivo, tanto general como específicos, diseñando una tabla en Excel donde se va a colocar el resumen de las ideas principales y secundarias a través la técnica de triangulación de métodos de recolección de datos.
- Escogida la teoría se procedió a determinar las categorías y sub categorías que permitieron establecer la relación entre estos elementos y los objetivos planteados de la investigación
- Definida la metodología a utilizar en la investigación, se procederá a la recolección de datos diseñando la ficha de análisis documental, la cual se utilizó para hacer la síntesis de los argumentos más importantes de cada fuente primaria.
- Luego se procedió al diseño de los instrumentos con respecto a cada técnica establecida, utilizando los programas de Microsoft Word y Excel para almacenar y ordenar la información recabada de manera digital.
- Se aplicaron las entrevistas, por medio de sesiones planificadas, previa invitación formal a los entrevistados por correo electrónico. Una vez confirmada la disposición de los expertos, se procede a realizar la sesión por los medios disponibles electrónicos para recabar la información necesaria en el desarrollo de la investigación.

- Seguidamente se realizará el tratamiento de los datos, una vez hechas las fichas de análisis documental, se sistematizo los datos obtenidos para su respectivo análisis, a través de cuadro en Excel, el cual facilitó la triangulación de la información y el desglosamiento de los resultados.

Concretada la recolección de los datos, se procedió a definir el método para el análisis de datos, el cual será el método comparativo, el cual consiste confrontar dos o varias propiedades mencionadas en dos o más objetos, en un momento preciso o en un arco de tiempo más o menos amplio. En este método se comparan unidades geopolíticas, procesos, e instituciones, en tiempo real. (Fideli, 1998) En el caso de la presente investigación, se compararon las diferentes revisiones bibliográficas de acuerdo a su relación con cada categoría definida, de acuerdo a una escala de valores, efectuando el análisis de los resultados obtenidos en cada una de las categorías y sub categorías mediante el software "Excel."

Por ser una investigación jurídica, el método de análisis de información que se realizo fue a través del método exegético – dogmático, el cual consiste en la interpretación y el estudio de los textos legales y que se centra en la forma en la que fue redactada la ley o regulación por parte del legislador. (Sánchez, 1980), es decir que, para determinar la necesidad de incorporar la regulación del Big Data en la ley Nº 29733 en la protección de datos personales, se hará un análisis literal del contenido de las normas jurídicas vigentes que regulan esa materia, conjuntamente con la interpretación realizada en la jurisprudencia y expertos en la materia, para luego comparar y contrastar resultados a través de la triangulación de la información. Obtenidos los resultados se procederá a realizar la discusión en consonancia con los estudios previos citados, las conclusiones y las recomendaciones.

2.4 Aspecto ético

La investigación se enmarcó en los estándares existentes y permitidos dentro del proceso de investigación científica. En su desarrollo se respetó la confidencialidad de las personas involucradas en el proceso; además de tratarse de una investigación inédita, ya que el estudio no es una compilación, replicación o copia de otras investigaciones realizadas con anterioridad; es original, porque los autores empleados en el desarrollo de la investigación y que dan soporte a la misma se referenciaron en base a lo indicado en el Manual APA sexta edición versión en español.

En la presente investigación se utilizaron los datos obtenidos, sólo para uso de la discusión y resultados; los lineamientos éticos básicos como son: respeto a la dignidad humana, honestidad, equidad, respeto de los derechos de terceros, veracidad de la información, relaciones de igualdad y confidencialidad, asumiendo en todo momento el compromiso ético durante las diferentes etapas de realización de la investigación, con el propósito de dar cumplimiento a los principios ya enunciados.

CAPÍTULO III: RESULTADOS

Para Bernal (2010) menciona que, recolectada la información, queda contrarrestarla con los objetivos de manera cuidadosa. Esta etapa se denomina los resultados de la investigación". Por lo tanto, este proceso comprende la recolección de la información proveniente de las técnicas señaladas en la metodología, es por ello que, en esta etapa de la investigación, se llegaron a los siguientes resultados.

3.1 Resultados obtenido con la técnica: Entrevista

- **Objetivo General**

  Determinar los efectos de la regulación jurídica del Big Data en la ley Nº29733 que garantice la protección de datos personales

  Pregunta: Desde los avances legislativos que se han ido materializando a nivel nacional en materia de protección de datos personales ¿Cómo analiza la situación en torno a la masificación del uso de tecnologías de información y comunicación como el Big data y su afectación en los derechos de las personas en cuanto al uso de los datos personales?

Alvarado (2022) considera que con el uso masivo del Internet a nivel global, cada vez se generan más datos en la web, grandes volúmenes de datos, principalmente data no relacional, esto da origen a que la información quede cada vez más expuesta, más aun con la proliferación de herramientas de Inteligencia Artificial, las cuales hacen que la información obtenida por fuentes externas sea aún más valiosa, para que los usuarios se vean menos afectados por esta "invasión de la privacidad", se han venido gestando a lo largo del tiempo algunas normativas que están ayudando a que la información sea menos vulnerable.

Franco (2022) considera que desde la publicación de la ley de protección de datos personales la tecnología y el uso de los sistemas de información se ha masificado, donde se puede observar que el uso de la información es de forma constante por parte de los sistemas privados y del estado si la entidad no ha realizado la implementación de la ley de protección de datos personales posiblemente el protocolo que tienen para el uso de la información no sea el adecuado y pueda afectar la información existente.

González (2022) explica la forma en que se dividen los datos: en datos no estructurados (documentos, vídeos, audios, etc.), datos semi-estructurados (software, hojas de cálculo, informes.) y datos estructurados. En cuanto a las medidas necesarias para cada tipo de tratamiento para evitar los riesgos que podrían darse, considera que la legislación no va por ahí sino que considera que existe un checklist de medidas que se tienen que realizar en la que no se incluye la evaluación del impacto de los riesgos y las medidas para cada tipo tratamiento sino que señala que tiene que haber una trazabilidad que tiene que ser proporcional, que las medias de seguridad tendrían que ser adecuadas, entonces faltaría aterrizar en ese punto en específico, eso paso porque tampoco tenemos todavía una cultura protección de datos personales, las empresas más grandes que tienen negocios con Europa si lo hacen por cumplir las normas de Europa al momento de recopilar los datos; por otro lado, las empresas que tienen sus negocios en Perú no necesariamente realizan esta evaluación.

Vera (2022) considera la Autoridad Nacional de Protección de Datos Personales adscrita al Ministerio de Justicia y Derechos Humanos tiene como funciones, entre otras, hacer que las entidades públicas y privadas cumplan las obligaciones que establece la Ley de Datos Personales y su reglamento, coligiéndose que el ámbito de aplicación de ambas normas rige tanto para el sector público como el privado. No obstante, cabe señalar que, si

bien el tratamiento de datos personales está regulado en la Ley de Protección de Datos Personales y su reglamento, ambas normas no profundizan o abordan de manera específica en cuanto al tratamiento masivo de datos estructurados (tradicionalmente utilizados en tratamiento de datos, se caracterizan por ser almacenables en tablas, con clara definición de longitud y formato, como por ejemplo: los números, cadenas de caracteres y fechas); de datos no estructurados (no poseen un formato específico que permita almacenarlos de forma tradicional pues no se puede desglosar la información que facilitan a tipos de datos definidos en longitud y formato, como por ejemplo: email, presentaciones multimedia como Power Point, archivos en formato PDF) y datos semi-estructurados (siguen cierta estructura pero al ser irregular no permite gestionarla como datos estructurados, por ejemplo: el HTML, lenguaje para la elaboración de páginas Web) y es ahí donde entra a calar la tecnología del big data que se constituye como una herramienta de análisis masivo de datos; siendo importante resaltar que aunque de manera posterior, el Estado ha emitido una serie de normas donde se dispone de manera general el uso eficiente de datos masivos para promover el aprovechamiento de tecnologías emergentes, las mismas circunscriben más que nada su ámbito de aplicación a las entidades del Estado y no abordan de manera directa y profunda una regulación sobre big data.

> **Pregunta:** Desde su experiencia ¿Cómo ha resuelto la legislación nacional vigente la regulación de la protección de datos personal a través del uso de tecnologías como el Big data y cuáles han sido sus efectos en los últimos años?

Franco (2022) considera que, en atención a este principio, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiese prestado su consentimiento libre, previo, expreso, informado e inequívoco. Actualmente, el principal mecanismo que permite que las empresas traten nuestros datos personales utilizando el Big Data es a través

de las políticas de privacidad ofrecidas a los usuarios como términos unilaterales y contractuales, que se han convertido en la piedra de la protección de la privacidad, a pesar de la aplastante evidencia de que la mayoría de las personas ni siquiera lee los términos o no los comprende.

Por otro lado, Alvarado (2022) considera que la protección de datos personales está contemplada inclusive en la constitución de 1993, sin embargo en los últimos años, se han estado ampliando los alcances a través de normativas y regulaciones jurídicas las cuales se van actualizando de acuerdo a las necesidades actuales, en mi opinión los efectos han sido favorables, pues estas normativas obligan a las plataformas de servicios web que las contemplen y se rijan a ellas, disminuyendo así el riesgo de vulnerar nuestra información y a no suministrar información que afecten la intimidad personal y familiar.

En el caso de González (2022) menciona que la Ley N° 27933, Ley de Protección de Datos Personales y su reglamento, se respalda del Decreto Legislativo N° 1412, (que aprueba la Ley de Gobierno Digital) y en su reglamento (aprobado con Decreto Supremo Nº 029-2021-PCM) los cuales señalan la existencia de un oficial de datos para entidades públicas y que las entidades públicas si tienen que aplicar la privacidad desde el diseño, ese sería el avance que hay en esa materia. Asimismo, la norma refiere el oficial mayor debe ser un especializado en la materia, y del mismo modo, señalar que el Perú aún no está en el estándar de reglamento de protección de datos personales de Europa, ahí indican que tiene que tener cierta autonomía, vínculo con la alta dirección, y además eso solo aplica para entidades públicas en nuestro caso, no aplica para empresas privadas que hagan tratamiento de datos masivos, para tal caso existe una tarea pendiente por desarrollar.

Por último, Vera (2022) considera que la Ley N° 27933 y su reglamento regula el tratamiento de datos personales, pero no profundiza o aborda de manera específica el

tratamiento masivo de datos personales a través de la tecnología big data. Asimismo, el Estado ha emitido una serie de normas donde se dispone de manera general el uso eficiente de datos masivos para promover el aprovechamiento de tecnologías emergentes, sin abordar de manera directa y profunda una regulación sobre big data. Así se tiene al Decreto Legislativo N° 1412, (que aprueba la Ley de Gobierno Digital) y su reglamento (aprobado con Decreto Supremo Nº 029-2021-PCM); al Decreto de Urgencia Nº 006-2020 (que crea el Sistema Nacional de Transformación Digital) y su reglamento (aprobado con Decreto Supremo Nº 157-2021-PCM); a la Resolución de Secretaría de Gobierno Digital Nº 003-2019-PCM-SEGDI (que dispone la creación del Laboratorio de Gobierno y Transformación Digital del Estado en la Presidencia del Consejo de Ministros). Sobre el particular, si bien tales normas (aplicables algunas solo en el ámbito público) disponen que su aplicación debe efectuarse garantizando la protección adecuada de los datos personales de los titulares, hay tener claro que ello es un primer paso que se ha dado y es bueno; no obstante, debo precisar que el Perú aún no está en el estándar de protección regulado en el continente europeo, como de manera ilustrativa cabe mencionar al reglamento de protección de datos personales de Europa (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo).

- **Objetivo Especifico 1**

  Analizar los mecanismos de protección de datos personales contemplados en la Ley N° 29733

  Pregunta: ¿Considera usted que han sido efectivos los mecanismos establecidos en la Ley N°29733 de Protección de Datos Personales y como ha sido el tratamiento jurisprudencial en cuanto a la aplicación de esta norma?

Franco (2022) considera que La ley estable sus normas, pero el tratamiento de la información va depender de la aplicación de ley. Este poder de decisión y protección que le

da el Estado respecto a las posesiones que tengan los demás de estos datos tendrá la protección para evitar exposiciones y riesgos a los que estamos tales como los robo de identidad, extorsiones y otras formas que vulneren nuestra privacidad, asimismo poder dar una orientación correcta de la información que deseara recibir de los demás, establecer parámetros debidos para recibir publicidad, ofertas y demás servicios análogos que más de una ocasión a puede habernos simplificado la búsqueda o satisfacción de una necesidad.

Alvarado (2022) afirma que los mecanismos establecidos en la citada norma han sido efectivos, ya que estos van evolucionando de acuerdo a las necesidades actuales y al avance de la tecnología en cuanto al Big Data, ya que el avance de esta tecnología hace que nuestra información sea más vulnerable por la gran cantidad de información que se genera día a día a través del Internet, ya sea en nuestro ordenador o teléfono inteligente, en cuanto al tratamiento jurisprudencial respecto a esta materia, ha sido positivo también, ya que gracias a la ayuda de las herramientas de Big Data se han recopilado un sin número de casos, que están permitiendo tenerlos como referencia para el tratamiento de casos similares.

Por otro lado, González (2022) considera que no es un problema de efectividad de la norma, sino que debe ir evolucionando conforme también evoluciona y evolucionará la tecnología (Cookies, big data), la Autoridad Nacional de Protección de Datos Personales tiene la potestad de hacer directivas que se tienen planificadas y trazadas; asimismo, sería necesario que la Autoridad crezca como otras entidades más grandes como el caso de Indecopi, que tenga cierta autonomía administrativa, no en el tema de tomar decisiones respecto a los procedimientos administrativos, dado que hay si existe autonomía, pero solo tener autonomía administrativa no es suficiente para que crezca la Autoridad Nacional de Protección de Datos Personales, como si es el caso de otros países.

Por último, Vera (2022) menciona que de alguna manera es saludable la existencia de dichas normas (Ley y su reglamento), y claro que han tenido efectos positivos en los ciudadanos, no obstante muchas de las prácticas empresariales y actividades a veces se realizan para demostrar que se está cumpliendo con lo que está redactado en el texto de una ley, sin embargo cabe la posibilidad que se podría estar afectando negativamente al titular de los datos personales (persona que brinda sus datos personales para tratamiento), en este caso no basta solo demostrar que existen los mecanismos necesarios (políticas, procedimientos, avisos, etc.) sino demostrar que se cumpla el objetivo para el cual han sido incluidos en la Ley 29733, debiendo tener espacial énfasis en la valoración del cumplimientos de los principios rectores de la precitada Ley y ello debe aplicarse a las nuevas tecnologías que no paran de evolucionar día tras día (Cookies, big data, etc).

> **Pregunta:** ¿Cuáles han sido los beneficios y las desventajas que ha traído la promulgación de esta norma en cuanto a los mecanismos establecidos para la protección de los datos personales relacionadas como el uso de tecnologías como el Big Data?

Franco (2022) enumera que las principales ventajas serian: Aumentar la seguridad de la información y protege frente a fraudes, ciberataques como hackeos o suplantación de identidad. Permitir que solo accedan a nuestros datos aquellos usuarios, empresas o proveedores de servicios a los que hayamos otorgado nuestro consentimiento. Adecuar a nuestro perfil y nuestros intereses los contenidos, productos o servicios que se nos ofrecen. Concienciar cada vez más a la gente sobre la importancia de proteger los datos personales. Las principales desventajas serian: Si la información llega sale de la infraestructura de datos de una entidad pública o privada y llega al Internet que es una red inmensa, en la que circula una cantidad ingente de datos. Por tanto, tratar de controlar todo este flujo de información

no es un objetivo realista. Entra en conflicto con los intereses de grandes empresas y corporaciones. Muchas de estas compañías tienen un enorme poder y prefieren hacer frente al pago de multas antes que hacer caso a las normas sobre privacidad que dictan los gobiernos. Todavía existe mucha gente que no comprende la importancia de proteger la información. Muchas personas siguen aceptando términos y condiciones de uso sin leerlas. A las generaciones pasadas les cuesta adaptarse a las nuevas exigencias en este campo, ya que la era digital avanza rápidamente y no espera por nadie.

En el caso de Alvarado (2022) considera que han sido más ventajas que desventajas y las ventajas van más por el tema de seguridad de la información, pues a través de la utilización de mecanismos legales y tecnológicos que permitan cumplir este cometido, nuestra información será menos propensa a vulnerabilidades de todo tipo y a ser mal utilizada si esta cae en las manos equivocadas.

Por otro parte, González (2022) considera que la protección de datos ha sido lo fundamental, el cual es un derecho fundamental que está consagrado en la Constitución y nos permite pues tener mayor control sobre nuestra información, ver con quien las compartimos, que nos informen para que la van a usar y nosotros poder decidir si damos o no estos datos. Por otro lado, las desventajas podríamos decir que las empresas tienen más libertad para con sus operaciones (marketing, servicios en la nube, sector financiero), pero la aplicación de un derecho no puede ser considerado una desventaja.

En el caso de Vera (2022) considera que los beneficios que la norma desarrolla es el derecho a la protección de datos, el cual es un derecho fundamental que está consagrado en el artículo 2°, numeral 6 de la Constitución Política del Perú, en el cual nos permite tener un control sobre la información que proporcionamos sea a una entidad pública o privada, es decir tener garantiza el derecho irrestricto a la autodeterminación informativa a la protección

de datos como parte de las libertades de derechos que debe tener todo ciudadano que le permitan a uno realizar su proyecto de vida sin intromisión de terceros y con la garantía del estado de por medio. Por otro lado, afirma que la aplicación de un derecho (Ley N° 29733, reglamento, etc.) como una desventaja, eso no quita que, en algunos extremos, con respecto al big data, puedan existir problemas, ambigüedades, deficiencias o vacíos normativos.

> **Pregunta:** ¿Considera usted que es necesaria que exista una regulación especial en la protección del derecho al resguardo de los datos personales de las personas en el uso de estas tecnologías? ¿Existe alguna propuesta legislativa?

Franco (2022) menciona que es necesario porque la información que se procesa son datos personales se refieren simplemente a los registros u otra información que por sí sola o vinculada con otros datos, puede revelar la identidad de una persona viva. Así, por ejemplo, puede utilizar números en lugar de nombres como identificadores en una encuesta, pero si mantiene otro registro vinculando esos números a los nombres reales, se considera que cada registro contiene información personal. Son considerados “Datos personales” datos como teléfono, edad, dirección personal o laboral, colegios o establecimientos educacionales a los que asistió una persona, entre otros.

Por su parte, Alvarado (2022) menciona que desconoce si existe alguna propuesta legislativa respecto a este tema, pero afirma que debe existir una regulación especial en la protección del derecho al resguardo de los datos personales de las personas en el uso de estas tecnologías, pues el tráfico de datos en la web aumenta cada día, a su vez cada vez se liberan herramientas más inteligentes de procesamiento de datos a gran escala, las cuales sumadas a los algoritmos de inteligencia artificial que están por toda la red, es necesario tener normativas de regulación cada vez más específicas para cumplir con el objetivo de protección de la información.

Por otro lado, González (2022) considera necesario tomar en cuenta la reforma legal en el marco de la protección de datos personales en el uso de esta tecnología, dado que es un tratamiento masivo específico y que requiere ciertos cuidados, yo creo que pasaría por una evaluación de impacto y me parece que con eso ya podríamos tener el tema más más aterrizado, pero todavía nos falta una cultura de protección de datos personales.

Por último, Vera (2022) menciona que si debe existir una reforma con urgencia, dado que implica un tratamiento especial que comprende grandes volúmenes de datos el cual requiere ciertos cuidados, por dar un ejemplo en cuanto al procesamiento del big data, afirma que la legislación presenta ciertas limitaciones con respecto al consentimiento y sus características requeridas por ley, en el especifico de que el procesamiento de grandes cantidades de datos hace imposible prever todas las finalidades para las cuales se utilizarán dichos datos (lo cual va íntimamente ligado con el escenario en el cuales se requiere dar un nuevo uso a los datos personales respecto de los cuales en un primer momento si se cumplió con recabar el consentimiento informado, expreso e inequívoco del titular); o determinar quiénes se beneficiarán de los mismos, entre otros, es decir algunos principios rectores consagrados en el Título I de la Ley N° 29733 son rebasados por el Big Data, en ese sentido, creo que es importante iniciar este camino de conciencia común sobre lo que implica este derecho fundamental.

- **Objetivo Especifico 2**

  Analizar las sentencias de los tribunales nacionales e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data.

  Pregunta: ¿Cuál ha sido el tratamiento jurisprudencial nacional en materia de protección de datos personales en el uso de tecnologías como el Big Data? En caso

de que no exista poco desarrollo jurisprudencial en esta materia ¿A que se debe esta situación?

Franco (2022) considera que en la realidad actual el uso de aplicaciones móviles y de Internet de las Cosas ya que son parámetros que se tiene que tomar en cuenta. No se puede poner en duda que, a través de las aplicaciones móviles y el uso que hacemos de determinados dispositivos conectados a la red expresamos, quizá de la manera más genuina posible, nuestras opiniones y deseos más íntimos.

Por su parte, Alvarado (2022) afirma que, a medida que se incrementan los casos de vulnerabilidad de los datos personales, se han emitido un sin número de jurisprudencias las cuales sirven como antecedente para el tratamiento de nuevos casos o casos similares, coadyuvando de esta manera a que se resuelvan de una manera más efectiva y en instancias iniciales, esto es posible gracias a herramientas de Big Data, las cuales permiten hacer consultas a grandes volúmenes de datos en un tiempo récord, como por ejemplo Big Query de Google.

González (2022) considera que se ha podido observar que las denuncias por el uso de datos a través de las de las llamadas podrían estar siendo almacenadas a través de la tecnología Big Data los teléfonos, y afirma que hasta el momento no se han tenido denuncias específicamente por Big Data, más que todo se ha dado casos por tratamientos particulares, mas no de un conjunto de personas afectadas. (Llamadas, publicidad, etc), no ha existido denuncias de gran dimensión.

Vera (2022) menciona que en el mundo existen más de una docena de países que son considerados con un nivel adecuado de protección de datos, en el caso de Latinoamérica los países que se han adecuado a la legislación de la Unión Europea son Uruguay y Argentina,

en el marco de lo dispuesto en el artículo 45° Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Pregunta: ¿Qué opinión tiene acerca del avance jurisprudencial que han tenido los países de Latinoamérica con relación a la protección de datos personal en el uso de tecnologías como el Big Data? ¿Qué países han tenido más evolución normativa?

Franco (2022) considera que en Latinoamérica y el Caribe tienen en conjunto una población aproximada de 670 millones de habitantes distribuidos en 46 países. Varios de ellos 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/EC. A partir de la entrada en vigor del RGPD el 25 de mayo del 2018.

Alvarado (2022) menciona que los países latinoamericanos que han tenido más avance jurisprudencial en el tema de protección de datos, gracias a la utilización de herramientas de Big Data son Chile, Colombia y México, lo cual no es una coincidencia, ya que los países citados son los referentes en Tecnología a nivel de América Latina.

Por su parte, González (2022) afirma que, en el caso de Latinoamérica los países que se han adecuado a la legislación de la Unión Europea son Uruguay y Argentina, sin perjuicio de revisar su jurisprudencia sobre el tema materia de consulta.

Vera (2022) considera que en el mundo existen más de una docena de países son considerados con un nivel adecuado de protección de datos, en el caso de Latinoamérica los países que se han adecuado a la legislación de la Unión Europea son Uruguay y Argentina, en el marco de lo dispuesto en el artículo 45° Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Pregunta: ¿Qué elementos considera usted que deben ser tomados en cuenta por el órgano jurisdiccional peruano de la jurisprudencia internacional en cuanta a la regulación de las controversias en materia de protección de datos personales en el uso de tecnologías como el Big Data?

Franco (2022) considera que los elementos que deben ser tomado y que es de gran importancia serían los datos personales como toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados Complementando dicho concepto, el Reglamento señala que constituyen datos personales, aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales De la misma forma, conceptualiza los datos sensibles como aquellos datos personales constituidos por lo datos biométricos que por sí mismo pueden identificar a un titular. Esto es, datos referidos al origen racial y étnico, a los ingresos económicos, a las opiniones o convicciones políticas, religiosas, filosóficas o morales, a la afiliación sindical y a la información relacionada con la salud y la vida sexual.

Por su parte, Alvarado (2022) considera que los elementos que deben ser tomado para la protección de datos personales por parte del órgano judicial son la inminencia, la cual exige la toma de medidas inmediatas, la urgencia que tiene el sujeto de derecho por salir de ese perjuicio inminente y la gravedad de los hechos lo cual hace impostergable el accionar de las autoridades.

González (2022) afirma que La diferencia con el tratamiento de Big Data son las medidas de seguridad, ver si estás medidas son lo suficientemente adecuadas para proteger su información y que no se vaya a filtrar porque nosotros tenemos las medidas de seguridad previstas en el reglamento del artículo 39° al 46° (Decreto Supremo Nº 003-2013-JUS) que

es básicamente un check list general, quizás para el tema del Big Data no ha abordado de manera específica o profundizado, es decir ese tipo de almacenamiento o procesamiento de la información de dimensiones gigantescas, sin embargo, el tratamiento de datos si está regulado; asimismo, cabe precisar que, la evaluación de impacto de este tipo de tratamiento de acuerdo a las plataformas que uso por dar un ejemplo, nos podrían ayudar a que los datos almacenados estén más seguros lo que no quiere decir que estén libres, ya que tienen que tener la confidencialidad de la información, trazabilidad de la información, quien tuvo acceso, que cosa hizo, no se puede filtrar pero como son medidas generales una evaluación de impacto de la plataforma que se está usando y del tipo de tecnología que se está usando, podría ayudar a que las medidas de seguridad sean más consistentes.

Por último, Vera (2022) considera que se debe tomar los ejemplos que ha brindado la jurisprudencia internacional, ya que se debe tener en cuenta que el valor de la información ya no reside solamente en su uso original o primario, sino que es compartida con los múltiples usos secundarios a la cual será sometida para encontrar correlaciones, la gran cantidad de data facilita la "re-identificación" de sujetos luego de la anonimización de la información ; no obstante, ciertos investigadores de seguridad advierten que el uso de herramientas para anonimizar datos no es cien por ciento fiable, máxime si el Big Data al tener un formato estructurado y la masiva cantidad de los datos, es posible re identificar al individuo, es por tal razón, entre otras tantas, que se tienen que encontrar soluciones aceptables a los problemas de privacidad que se generan con el desarrollo del Big Data en relación a la protección de datos personales, buscando mitigar los riesgos sin renunciar a los beneficios que esta proporcione.

3.2 Resultados de la técnica: Análisis Documental

En relación al objetivo general: "Determinar la existencia de la regulación jurídica del Big Data en la ley Nº29733 que garantice la protección de datos personales." se procede a mostrar los resultados obtenidos, ordenados de acuerdo a las dimensiones de cada variable, los cuales se procesaron en los instrumentos de recolección de datos: ficha de análisis documental.

Cubillos (2017) señala que la revolución tecnológica ha provocado cambios importantes en el funcionamiento de la economía, el empleo, la política o incluso en los hábitos sociales de la población con es el caso de las redes sociales. Otros fenómenos tecnológicos más recientes como el big data o los incipientes desarrollos de inteligencia artificial, robotización y el aprendizaje de máquinas (machine learning) se interpretan como la antesala de la cuarta revolución industrial en la que veremos probablemente vehículos autónomos, drones, la popularización de la impresión 3D, los asistentes virtuales y otros muchos productos y servicios que a día de hoy se desconocen ya sea porque se encuentran todavía en desarrollo en las plantas de ingeniería o tan solo en la mente de los ingenieros, lo que va a originar también grandes cambios en el ordenamiento jurídicos de los Estados.

Gómez et al (2017) menciona que los cambios operados en los últimos 25 años en la tecnología y la economía están produciendo cambios significativos en la concepción que se tiene acerca de la protección de datos. El modelo normativo construido para garantizar el respecto de este derecho fundamental ha sido fuertemente impactado por el Internet y las distintas expresiones que de forma global presenta la digitalización, por lo que se hace necesario cambiar el paradigma en el enfoque de la privacidad y de los derechos vinculados a ella para adaptarlo a las circunstancias actuales.

Cerna y Lescano (2012) determinaron que la respuesta desde la normativa peruana de protección de datos frente al reto que plantean estos factores de cambio, debe ser el de superar el modelo de gestión de datos para insertarse en un esquema de responsabilidad proactiva que contemporice con el fenómeno del Internet, con el Big Data, las redes sociales y, en general con todas aquellas nuevas formas de tratar datos personales para relacionarse o hacer de negocios, sin que por ello tenga que afectarse el núcleo esencial del derecho fundamental a la protección de datos como es la capacidad de control por parte del titular de la información.

Con respecto a la masificación de los datos y el uso extensivo de ellos por Internet, Martínez (2019) señala que las políticas de privacidad de los gigantes de internet no protegen los datos personales, es por ello la necesidad de fortalecer los sistemas jurídicos vigentes en torno a la protección de estos datos, a fin de ejercer un control activo sobre el tratamiento y manipulación de los mismos. El fenómeno de la internacionalización de los datos constituye un desafío fundamental para la protección, así como la posibilidad de ejercer el derecho a la supresión de datos. Pese a los avances logrados en la región en materia de regulación de datos personales, varios retos persisten y el esfuerzo legislativo debe ser mayor.

En relación a la normativa vigente en materia de protección de datos, la ley de protección de datos personales (Ley Nº 29733, 2011) presente una clara ausencia en la regulación de datos masivos y uso de tecnologías que involucren IA y Big Data, las cuales en su mayoría son controladas por agentes que se encuentran fuera del territorio nacional, al establecer en el Artículo 3:

> La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el

territorio nacional. Son objeto de especial protección los datos sensibles. (p. 3)

En cuanto a los resultados relacionados con el objetivo específico Nº1 "Analizar los mecanismos de protección de datos personales contemplados en la Ley Nª29733" se presenta lo siguiente:

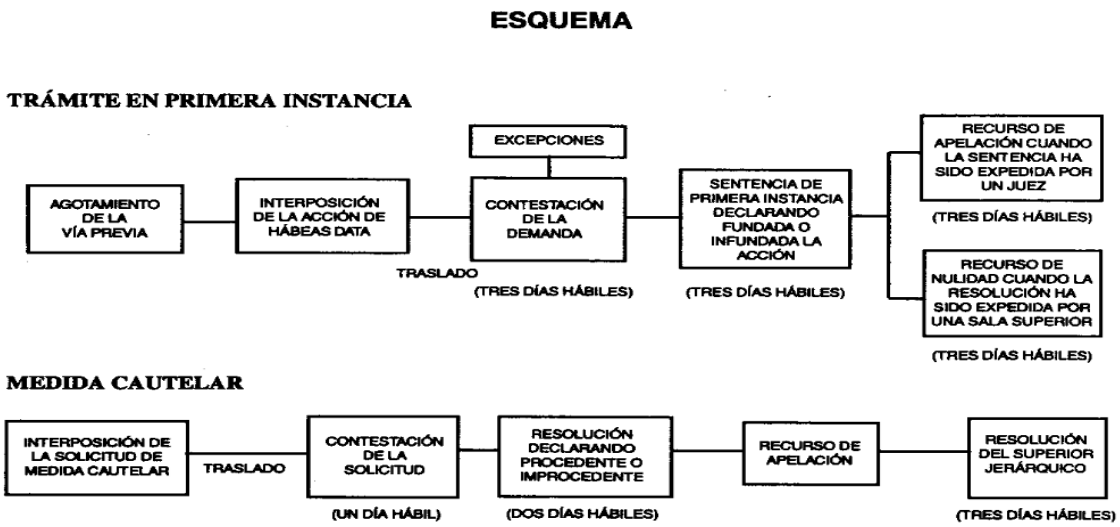
García (2017) señala que, en la actualidad, la Constitución Política reconoce el derecho fundamental a la autodeterminación informativa como una de las facultades que tienen las personas para resguardar la información ante el registro, uso y revelación de los datos que considere sensibles y que no deberían ser difundidos. A partir de ahí, el legislador ha establecido un marco legal para desarrollar este derecho a través de la Ley de Protección de Datos Personales (Ley 29733, 2011); y de su reglamento, aprobado por Decreto Supremo 003-2013-JUS.

Gil (2015) menciona que, como parte de los mecanismos judiciales que establece la normativa referente a la protección de datos personales, se encuentra el proceso de habeas data, el cual consiste en que el titular de los datos puede solicitar al Juez el derecho a conocer, actualizar, incluir, suprimir o rectificar la información referida a su persona que se encuentre almacenada o registrada en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o privadas que brinden servicios o acceso a terceros. Asimismo, puede suprimir o impedir que se suministren datos de carácter sensible que afecten su intimidad. Este proceso constitucional está reconocido en el artículo 200.3 de la Constitución Política y es desarrollado por el Código Procesal Constitucional.

Este procedimiento se presenta de acuerdo a las etapas que se describirán a continuación:

Figura 1

Procedimiento del Habeas Data



Fuente: Asesoría Legal AZ

También se puede generar, por vía administrativa, una solicitud dirigida al titular del banco de datos o al encargado del tratamiento, el titular del dato personal puede requerir el acceso, rectificación, corrección u oposición a cualquier tratamiento. Si el titular del banco o el encargado se niegan o no responden la solicitud, entonces se puede iniciar un procedimiento trilateral de tutela ante la Autoridad Nacional de Protección de Datos Personales. La resolución que emita la Autoridad agota la vía administrativa, por lo que podrá ser cuestionada judicialmente vía proceso contencioso administrativo.

Un aspecto a considerar como parte de la regulación de la protección de datos personales y que puede brindar un aporte significativo al menos de datos masivos es el flujo transfronterizo de los datos, contemplado en la Ley 29733 (2011) el cual consiste en la transferencia de datos personales hacia un destinatario que se encuentra en un país distinto del país de envío, cualquiera sea el soporte en que se encuentren, los medios utilizados para su transferencia o el tratamiento que reciban. De acuerdo con el principio de nivel de

protección adecuado, para transferir datos personales al extranjero se debe garantizar un nivel suficiente de protección para el tratamiento que se vaya a aplicar, que por lo menos sea equivalente a lo previsto en la Ley 29733 o a los estándares internacionales en la materia. Si el país destinatario no cuenta con niveles adecuados de protección, el emisor del flujo transfronterizo deberá garantizar que el tratamiento de los datos personales se efectuará con respeto de los derechos de sus titulares.

En cuanto a los resultados relacionados con el objetivo específico Nº2 "Analizar las sentencias de los tribunales nacionales e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data." se presenta lo siguiente:

Tabla 5

Jurisprudencia: sentencias de los tribunales nacionales e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data

Datos generales	Sumilla	Argumentos jurídicos relevantes
FXP N ° 04027 2013-PIID/TC LAMBAYEQUE ADALBERTO SANTOS JUÁREZ Recurso de agravio constitucional interpuesto por don Adalberto Santos Juárez contra la resolución de fojas 85, su fecha 12 de junio de 2013	Conforme se aprecia del petitorio de la demanda, lo que el actor pretende esacceder a una información que la emplazada custodiaría respecto de su vida laboral desde el mes de enero de 1948 hasta el mes de diciembre de 1992, situación que evidencia que el derecho del cual el recurrente viene haciendo ejercicio es el de autodeterminación informativa, y no el de acceso a la información pública, corno erróneamente invoca.	(...) la protección del derecho a la autodeterminación informativa a través del hábeas data comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no. cualquiera que sea su naturaleza. en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información ah como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el habeas data puede tener la finalidad de agregar datos al registro que se tenga, sea por la necesidad de que se actualicen los que se encuentran registrados, o con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados. (STC N.° 03052-2007-PHOTC, FJ 3)

EXP. N.° 05484-2015-PHD/TC

LAMBAYEQUE

ROBERTO TELLO MORI

Recurso de agravio constitucional interpuesto por don Roberto Tello Mori contra la sentencia de folios 71, de 10 de agosto de 2015

El artículo 62 del Código Procesal Constitucional dispone que para la procedencia del habeas data se requerirá que el demandante previamente haya reclamado, por documento de fecha cierta, el respeto de los derechos a que se refiere el artículo antedicho, y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del derecho reconocido por el artículo 2, inciso 5 de la Constitución o dentro de los dos días si se trata del derecho reconocido por el artículo 2, inciso 6 de la Constitución.

El habeas data es un proceso constitucional que tiene por objeto la protección de los derechos reconocidos en los incisos 5) y 6) del artículo 2 de la Constitución, los cuales establecen que "toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional", y "que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar", respectivamente.

Pues bien, conforme lo expone este Tribunal en la sentencia recaída en el Expediente 04387-2011-PHD/TC (fundamento 9): "[1]a referencia a la identidad debe entenderse, sin embargo, no de modo restrictivo, como datos que revelen sólo las señas personalísimas del titular (nombre, sexo, edad, estado civil, etc.), pues de este modo se confundiría el derecho a la protección de datos personales con el derecho a la intimidad personal o familiar, sino que su comprensión debe ser más amplia, en el sentido de incluir información que revelen aspectos de la identidad relacional, social, económica, política, religiosa, cultural, etc. de la persona (desempeño laboral, operaciones comerciales, afiliación política, etc.)".

Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica.	El Defensor del Pueblo ha interpuesto el presente recurso de inconstitucionalidad contra ciertos incisos de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica de Protección de Datos de Carácter Personal (L.O.P.D., cuya Disposición final segunda les priva de la forma de Ley Orgánica) que, a su juicio, vulneran frontalmente la reserva de ley del art. 53.1 C.E., el art. 18.1 y 4 C.E., al no respetar el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar, así como del derecho fundamental que este Tribunal ha denominado de «libertad informática» (SSTC 254/1993, de 20 de julio, 94/1998, de 4 de mayo, y 202/1999, de 8 de noviembre).	En primer término, la posibilidad prevista en la L.O.P.D. de que una norma reglamentaria pueda autorizar la cesión de datos entre Administraciones Públicas para ser empleados en el ejercicio de competencias o para materias distintas a las que motivaron su originaria recogida sin necesidad de recabar previamente el consentimiento del interesado (art. 11.1 L.O.P.D., en relación con lo dispuesto en los arts. 4.1 y 2 y 5.4 y 5), es decir, la cesión de datos inconsentida autorizada por una norma infra legal, soslaya que el art. 53.1 C.E. reserva en exclusiva a la Ley la regulación y limitación del ejercicio de un derecho fundamental, vulnerando por consiguiente el derecho fundamental mismo, al privarle de una de sus más firmes garantías. En segundo lugar, las habilitaciones a la Administración Pública estatuidas en el art. 24.1 y 2 L.O.P.D. para que ésta pueda decidir discrecionalmente cuándo denegar al interesado la información sobre la existencia de un fichero o tratamiento de datos de carácter personal, sobre la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, sobre las consecuencias de la obtención de los datos o de la negativa a suministrarlos, sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, sobre la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Sentencia del 21.7.03 (Colombia) en una acción de tutela por la violación al derecho constitucional de habeas data, autodeterminación informática y la intimidad mediante spam.	La presente acción de tutela fue remitida al Juzgado Promiscuo Municipal Reparto, por correo electrónico oficial (xxxxx@cendoj.ramajudicial.gov.co) por el accionante J.C. ** ** representado por apoderado judicial Dr., Á.R.B, poder presentado virtualmente ante el Señor Notario Diecinueve del Círculo de Bogotá (info@notaria19.com) Dr. N.S.F .quien da fe del contenido del mensaje/poder otorgado, acción que fuera repartida extraordinariamente en soporte electrónico, correspondiéndole al Juzgado Segundo Promiscuo Municipal su trámite.	Actualmente existe un nutrido conjunto de normas legales que regulan el tratamiento de datos personales y, con diversidad de enfoques y mayor o menor intensidad, el spam. Aun cuando no es posible examinar detalladamente aquí la fisonomía de las distintas regulaciones, un rápido examen de algunas proposiciones para regular el spam puede dar noticia acerca de los contornos entre los cuales se mueven los cuerpos normativos. Según Maza Gazmuri pueden considerarse cinco opciones al momento de regular el spam: (1) la opción prohibitiva, (2) el “etiquetamiento” de spam como spam, 3) la opción anti-fraude, (4) La utilización de bienes muebles sin autorización (trespass to chattels), y (5) la opción “opt. out.” (1) En su versión extrema, la opción prohibitiva consiste en proscribir todo tipo de publicidad comercial no consentida. Una versión más popular consiste en prohibir únicamente el envío de publicidad por correo electrónico

	cuando esta no haya sido solicitada –es decir el receptor haya prestado su consentimiento sobre la recepción de correos- o bien exista una relación anterior entre el emisor y el receptor. La ventaja de este enfoque es evidente, por una parte, reduce significativamente el número de correos enviados, y por otra, solo reciben correos quienes lo desean.
	Una defensa frente a la "aterritorialidad" de Internet consiste en sostener que esta puede ser corregida a través de tratados internacionales. Esto, sin embargo, supone uniformidad entre las diversas legislaciones sobre spam que, como se ha advertido, a la fecha no existe, sólo conocemos la ya referenciada española y el proyecto de ley colombiano. Junto al problema de la aterritorialidad de Internet, aún es posible registrar tres inconvenientes más al momento de utilizar la legislación para regular el envío masivo de correos no solicitados. El primero es el dinamismo de la tecnología, el segundo es la legitimación de ciertas formas de correo no deseado al prohibir otras Finalmente, el tercero, tiene que ver con la especial protección que suele recibir la libertad de expresión.

Fuente: Elaboración propia

CAPÍTULO IV: DISCUSIÓN Y CONCLUSIONES

Bernal (2016) señala que en esta sección se analizan implicancias, las limitaciones que se presentaron en el análisis de contenido, así como la obtención y recolección de los datos, se determina cómo se respondieron las preguntas formuladas en la investigación y el alcance de los objetivos propuestos, se relacionan los resultados con los antecedentes y se discuten los resultados obtenidos, entre otros.

Debido a que el tema de investigación es novedoso y muy poco abordado en el ámbito de las ciencias jurídicas, se presentaron como limitantes, la falta de documentos, antecedentes y jurisprudencia nacional en torno a la regulación de herramientas como el Big Data en relación a la protección de datos personales, además que los aportes que hay sobre el tema solo se concentrar en legislaciones europeas y muy poco avance en la región latinoamericana.

Otra limitante importante fue la dificultad de poder aplicar otros instrumentos de recolección de datos, tales como la entrevista, en virtud de la coyuntura que existe actualmente por la pandemia del COVID-19 que impide poder coordinar con especialista en la materia que se encuentran en los organismos del Estado.

De acuerdo a la identificación del problema, los resultados de campo contrastado con los antecedentes nacionales e internacionales, realidad problemática, y todo lo desarrollado en relación a la tecnología del Big Data y la protección de datos personales, se ha descrito en modo comparativos los resultados, basado en las entrevistas y análisis documental, lo cual se muestra a continuación:

En cuanto al objetivo general de la investigación: Determinar los efectos de la regulación jurídica del Big Data en la ley Nº29733 que garantice la protección de datos personales, es evidente que en, la legislación vigente en materia de protección de datos

personales presenta ciertas limitaciones en su regulación, debido a que el ámbito de aplicación de la ley Nº29733 no contempla mecanismos de protección para la manipulación de datos masivos a través de tecnologías Big Data, encontrándose una clara desventaja en cuanto a la seguridad jurídica de las personas frente a los desafíos de un mundo tecnológico globalizado, donde se encuentran expuestos una gran cantidad de datos en tecnologías donde manipulan sin ningún control jurídico y sin seguimiento por parte de los usuarios.

Los entrevistados coinciden en que, si bien el tratamiento de datos personales está regulado en la Ley de Protección de Datos Personales y su reglamento, ambas normas no profundizan o abordan de manera específica en cuanto al tratamiento masivo de datos estructurados, no estructurados y semiestructurados y es ahí donde entra a calar la tecnología del big data que se constituye como una herramienta de análisis masivo de datos. Además, consideran que la Ley N° 27933 y su reglamento regula el tratamiento de datos personales, pero no profundiza o aborda de manera específica el tratamiento masivo de datos personales a través de la tecnología big data. Asimismo, el Estado ha emitido una serie de normas donde se dispone de manera general el uso eficiente de datos masivos para promover el aprovechamiento de tecnologías emergentes, sin abordar de manera directa y profunda una regulación sobre big data.

Este planteamiento se evidencia en atención a lo contemplado en el artículo 3 de la Ley de Protección de Datos (Ley N° 29.733) el cual establece que, esta normativa es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional.

Cerna y Lescano (2012) Martínez (2019) coinciden con respecto a la ausencia de esta regulación al señalar que, la respuesta de la normativa peruana en materia de protección de

datos no está preparada para enfrentar el reto que plantean los cambios en cuanto a las tecnologías de información y comunicación actuales, es por ello que se debe promover un nuevo modelo de gestión de datos a través de una reforma legislativa para insertarse en un esquema de responsabilidad proactiva que este a la par del fenómeno del Internet, con el manejo del Big Data, las redes sociales y, en general con todas aquellas nuevas formas de manipulación de datos personales para relacionarse o realizar acto comerciales de gran envergadura, sin que por ello tenga que afectarse el núcleo esencial del derecho fundamental a la protección de datos como es la capacidad de control por parte del titular de la información.

Partiendo de estos planteamientos, Cubillos (2017) y Gómez et al (2017) coinciden que en los últimos años, el uso de tecnologías de datos masivos están produciendo cambios significativos en la denominación que se tiene acerca de la protección de datos, es por esto que las normas jurídicas diseñadas actualmente han sido fuertemente impactadas por el Internet y las distintas plataformas que manejan datos personales masivos y que, en algunos casos presentan ausencia en estas situaciones; es por ello que se plantea la necesidad de un cambio en el paradigma en cuanto al enfoque de la privacidad y de los derechos vinculados a ella para adaptarlo a las circunstancias actuales.

En cuanto a los argumentos de Valdivia (2019), Navas (2015) y Aguad (2018) coinciden en que las políticas de privacidad y protección de datos personales ofrecidas a los usuarios son unilaterales y de difícil comprensión, trayendo como consecuencia la falta de entendimiento por parte de estos usuarios del alcance que tienen los titulares de las bases de datos donde y de la manipulación que hagan estos de dicha información, aunada a la falta de protección jurídica por ausencia de regulación sobre estas tecnologías, lo que conlleva que las políticas de privacidad diseñadas por las grandes empresa de internet no protegen los

datos personales, es por ello la necesidad de fortalecer los sistemas jurídicos vigentes en torno a la protección de estos datos, a fin de ejercer un control activo por parte de los Estados sobre el tratamiento y manipulación de los mismos.

Con relación al objetivo específico Nº1 Analizar los mecanismos de protección de datos personales contemplados en la Ley Nª29733, se ha podido constatar en la normativa vigente y la opinión de algunos autores que en la Constitución Política del Perú de 1993 se reconoce el derecho fundamental a la autodeterminación informativa como una de las facultades que tienen las personas para resguardar la información ante el registro, uso y revelación de los datos que considere sensibles y que no deberían ser difundidos. A partir de este precepto constitucional se aprueba la Ley de Protección de Datos Personales (Ley 29733, 2011); y de su reglamento, aprobado por Decreto Supremo 003-2013-JUS.

Los entrevistados coinciden en que no se trata de un problema de efectividad de la norma lo que está ocurriendo en el Perú, sino que la misma no ha evolucionado con respecto a los avances tecnológicos, es por ello que depende de la Autoridad Nacional de Protección de Datos Personales la potestad de hacer directivas que se tienen planificadas y trazadas; asimismo, es necesario que tanto este organismo como el INDECOPI adapten sus reglamentos a estas situaciones, partiendo de cierta autonomía administrativa. No obstante consideran que muchas de las prácticas empresariales y actividades que se realizan están acordes a lo pautado por la norma, sin embargo esta situación ha afectado negativamente al titular de los datos personales, ya que no basta solo demostrar que existen los mecanismos necesarios sino también que se cumpla el objetivo para el cual han sido incluidos en la Ley 29733, debiendo tener espacial énfasis en la valoración del cumplimientos de los principios rectores de la precitada Ley y ello debe aplicarse a las nuevas tecnologías que no paran de evolucionar día tras día.

En cuanto a las motivaciones para regular el uso y manipulación de los datos electrónicos, Alvarado (2016) y Guevara (2018) coinciden en que el interés por la protección de datos personales es consecuencia de la pérdida de confidencialidad e integridad debido al mal uso que se ha hecho de esta información de manera automatizada, la cual ha ido aumentando progresivamente con la aparición de tecnologías donde utilizan algoritmos complejos que manipulan grandes cantidades de datos sin la debida supervisión y control por parte del usuario. Con la promulgación de normas jurídicas en varios países de la región se ha incorporado el principio de seguridad, que obliga a los titulares de las bases de datos y a los encargados de manipular la data, documentar todas las medidas de seguridad implementadas, tanto para la información digital como el almacenamiento de documentación no automatizada con el objetivo de evitar el riesgo de adulterar o alterar la información en beneficio de un tercero o la pérdida de información y cualquier tratamiento ilegal.

Por otro lado, Miyagusuku y León (2019) y Olivos (2020) difieren parcialmente del anterior planteamiento al señalar que los países de la región, a pesar del tiempo transcurrido y del avance del internet y las tecnologías de manipulación de datos, aún sigue siendo de pobre desarrollo en cuanto a mecanismo de manipulación y protección de datos masivos. En el caso del Perú, los modelos de regulación vigente fueron tomados del sistema europeo e incorporados con la entrada en vigencia en el 2016 del Reglamento General de Protección de Datos, el cual parte de la concepción de que el tratamiento de datos personales debe estar concebido para proteger a la humanidad.

Gil (2015) coincide que el interés por aplicar instrumentos de regulación jurídica de datos masivos en la región tiene su base en el desarrollo jurídico que se ha presentado en materia de protección de datos unificada en todos los Estados miembros de la Unión Europea, los cuales consideran que la tecnología del Big Data es una herramienta de mucha

importancia para el desarrollo comercial de los países, ofreciendo información necesaria para el consumidor con el objetivo de poder ofrecer mejores condiciones comerciales. Aunque el autor sostiene que este planteamiento debe ser analizado con mucho cuidado, ya que pone en tela de juicio hasta qué punto estas tecnologías traspasan el límite de la voluntad de las partes en el seguimiento y monitorización de su información, exponiendo los datos más personales y desdibujando la diferencia entre vida privada, pública e intimidad.

Esta influencia europea ha permitido implementar algunos mecanismos efectivos para la protección de datos personales, los cuales coinciden con los establecidos por la Ley Nº 29733, entre ellos tenemos el proceso de habeas data, el cual consiste en que el titular de los datos puede solicitar al Juez el derecho a conocer, actualizar, incluir, suprimir o rectificar la información referida a su persona que se encuentre almacenada o registrada en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o privadas que brinden servicios o acceso a terceros. Asimismo, puede suprimir o impedir que se suministren datos de carácter sensible que afecten su intimidad. Aunque Olivos (2020) difiere de este recurso, ya que el mismo solo es aplicable ciñéndose al ámbito de aplicación de este instrumento jurídico contenido en el artículo 3, sin extender su aplicación para el resguardo de datos masivos manipulados por tecnologías del Big Data.

Con relación al objetivo específico Nº2 "Analizar las sentencias de los tribunales nacionales e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data" se observa en base a los documentos recogidos que, en la mayoría de los países de la región coinciden en que deben existir mecanismos de protección de datos masivos al utilizar tecnologías del Big Data y otras de igual naturaleza, en base al principio de la autodeterminación informativa, donde el usuario es el único que autoriza la utilización

de sus datos por cualquier propósito y debe poseer herramientas para hacer seguimiento a dicha información privada.

En el caso de los entrevistados consideran que no existe muchas causas a nivel nacional en cuanto a controversias por el uso de tecnologías como el Big Data y su influencia en la protección de datos personales, sin embargo afirman que deben tomarse en cuenta ciertos elementos de gran importancia tales como que toda información sobre una persona natural que la identifica o la hace identificable a través de medios debe ser razonablemente utilizados por aquellos servicios que manipulan datos masivos; señala además que el reglamento afirma que los datos personales es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales, por ende deben tomarse todos estos tipos de datos sensibles para la ciudadanía. De la misma forma, conceptualiza los datos sensibles como aquellos datos personales constituidos por lo datos biométricos que por sí mismo pueden identificar a un titular. Esto es, datos referidos al origen racial y étnico, a los ingresos económicos, a las opiniones o convicciones políticas, religiosas, filosóficas o morales, a la afiliación sindical y a la información relacionada con la salud y la vida sexual.

Es por ello que, en el Perú, al igual que en España se acogen a estos lineamientos, lo cual se ve reflejado en las sentencias Nº 04027 2013 y Nº 292/2000 donde establecen que, la protección del derecho a la autodeterminación informativa se puede materializar a través del recurso de hábeas data, el cual comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no y cualquiera que sea su naturaleza en los que se encuentren almacenados los datos de una persona. Este mecanismo tiene por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información y a las

personas que recabaron dicha información. En segundo lugar, el habeas data puede tener la finalidad de agregar datos al registro que se tenga, sea por la necesidad de que se actualicen o se decida eliminarlos.

Esto coincide y es reafirmado por otra sentencia del Tribunal Constitucional del Perú Nº 05484-2015 la cual establece que, el habeas data es un proceso constitucional que tiene por objeto la protección de los derechos reconocidos en los incisos 5) y 6) del artículo 2 de la Constitución en cuanto al derecho de intimidad y valoración de los datos personales, los cuales establecen que toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido; pero este recurso presente en la normativa peruana contiene una excepción que impide que se extienda a la manipulación de datos de otras fuentes y tecnologías, tales como el Big Data, ya que se excluyen las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional, y que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar, respectivamente, limitándose taxativamente al ámbito nacional sin tomar en cuenta las operaciones fuera del territorio.

Con respecto a Colombia, en sentencia de fecha 21 de Julio de 2003 extiende la protección del recurso de habeas data, al considerar que la noción de identidad en los datos debe ampliarse a una serie de información vinculante e importante para el usuario y debe entenderse, sin embargo, no de modo restrictivo, como datos que revelen sólo la información básica del titular (nombre, sexo, edad, estado civil, etc.), pues de este modo se confundiría el derecho a la protección de datos personales con el derecho a la intimidad personal o familiar, sino que su comprensión debe ser más amplia, en el sentido de incluir información

que revelen aspectos de la identidad relacional, social, económica, política, religiosa, cultural, etc. de la persona (desempeño laboral, operaciones comerciales, afiliación política, etc.) y que pueden estar contenido no solo en base de datos locales sino en aquellos que se encuentra en bases de datos masivas y que sean manipuladas por tecnologías tales como el Big Data, el Spam, etc.

Respecto a las implicancias, se tiene desde el punto de vista teórico, que la investigación ha logrado desarrollar una temática que hasta ahora era desconocida en la regulación de datos personales masivos y su manipulación por parte de tecnologías como el Big Data que han contribuido a crear una problemática existente en cuando al alcance que tienen dichas tecnologías en razón de los derechos que tienen los usuarios en el usos de sus datos personales, siendo importante acotar la definición de Guevara (2018) con respecto al Big Data al mencionar que son el conjunto de tecnologías que permiten procesar cantidades masivas de información y datos personales a través del uso de algoritmos, con el propósito de darles utilidad en plataformas digitales y para la publicidad en línea. Así mismo, los resultados obtenidos sirven de insumo para otras investigaciones al aportar la información pertinente acerca de la situación a nivel nacional e internacional acerca de la regulación de los datos masivos utilizados por tecnologías como el Big Data.

En referencia a la implicancia metodológica, se puede indicar que el diseño realizado para la ficha de análisis documental se realizó con el fin de sintetizar los aportes de la doctrina y que permitiera contrastarlo con mayor facilidad con la jurisprudencia recabada, lo cual servirá de fuente de información para su uso o adaptación en futuras investigaciones con temáticas de investigación similares al estudio llevado a cabo.

En cuanto a la implicancia práctica, esta investigación ha mostrado la necesidad de recabar información sobre la protección de datos personales, como derecho consagrado en

la Constitución Política del Perú y las leyes vigentes sobre la materia, con el fin de demostrar la precariedad que tiene el sistema jurídico en cuanto a la regulación de tecnologías como el Big Data para la protección de los derechos y garantías de los ciudadanos que se ven expuesto al avance tecnológico mundial; por lo tanto, el análisis realizado, tanto teórico como practico en esta investigación permitirá a los funcionarios especializados abordar esta temática, además que servirá como punto de partida para una futura reforma legislativa.

De acuerdo a los resultados obtenidos y aplicando la metodología estipulada, se ha logrado dar respuesta a los objetivos establecidos en la presente investigación y se ha determinado en base al análisis documental y la revisión de los antecedentes expuestos en la misma, a continuación:

- No se cumple con el objetivo general "Determinar los efectos de la regulación jurídica del Big Data en la ley Nº29733 que garantice la protección de datos personales" ya que se pudo constatar a través de la doctrina nacional, el análisis jurisprudencial y los dispositivos contemplados en la ley vigente en materia de protección de datos personales no contempla mecanismos de protección en cuanto al uso y manipulación de datos masivos a través de tecnologías Big Data, poniendo en gran riesgo en cuanto a la seguridad jurídica a las personas que tienen datos personales y profesionales en plataformas de información que se encuentra en el Internet o redes empresariales masivas, las cuales se encuentran grandes cantidades de datos en tecnologías donde se manipulan sin ningún control jurídico y sin seguimiento por parte de los usuarios; por consiguiente la legislación actual no está preparada para regular los cambios que se presentan en las tecnologías de información y comunicación actuales, evidenciando la necesidad de promover un modelo de gestión de datos a través de una reforma legislativa que permita crear un

esquema de responsabilidad proactiva que este a la par del fenómeno del Internet, con el manejo del Big Data y otras redes que manejen datos masivos susceptibles de ser alterados.

- Se cumple con el objetivo específico N°1 "Analizar los mecanismos de protección de datos personales contemplados en la Ley Nª29733" ya que partiendo de los preceptos legales contemplado en la ley vigente, conjuntamente con la opinión de algunos doctrinarios y el análisis jurisprudencial se evidencia que los mecanismos establecidos en la norma tienen su basamento en lo contemplado por la Constitución Política del Perú, la cual reconoce el derecho a la autodeterminación informativa que permite a las personas, resguardar la información ante el registro, uso y revelación de los datos que consideren sensibles y que no deberían ser difundidos; es por ello que en la norma vigente se encuentra el principio de seguridad, que obliga a los titulares de las bases de datos que manipulan la información de las personas, documentar todas las medidas de seguridad implementadas, tanto para la información digital como en el almacenamiento de documentación no automatizada con el fin de evitar la alteración de la información en beneficio de un tercero o la pérdida de información y cualquier tratamiento ilegal, además que existe el recurso de *habeas data*, el cual consiste en que el titular de los datos puede solicitar al Juez el derecho a conocer, actualizar, incluir, suprimir o rectificar la información referida a su persona que se encuentre almacenada o registrada en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o privadas que brinden servicios o acceso a terceros.
- Se cumple parcialmente con el objetivo específico N°2 "Analizar las sentencias de los tribunales nacionales e internacionales donde regulen la protección de datos personales en el uso de tecnologías Big Data" ya que partiendo del análisis realizado

a un conjunto de sentencias provenientes de los tribunales, tanto nacionales como internacionales, se evidencia que en el caso del Perú no existe precedente jurisprudencial donde se aplique alguno de los mecanismo de protección de datos contemplado en la norma vigente, referente al uso de tecnologías Big Data y de la manipulación de datos masivos, lo cual solo se limita al ejercicio del recurso de habeas data, el mismo que contiene una excepción que impide que se extienda a la manipulación de datos de otras fuentes y tecnologías, tales como el Big Data, al excluir los datos que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional, y que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar, respectivamente, limitándose taxativamente al ámbito nacional sin tomar en cuenta las operaciones fuera del territorio. En el caso de las decisiones en otros países como es el caso de Colombia, no interpretan la acción del habeas data como algo restrictivo a nivel local o nacional ya que consideran que la noción de identidad en los datos debe ampliarse para el usuario y debe entenderse, sin embargo, no de modo restrictivo, sino extendiéndose a cualquier base de datos que revelen información vinculante para el titular, tales como datos económicos, políticos, religiosos, culturales, etc. de la persona y que pueden estar contenido no solo en base de datos locales sino en aquellos que se encuentra en bases de datos masivas y que sean manipuladas por tecnologías tales como el Big Data, el Spam, etc.

REFERENCIAS BIBLIOGRAFICAS

Aguad, L. M. (2018). El Internet, el Big Data y el tratamiento de datos personales. Advocatus, (036), 205-223.

Alvarado, F. J. (2016). La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales. *Foro Jurídico*, (15), 26-41.

Álvarez, J. M. (1999). La defensa de la intimidad de los ciudadanos y la tecnología informática. Editorial Aranzadi.

Arias, F. (2016). El Proyecto de Investigación. Introducción a la Metodología. 7a. Ed. Caracas: Editorial Episteme

Atehortúa, F & Zwerg, A (2012). Metodología de la investigación: más que una receta/Research Methodology: More than a recipe. *Ad-minister*, (20), 91.

Bernal, A. (2016). Metodología de la Investigación (Cuarta edición ed.). *México: Pearson Educación. Retrieved*, *6*(18), 2016.

Canales, M (2006). Metodologías de la investigación social. Santiago: LOM Ediciones; 2006. p. 163-165.

Carrasco, S. (2006). Metodología de la Investigación Científica. Editorial San Marcos. Lima.

Dulzaides, M., & Molina, A. (2004). Análisis documental y de información: dos componentes de un mismo proceso. *ACIMED*, *12*(2). Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200011

ESPAE. (2017). *ESPAE.ESPOL*. Retrieved from http://www.espae.espol.edu.ec/wp-content/uploads/2016/12/industriasoftware.pdf

Gayo, M (2017). Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, (17), 3.

García, L (2017). Muestreo probabilístico y no probabilístico. Teoría. Recuperado de https://www.gestiopolis.com/muestreo-probabilistico-no-probabilistico-teoria/

González, J. C., Ruiz, E., & Pollo, M. F. (2016). Buenas prácticas para la protección de datos personales en ambientes de big data. In II Simposio Argentino de grades datos (AGRANDA 2016)-JAIIO 45 (3 de Febrero 2016).

Guevara, M (2018). El impacto del Big Data en la protección de datos personales. (Tesis de Pregrado) Repositori Universitat Jaume I. Madrid, España

Herrán, A. (1998) La violación de la intimidad en la protección de datos personales. Editorial Dykinson.

Hernández, C (2019). Estudio de la seguridad en big data, privacidad y protección de datos mediante la ISO/IEC 27007: 2017-aplicado a los datos académicos de la Universidad Técnica del Norte (Tesis de Pregrado). Universidad Técnica del Norte, Ibarra, Ecuador.

Hernández, J. (2013). El derecho a la protección de Datos Personales en la Doctrina del Tribunal Constitucional, Editorial Thomson Reuters Aranzadi.

Hernández R, Fernández C, Baptista P. (2014). Metodología de la Investigación. 6ta Edición. Editorial Mc GrawHill. México.

ISACA (2009) Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento, Editorial Isaca.

Martínez, R. (2017). Big data, investigación en salud y protección de datos personales. ¿Un falso debate? Revista Valenciana d'Estudis Autonòmics, 2017, num. 62, p. 235-280.

Miyagusuku, J. T., & León, A. R. (2019). Algoritmos laborales: big data e inteligencia artificial. THĒMIS-Revista de Derecho, (75), 255-266.

Navas, S. (2015). Computación en la nube: Big Data y protección de datos personales (Cloud Computing: Big Data and Personal Data Protection). *InDret*,

Olivos, M. (2020). El derecho a la protección de datos personales en el Perú: 27 años desde su incorporación en la constitución política de 1993. *IUS*: Revista de investigación de la Facultad de Derecho, 9(1), 83-100.

Schmarzo, B (2013) "Big Data: Understanding How Data Powers Big Business*".* Indianapolis: John Wiley & Sons Inc, 2013, p. 19.

Relat, J (2010). Introducción a la investigación Básica. *Revista andaluza de patología digestiva*, 2010, vol. 33, no 3, p. 221-227.

Tabesh, P., Mousavidin, E., & Hasani, S. (2019). Implementing big data strategies: A managerial perspective. Business Horizons, 62(3), 347–358. https://doi.org/10.1016/j.bushor.2019.02.001

Valdivia, D. Z. (2019). La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información. In La proyección del Derecho Administrativo peruano: estudios por el Centenario de la Facultad de Derecho de la PUCP (pp. 165-208). Palestra Editores.

ANEXOS

Anexo 1

Matriz de categorización

CATEGORIAS	DEFINICION CONCEPTUAL	SUBCATEGORIAS	INSTRUMENTOS
Big Data	Es el conjunto de tecnologías que permiten procesar cantidades masivas de información y datos personales a través del uso de algoritmos, con el propósito de darles utilidad en plataformas digitales y para la publicidad en línea (Guevara, 2018).	Tipos de datos Ciclo de análisis Inconvenientes	Análisis documental
Protección de datos personales	Toda persona física está facultada para controlar los datos almacenados de carácter personal que estén ubicados en cualquier base de datos, así como dar su autorización para ser manipulados por terceros. (Carta de los Derechos Fundamentales de la UE, 2001)	Principios reguladores Recursos admitidos Órgano Competente	Entrevistas Análisis documental

Fuente: Elaboración propia, 2020

Anexo 2

Matriz de Consistencia

PROBLEMA	OBJETIVOS	CATEGORIAS	METODOLOGIA	POBLACION
Problema General	**Objetivo General**			
¿De qué manera la regulación jurídica del Big Data en la ley Nº29733 garantizara la protección de datos personales?	Determinar la existencia de la regulación jurídica del Big Data en la ley Nº29733 que garantizara la protección de datos personales.	Categoría 1: Big Data Categoría 2: Protección de datos personales	Tipo de Investigación: Enfoque: Cualitativo Nivel: Correlacional Propósito: Básica Diseño de Investigación: No experimental – Transversal Técnica: Análisis Documental y la Entrevista Instrumentos: Ficha de análisis documental y guion de entrevista	**Población:** Artículos Científicos Trabajos de Investigación Sentencias Abogados especialistas **Muestra:** Artículos científicos (5) Trabajos de Investigación (5) Sentencias (4) Abogados especialistas (2) Expertos en protección de datos (2)
Problemas Específicos	**Objetivos Específicos**			
¿Cuáles son los mecanismos de protección de datos personales contemplados en la Ley Nª29733? ¿Existen mecanismos implícitos de regulación del Big Data en la ley Nº 29733 para la protección de datos personales? ¿Existen sentencias de los tribunales donde regulen la protección de datos personales en el uso de tecnologías Big Data según la Ley Nº 29733?	O.E1 Analizar los mecanismos de protección de datos personales contemplados en la Ley Nª29733. O.E2 Identificar los mecanismos implícitos de regulación del Big Data en la ley Nº 29733 para la protección de datos personales. O.E3 Interpretar las sentencias de los tribunales donde regulen la protección de datos personales en el uso de tecnologías Big Data según la Ley Nº 29733.			

Fuente: Elaboración Propia