PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Replanteando el consentimiento: Mecanismos de protección de los datos personales en el contexto del Big Data y las nuevas tecnologías en el marco legal peruano

Tesis para obtener el título profesional de Abogada que presenta:

Phyerina Tania Ramos Contreras

Asesora:

Noemí Cecilia Ancí Paredes

Lima, 2025

Informe de Similitud

Yo, **Noemí Cecilia Ancí Paredes,** docente de la **Facultad de Derecho** de la Pontificia Universidad Católica del Perú, asesora de la tesis titulada:

Replanteando el consentimiento: Mecanismos de protección de los datos personales en el contexto del Big Data y las nuevas tecnologías en el marco legal peruano

De la autora:

Phyerina Tania Ramos Contreras

Dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 26%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el **10/09/2025**.
- He revisado con detalle dicho reporte y confirmo que cada una de las coincidencias detectadas no constituyen plagio alguno.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 10 de setiembre del 2025.

<table>
<tr><td colspan="2">Apellidos y nombres del asesor / de la asesora:
ANCI PAREDES, NOEMI CECILIA</td></tr>
<tr><td>DNI: 45618074</td><td rowspan="2">Firma:
  </td></tr>
<tr><td>ORCID:
https://orcid.org/0000-0002-0607-716X</td></tr>
</table>

A mis padres, Fredy y Judith, por los incontables sacrificios que hicieron para permitirme soñar.

A mis hermanos, Adriana y Aarón, por ser la alegría y compañía de mi vida.

A mis abuelos, por alentarme a volar cada vez más alto.

Y a la Virgen de la Candelaria por iluminar y protegerme en cada etapa.

Resumen

El derecho a la protección de datos personales, o derecho a la autodeterminación informativa, fue consagrado en la Constitución peruana de 1993, aunque su desarrollo y regulación no se concretó, hasta casi dos décadas después, con la promulgación de la Ley No. 29733, Ley de Protección de Datos Personales, y su respectivo Reglamento. Estas normativas establecen el principio de consentimiento como regla general para el tratamiento de datos personales.

Sin embargo, nos encontramos en una nueva era, con donde la información se convierte en el pilar del poder. Como en ningún otro momento de la historia, la producción de información ha experimentado un crecimiento exponencial, ello se debe fundamentalmente al desarrollo de nuevas tecnologías y a la irrupción del internet. A este nuevo paradigma de organización de la sociedad se lo denominó como “Sociedad de la información”. En este nuevo contexto, las tecnologías de Big Data cobraron importancia al convertirse en uno de los modelos de procesamiento de información mas importantes. En ese sentido, la presente investigación tiene por objetivo principal es determinar si el principio del consentimiento garantiza una adecuada tutela del derecho fundamental a la protección de datos personales en el marco de la sociedad de la información contemporánea, en especifico, ante los sistemas de procesamiento que utilizan la tecnología del Big Data. Asimismo, se busca establecer la existencia de una incompatibilidad entre la protección establecida en la normativa relativa a la protección de datos personales y las tecnologías de procesamiento de datos basadas en el Big Data. Por último, se propone determinar la existencia de otras medidas eficientes de protección, además del consentimiento, para la recolección y tratamiento de nuestros datos personales.

Palabras clave: Derecho a la autodeterminación informativa, Protección de datos personales, Principio de consentimiento, Sociedad de la información, Big Data

Abstract

The right of informational self-determination was enshrined in the Peruvian Constitution of 1993, although its development and regulation did not materialize until almost two decades later, with the promulgation of Law No. 29733, the Personal Data Protection Law, and its respective Regulation. These legislations establish the principle of consent as a general rule for processing personal data.

However, we find ourselves in a new era, where information has become the pillar of power. Like at no other time in history, the production of information has experienced exponential growth, mainly due to the development of new technologies and the emergence of the Internet. This new paradigm of organization of society was called the “Information Society”. In this new context, Big Data technologies have gained importance by becoming one of the most important information processing models. In this sense, the main objective of this research is to determine whether the principle of consent guarantees adequate protection of the fundamental right to the protection of personal data within the framework of the contemporary information society, specifically, in the face of processing systems that use Big Data technology. It also seeks to establish the existence of an incompatibility between the protection established in the regulations relating to the protection of personal data and processing technologies based on Big Data. Finally, it is proposed to determine the existence of other efficient protection measures, in addition to consent, for processing personal data.

Keywords: Right to informational self-determination, Protection of personal data, Principle of consent, Information society, Big Data

Índice

Replanteando el consentimiento: Mecanismos de protección de los datos personales en el contexto del Big Data y las nuevas tecnologías en el marco legal peruano

1. Introducción

El consentimiento ha sido tradicionalmente considerado como la piedra angular para la protección de datos personales en el Perú. A través de este mecanismo, se justifica la recolección, tratamiento y procesamiento de datos personales. Sin embargo, este enfoque, que en su momento parecía adecuado, ha quedado obsoleto ante los vertiginosos cambios que la sociedad contemporánea está experimentando. En efecto, ello es así pues nos encontramos en plena transición hacia una sociedad de la información.

Lo cierto es que una gran mayoría de personas actualmente enfrenta desafíos inéditos en su intento por proteger sus datos personales. Esta nueva realidad, caracterizada por el desarrollo frenético de la tecnología, trae consigo nuevas formas de recolectar, procesar y tratar nuestra información. Una de estas manifestaciones es la popularización del uso del denominado Big Data, herramienta utilizada para la recolección masiva de datos personales. Con ello, se ha transformado la forma en que las empresas y organizaciones operan y toman decisiones. Sin embargo, esta revolución tecnológica no viene exenta de riesgos. La protección de datos personales se ha convertido en una preocupación creciente, y la normativa actual parece insuficiente para abordar los desafíos que presenta este nuevo escenario. No basta con reforzar las medidas existentes; es imperativo cambiar el enfoque de la normativa. Por ello, esta investigación propone una revisión profunda del concepto de consentimiento, tradicionalmente considerado como el fundamento de la protección de datos y sugiere que el mismo debería desempeñar un papel secundario o complementario, ello en el contexto de sociedad de información que vivimos.

En lugar de poner el peso de la responsabilidad en el individuo, que muchas veces no está plenamente consciente de la magnitud e importancia de sus datos, proponemos trasladar esa responsabilidad hacia quienes recolectan y tratan esos datos; es decir, las empresas y otras organizaciones. Es esencial establecer nuevas responsabilidades y obligaciones que reflejen las realidades de la era digital.

Ahora bien, ¿por qué es crucial abordar este tema ahora? Los cambios tecnológicos y sociales se suceden a un ritmo sin precedentes. Grandes corporaciones, tanto en el Perú como en el resto del mundo, están adoptando modelos de Big Data cada vez más sofisticados, aprovechando las ventajas competitivas que estos ofrecen. Sin embargo, las legislaciones y normativas relacionadas con la protección de datos no han evolucionado al mismo ritmo; muchos países, entre ellos el Perú, no han actualizado la normativa de protección de datos personales. Si bien es esencial que podamos continuar beneficiándonos de las innovaciones tecnológicas, lo cierto es que esto no debe hacerse sacrificando nuestros derechos fundamentales. La protección basada únicamente en el consentimiento se ha revelado, en muchos casos, como un mito. En la práctica, muchas veces se encuentra desvinculada de nuestra realidad cotidiana, reduciéndose a simples formalidades que los usuarios aceptan sin leer o comprender plenamente.

La protección de datos personales ha emergido como uno de los temas más relevantes en el panorama global, especialmente en las últimas décadas. Esta creciente preocupación se debe, en gran medida, a la acelerada digitalización de la información y a la globalización de las comunicaciones. La revolución tecnológica ha transformado la forma en que interactuamos, comunicamos y hacemos negocios, y con ello, ha surgido la imperante necesidad de salvaguardar nuestra información personal. Como bien señala Santos Divino, la disciplina de protección de datos personales se ha convertido en un reflejo de los desafíos actuales, que están intrínsecamente ligados a cambios tecnológicos, sociales y económicos (Santos Divino, 2019).

En el contexto peruano, al igual que en muchas otras jurisdicciones, el consentimiento ha sido el pilar fundamental en la protección de datos personales. Sin embargo, la constante evolución tecnológica y los cambios en la dinámica social nos instan a reconsiderar este enfoque. El derecho a la protección de datos personales, o derecho a la autodeterminación informativa, fue consagrado en la Constitución peruana de 1993, aunque su verdadero desarrollo y regulación no se concretó, hasta casi dos décadas después, con la promulgación de la Ley 29733, Ley de Protección de Datos Personales y su respectivo Reglamento.

Estas normativas establecen el principio de consentimiento como regla general para el tratamiento de datos personales, tal como se refleja en los artículos 5 y 13.5 de la LPDP y en los artículos 7 y 11 de su reglamento. Mubarak, en su análisis, enfatiza la importancia del consentimiento al afirmar que este concepto es esencial en la protección de datos, ya que otorga al individuo el poder de decidir sobre el uso de su información personal por parte de terceros (Mubarak Aguad, 2017). El enfoque actual del modelo se fundamenta en que la entidad que recopila información de las personas informa a dichas personas sobre qué tipo de datos recogerá y con qué propósito los utilizará. De esta manera, la persona otorga su consentimiento, lo cual ha llegado a ser el pilar fundamental de los sistemas de protección de datos (Gil, 2016).

Sin embargo, nos encontramos en una nueva era, con donde la información se convierte en el pilar del poder y acceso a él (Castells, 2006a; Santos Divino, 2019). Como en ningún otro momento de la historia, la producción de información ha experimentado un crecimiento exponencial, ello se debe fundamentalmente al desarrollo de nuevas tecnologías y a la irrupción del internet. En efecto, tal como menciona Gonzales, actualmente, las personas generan una gran magnitud de datos en tiempo real que se almacenan y analizan mediante la interacción mediada por tecnologías digitales (González, 2019).

Ante ello, hemos sido testigos de la aparición de nuevos modelos de negocio que tienen como materia prima los datos, tales como el modelo Real Time Bidding, el cual se basa en la subasta en tiempo real de perfiles de consumo generados a partir de cookies y la información recopilada por corredores de datos cuando un usuario visita una página con espacios publicitarios (Gonzalez, 2018). Por otra parte, diversos gobiernos también se han beneficiado de la producción masiva de datos actual. En Estados Unidos, por ejemplo, se ha implementado el sistema Carnivore, una herramienta del FBI diseñada para interceptar comunicaciones individuales en tiempo real durante las operaciones virtuales en la red (Santos Divino, 2019).

Ahora bien, para la recopilación y tratamiento de estos datos se requiere de nuevas herramientas tecnológicas tales como las tecnologías de rastreo —siendo el principal exponente las cookies—, el data mining, el cloud computing, entre otras. Entre todas estas tecnologías emergentes, el Big Data destaca como la más popular, siendo más que una simple herramienta, representa un enfoque de trabajo centrado en extraer valor y beneficios del vasto volumen de datos generados diariamente (Gil, 2016, pp. 17). Este fenómeno ha introducido retos inéditos en la protección de datos. En efecto, el problema se presenta cuando tomamos en consideración que (i) “el análisis de datos masivos incluye datos personales” (Recio Gayo, 2017) y (ii) las leyes y regulaciones actuales se diseñaron pensando en el manejo de volúmenes de datos más limitados (Recio Gayo, 2017).

Así, uno de estos retos que se plantea es el del respeto al consentimiento, el cual, como ya hemos señalado es parte fundamental de la regulación actual sobre protección de datos personales. Si bien varias de las plataformas actuales que hacen uso de estas técnicas se han ido acomodando a las regulaciones existentes, cuestiones como el cómo el consentimiento queda en “zonas grises” (González, 2019). Esto se debe principalmente a que el núcleo de estas nuevas tecnologías es incompatible con los sistemas basados en el consentimiento informado. En efecto, planteamientos como el Big Data se benefician de los enormes flujos de datos caracterizados por ser (i) variados, (ii) de gran volumen y (iii) creados en tiempo real

(Kitchin & McArdle, 2016). Asimismo, el planteamiento de trabajo se nutre de algoritmos con la capacidad de inferir nueva información basada en los datos originarios y reutilizarlos para otros fines. Tal como menciona Murabak, “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” (Mubarak Aguad, 2017).

La realidad es que, a pesar de los avances tecnológicos y las transformaciones en la sociedad, la legislación peruana en materia de protección de datos no ha logrado adaptarse adecuadamente. Existe un evidente desfase entre las prácticas contemporáneas de tratamiento de datos y lo que la normativa establece. De la lectura de la Ley de Protección de Datos Personales y su Reglamento, como ya hemos señalado según su artículo 5 todo tratamiento de datos personales requerirá el consentimiento de su titular; aunado a ello, el artículo 13.5 señala que dicho consentimiento deberá ser previo, informado, expreso e inequívoco. Sin embargo, este planteamiento es insostenible debido a la irrupción de las nuevas tecnologías. Por ejemplo, ya hemos mencionado que el núcleo del Big Data, los algoritmos inherentes a él que permiten inferir información y reutilizar la información recopilada.

Lamentablemente, es este avance tecnológico lo que imposibilita el cumplimiento de la regulación, en particular el consentimiento informado. La naturaleza compleja y a menudo poco transparente de estos algoritmos dificulta que el titular de los datos entienda con claridad el procesamiento y uso de su información. Además, el Big Data tiene la capacidad de combinar y analizar conjuntos de datos de diversas fuentes, lo que puede resultar en inferencias y conclusiones que el titular nunca anticipó ni consintió. Esta capacidad de generar información no prevista a partir de datos ya recopilados desafía la noción tradicional de consentimiento basado en un propósito específico.

Es así como la presente investigación pretende evaluar la pertinencia de la protección de datos personales basada en el consentimiento en el contexto actual.

Asimismo, se busca establecer la existencia de una incompatibilidad entre la protección establecida en la normativa relativa a la protección de datos personales y las tecnologías de procesamiento de datos basadas en el Big Data. Por último, se propone determinar la existencia de otras medidas eficientes de protección, además del consentimiento, para la recolección y tratamiento de nuestros datos personales.

2. CAPÍTULO 1: El derecho a la protección de datos personales en la sociedad de información

2.1. La nueva sociedad de la información

Según Tim Urban, si pusiéramos la historia de la humanidad entera en un libro de 1000 páginas, el progreso de la sociedad estaría dividido en dos partes. En las primeras 999, dicho progreso estaría marcado por largos periodos de cambios graduales y lentos, en las cuales (i) la forma de comunicación estaría basada en cartas escritas y en la oralidad, (ii) la forma de almacenar la información se reduciría al papel y (iii) la existencia de la globalización era impensable. Sin embargo, en la página 1000, es decir en la última y única página, la cual representa el cambio de los últimos 250 años de historia, refleja el acelerado cambio producto de las nuevas tecnologías, en donde (i) los medios de comunicación estarían basados principalmente en la telefonía, videollamadas y mediante el internet, (ii) la forma de almacenar la información estaría basada en tecnologías de disco duros y en el Big Data y (iii) la globalización sería una realidad marcada desde la creación y popularización del internet.

Uno de los catalizadores de dichos cambios fue la evolución de los procesos de comunicación. En el año 1969, el mundo vio la creación de una de las primeras redes de computadoras con el proyecto ARPANET, la cual permitió que la comunidad militar y estadounidense tuviera la capacidad de compartir archivos en tiempo real (Flores Torres, 2020). La irrupción del internet marcó un antes y un después en la forma en la que la sociedad se comunicaba. Como menciona

Cervera, el internet introdujo tres conceptos nuevos a la comunicación: (i) interactividad, (ii) personalización y (iii) globalización (Cervera Fantoni, 2008).

En este contexto, se gesta un nuevo paradigma de organización de la sociedad, el cual el sociólogo Manuel Castells denominó como “sociedad informacional”, popularizado también como “Sociedad de la información”. Entre 1960 y 1970, se empieza a formular teóricamente este concepto (Alfonso Sánchez, 2016). Según Castells, este modelo de sociedad se caracterizaba por un cambio en las estructuras industriales y en las relaciones sociales, debido a las tecnologías de información (Castells, 2006b). En este nuevo paradigma social, el combustible de la sociedad está basado en la producción de la información (Alfonso Sánchez, 2016).

Si bien es cierto que la información y el conocimiento fueron fundamentales para la sociedad en todos sus momentos históricos, Castells destaca que, a diferencia de otras eras, “el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de la productividad y el poder, debido a las nuevas condiciones tecnológicas que surgen en este periodo histórico” (Castells, 2006a). La formulación hecha por Castells se corresponde a las características que señala Moore sobre la Sociedad de la Información: (i) la utilización de la información como recurso económico, (ii) la popularización del uso de la información entre todas las personas, y (iii) el desarrollo del sector tecnológico de la información (Moore, 1997).

Esta nueva sociedad trajo consigo un nuevo fenómeno: la creación y circulación masiva de información. Como menciona Monleón-Getino, “el 90% de los datos del mundo han sido creados en los últimos dos años” (Monleon-Getino, 2015). Asimismo, según Gil, para entender este fenómeno es necesario entender que, hasta el año 2003, la humanidad había generado 5 exabytes de datos; no obstante, esa misma cantidad se genera actualmente cada dos días (Gil, 2016). Es importante tener en cuenta que este fenómeno es uno en constante crecimiento, pues la forma

de creación y circulación de la información no se restringe a las personas, sino que en el océano digital también se registran datos entre máquinas (Monleon-Getino, 2015).

Un aspecto a tener en cuenta es que con el “volumen masivo, variedad y velocidad que ahora toma la información hace imprescindible capturar, almacenar y analizar todo este complejo engranaje” (Puyol, 2015). Como ya mencionamos, la información se convirtió en uno de los activos más importantes en la sociedad actual, lo cual permitió la creación de industrias basadas en la explotación del mismo. Además de crear oportunidades en nuevos sectores industriales, “el buen uso de los datos puede traer oportunidades a sectores más tradicionales, como el transporte, la salud o de fabricación” (Monleon-Getino, 2015).

Teniendo en cuenta ello, surge una nueva tecnología como respuesta al problema del exceso de producción de datos: el Big Data. En efecto, como Cárdenas señala, que en el contexto de la Sociedad de la Información, el Big Data marcó un hito debido a la posibilidad que ofrece de sistematización y análisis de la información (Cárdenas Cárdenas, 2019). En efecto, Trejo señaló que la forma en la que se trataba con la información en la Sociedad de la Información se caracterizaba por (i) amplia necesidad de transformar dicha información en conocimiento; (ii) la información se produce a gran velocidad, por lo que se necesita que el procesamiento de la misma se lleve, a su vez, de manera veloz; y (iii) no se requiere de transporte o concentraciones humanas grandes par tratar con la información (Trejo, 1996).

Ante todo ello, la tecnología del Big Data ofrece una solución en cuatro dimensiones, según IBM: (1) volumen, (2) velocidad, (3) variedad y (4) veracidad (IBM INSTITUTE FOR BUSINESS VALUE, 2012). Por su parte, Gil introduce dos conceptos adicionales como la quinta y sexta dimensión del Big Data: (5) visualización y (6) valor (Gil, 2016). A continuación se desarrollan a que se refieren estos términos:

1. **Volumen:** El Big Data es una tecnología de procesamiento que permite tratar con grandes volúmenes de datos. Actualmente, las herramientas de procesamiento de datos tradicionales como MS Excel o SQL no han demostrado eficiencia al tratar con el volumen actual de datos, por lo que ha sido necesario la utilización de nuevos sistemas que usan Big Data, como el NoSQL o el software Apache Hadoop que permiten tratar con millones de datos de manera eficaz (Gil, 2016).

2. **Velocidad:** La generación de la información no solo se caracteriza por su volumen, sino por la velocidad en la que esta se genera. Es así que necesitamos herramientas de procesamiento que puedan hacer frente a dicha información, como mencionan Conesa y Gómes, el tiempo de reacción es un factor crítico en este tipo de sociedades (Conesa & Gómez, 2015). Así, el Big Data se posiciona como la herramienta más eficiente y económica ante este desafío, pues es capaz de analizar tanto los datos dinámicos, los que se crean en tiempo real, como los estáticos, los que son datos históricos (Gil, 2016).

3. **Variedad:** La información generada es de diferentes tipos, por lo cual se requiere de una herramienta que permita el procesamiento de la variedad de datos que se producen. Si bien las herramientas tradicionales pueden procesar los datos estructurados, estas presentan problemas con los datos semi estructurados y, especialmente, con los no estructurados (Conesa & Gómez, 2015). Sumado al hecho de que en la actualidad la generación de datos estructurados es de solo el 20%, el Big Data se posiciona como la solución más eficaz, pues no solo permite procesar los tres tipos de datos, sino permite el tratamiento a pesar de que estos no se encuentren en ficheros con la misma estructura (Gil, 2016).

4. **Veracidad:** En la Sociedad de la Información, la creación del conocimiento juega un papel esencial, es por ello que la fiabilidad de la información resulta

relevante. Así, el Big Data busca conseguir datos de alta calidad, para lo cual utiliza sistemas que integran herramientas de reconocimiento y planificación de la incertidumbre (IBM INSTITUTE FOR BUSINESS VALUE, 2012).

5. **Visualización:** El Big Data busca otorgar una manera clara de entender la gran cantidad de datos que producimos. Como menciona Gil, "poder visualizar los datos es básico para comprenderlos y tomar decisiones en consonancia" (Gil, 2016).

6. **Valor:** Como última dimensión del Big Data, la profesora Gil incluye al valor, pues considera que la finalidad última de esta es justamente la de generar valor (Gil, 2016). Esto tiene coherencia con lo señalado por Bustamante y Guillén, quienes señalan que, en la sociedad actual, el valor de la información no solo se basa en la potencial obtención de conocimiento, sino en su reutilización (Bustamante Alonso & Guillén Alonso, 2017).

Teniendo en cuenta lo anterior, debe quedar claro que el contexto social en el cual se enmarca la presente investigación es uno en el cual la tecnología del Big Data se ha consolidado como la forma de procesamiento de datos que responde a las características de la Sociedad de la Información.

2.2. El contenido constitucionalmente protegido del derecho a la protección de datos personales

En la sección anterior hemos establecido y caracterizado el contexto en el cual se desarrolla la investigación. Sin embargo, antes de analizar cómo esta tecnología distorsiona la figura del consentimiento, es necesario determinar cuál es el contenido constitucionalmente protegido del derecho a la autodeterminación informativa. Esto es importante pues el consentimiento tiene como principal objetivo proteger el contenido constitucionalmente protegido de dicho derecho. Resulta

imposible avanzar con esta investigación, sin antes responder a la pregunta: ¿a qué nos referimos cuando hablamos del derecho a la protección de datos personales?

Para ello, en primer lugar, se desarrollarán los antecedentes que desencadenaron el reconocimiento de este derecho a nivel internacional. Se realizará un recorrido histórico por los aportes normativos y jurisprudenciales clave para el reconocimiento del derecho a la autodeterminación informativa como derecho fundamental autónomo. En segundo lugar, se analizará cuáles fueron los factores particulares que determinaron este reconocimiento a nivel nacional y cuál fue la configuración constitucional y legal que se utilizó en el Perú. Por último, abordaremos el papel que juega el consentimiento dentro de la configuración legal del derecho a la protección de datos personales, tanto a nivel nacional como internacional.

2.2.1. Antecedentes

En esta primera parte se desarrollarán los antecedentes normativos y jurisprudenciales que permitieron el reconocimiento del derecho a la protección de datos personales. Asimismo, se ahondará en las decisiones jurisprudenciales mediante las cuales se fue delimitando y caracterizando el contenido constitucionalmente protegido de este derecho.

Para comenzar, es necesario señalar que el derecho a la autodeterminación informativa tiene su origen histórico en la protección vinculada a los conceptos de privacidad e intimidad (Olivos, 2020). Con el paso del tiempo y con el avance tecnológico, surgieron preocupaciones concernientes con la privacidad, intimidad y sobre todo con el control de la información personal, lo cual ha impulsado desde los años 70 el desarrollo de un marco de protección legal ante dichos riesgos. En efecto, el desarrollo del derecho a la autodeterminación informativa estuvo influenciado por una serie de antecedentes, en principio, más históricos y anecdóticos (Olivos, 2020), doctrinales, normativos y jurisprudenciales, los cuales fueron determinantes para su evolución.

La evolución de este derecho ha estado marcada en sus inicios por contribuciones doctrinales estadounidenses las cuales permitieron sentar las bases para su configuración en diversos marcos normativos. Uno de los primeros pasos a dicha conceptualización fue dado en el siglo XIX por Thomas A. Cooley. Este autor acuñó la expresión “the right to be let alone” (en español, “el derecho a ser dejado en paz”) en el año 1879. Cooley señalaba que la privacidad debía (i) ser un derecho fundamental y (i) ser entendida de manera amplia, de manera tal que otorgara una protección a individuos ante cualquier intromisión externa, ya sea estatal o particular. Asimismo, dicho autor vinculó la protección de la privacidad con la Tercera, Cuarta y Quinta Enmienda de la Constitución de Estados Unidos. Es importante mencionar que la privacidad, en este contexto, no se encontraba prevista en la Constitución de dicho país, por lo cual los aportes de Cooley marcaron un primer precedente para el reconocimiento de la privacidad como derecho fundamental en Estados Unidos.

En 1890, Samuel Warren y Louis Brandies, en base a las ideas de Cooley, publican en la revista jurídica “Harvard Law Review” el artículo “The right to privacy”. En este los autores expenden el concepto de privacidad, pues hasta ese momento se entendía que esta era una protección contra intromisiones físicas. En efecto, los autores incluyeron dentro del alcance del concepto de privacidad el control de la información personal de los ciudadanos. Es claro que este aporte fue fundamental para la consolidación del derecho a la autodeterminación informativa como derecho autónomo.

Posterior a ello, ya en el siglo XX, en el año 1967, Alan Westion acuñó el término “informational privacy” (en español, “autodeterminación informativa”). Westin entendió que con el avance tecnológico la masificación del uso datos personales era inminente, por lo que era necesario una redefinición de la privacidad. Esta reconceptualización debía centrarse en el control de las personas sobre sus datos personales. Así, el autor define a la autodeterminación informativa como el derecho

de los individuos decidir cómo, cuándo y con qué finalidad su información debía ser tratada. El enfoque del autor sobre la privacidad iba más allá de la protección contra injerencias, sino que se centraba en el papel activo en la gestión de información de las personas.

Durante el siglo XX, posterior a la Segunda Guerra Mundial, se introdujeron los primeros cuerpos normativos que incorporan a la privacidad como un derecho. En efecto, en las primeras normas internacionales tenemos a: (i) la Declaración Universal de los Derechos Humanos de 1948 (en adelante, la "Declaración Universal") y (ii) el Pacto Internacional de Derechos Civiles y Políticos de 1966 (en adelante, (el "Pacto Internacional"). Cabe mencionar que al igual que en el desarrollo doctrinal, en el ámbito normativo, se comenzó con la protección de la privacidad entendida como una protección contra intromisiones físicas y evolucionó hasta eventualmente incluir el control de la información personal. Así, el enfoque de la Declaración Universal y del Pacto Internacional estuvo más ligado a la protección de la privacidad, lo cual sentó las bases para que con el tiempo se desarrollaran normativas que reconocieran el derecho a la autodeterminación informativa como un derecho autónomo.

Respecto de la Declaración Universal, en su artículo 12, se establece una protección sobre injerencias arbitrarias en contra de la vida privada, familiar, del domicilio o de la correspondencia. Si bien en este primer cuerpo normativo, no se hace referencia directa al derecho a la autodeterminación informativa, si se reconoce el derecho a la privacidad. Efectivamente, este reconocimiento fue una respuesta a los abusos e intromisiones de los regímenes totalitarios surgidos en la Segunda Guerra Mundial; es decir, surgió de la necesidad de proteger la privacidad de las personas ante ataques e injerencias arbitrarias e ilegales por parte de los Estados u otros actores. Además de ello, esta disposición resulta relevante debido a que no solo reconoce el derecho de privacidad de los individuos, sino también impone una obligación hacia los Estados de garantizar la efectividad de la protección. Igualmente, es

necesario mencionar que la definición de privacidad en esta disposición es de carácter amplio.

Por su parte, el Pacto Internacional establece en su artículo 17 de manera explícita el derecho a la privacidad de todo individuo. Ambos cuerpos normativos sentaron las bases para el desarrollo y reconocimiento del derecho a la autodeterminación informativa en diversos Estados. En efecto, en 1970, se promulgó la ley de protección de datos (Datenschutzgesetz) en el estado alemán de Hesse. Es importante mencionar que esta norma surge como respuesta al peligro que representaba el acceso a los bancos de datos públicos. Por dicha razón, se consideró que el título de la ley no era adecuado, pues la ley no protegía directamente los datos de las personas, sino los derechos de las personas cuyos datos eran tratados (Casal Tavasci, 2018).

La promulgación de esta norma dio inicio a un movimiento legislativo a nivel global. En efecto, en 1973, Suecia se convirtió en el primer país en regular una ley nacional de protección de datos (Datalagen). Asimismo, la República Federal Alemana en 1976 promulgó una ley nacional, la cual no solo buscaba proteger los datos personales en el ámbito público, sino también en el sector privado. Dos años más tarde, en 1978, Francia, Dinamarca y Austria publican normas especializadas en la protección de datos personales.

En Estados Unidos también se unió a este movimiento legislativo. En 1974, se publica el llamado “Privacy Act”, una norma de carácter federal que tuvo como objeto regular el tratamiento de datos personales por parte de las agencias gubernamentales. Un aspecto para destacar es que esta norma estableció los conocidos “Fair Information Practice Principles (FIPP)”. Estos eran un conjunto de principios destinados a regular la recopilación, uso y procesamiento de datos personales en Estados Unidos. Entre ellos tenemos a los siguientes: transparencia, limitación en la recopilación, calidad de datos, finalidad, no divulgación, acceso, corrección, entre otros. Estos principios son la base sobre la cual se cimientan la

normativa en Estados Unidos destinada a la protección de datos personales en diversos sectores.

Ahora bien, hasta este momento, la regulación de la protección de datos personales era a nivel legislativo. Esta situación cambia cuando en 1976, Portugal incluye en el artículo 35 de su Constitución el derecho a la autodeterminación informativa. De igual manera, en el año 1978, España reconoce este derecho, en conexión con el derecho a la intimidad, en el artículo 18 de su Constitución.

Finalmente, a nivel normativo es indispensable mencionar que en 1981, se publica la primera norma internacional jurídicamente vinculante especializada en materia de protección de datos personales. Efectivamente, el 28 de enero de dicho año, el Consejo de Europa publica el Convenio No. 108, “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”. Este convenio es fundamental pues en base al mismo el Tribunal Europeo de Derecho Humanos construyó jurisprudencia en relación a la protección del derecho a la autodeterminación informativa (Casal Tavasci, 2018).

Continuando con los avances en esta materia, a finales del siglo XX se produjeron los primeros hitos jurisprudenciales que definirán el contenido y alcance de este derecho. El primer gran antecedente jurisprudencial se le acredita al Tribunal Constitucional Federal con la sentencia del 15 de diciembre de 1983 (1 BvR 209, 269, 362, 420, 440, 484/83). En dicho pronunciamiento, el Tribunal señaló que a pesar de no contar con un reconocimiento expreso en la Constitución alemana, la autodeterminación informativa sí formaba parte del catálogo de derechos fundamentales. Asimismo, señaló que este derecho protege a los individuos contra la recopilación, almacenamiento, uso y difusión no autorizados de sus datos personales.

Posteriormente, en el año 2000, el Tribunal Constitucional Español publicó dos sentencias importantes en materia del derecho a la autodeterminación informativa:

las sentencias 290/2000 y la 292/2000. La primera de ellas confirmó la constitucionalidad de la Ley 5/1992 – Ley de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Además, en este fallo se reconoció al consentimiento informado como pieza de gran importancia al momento de tratar los datos de cualquier ciudadano.

Por su parte, la sentencia 292/2000 trajo consigo una de las contribuciones más grandes para el desarrollo de este derecho. En la misma, se señaló que existía una diferencia explícita entre el derecho a la autodeterminación informativa y el derecho a la intimidad. Como se mencionó anteriormente, en la Constitución española de 1978 se reconoce el derecho a la autodeterminación informativa en el artículo 18; sin embargo, este se encontraba en conexión y formaba parte del derecho a la intimidad. En la sentencia 292/2000, se señaló que ambos derechos se diferenciaban en su función, objeto y contenido.

Asimismo, esta sentencia fue la primera en dotar de contenido al derecho a la autodeterminación informativa:

> «7. [el derecho a la protección de datos de carácter personal] *consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la*

facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos» (STC 292/2000, 2000, p. 7).

El derecho a la protección de los datos personales, tal como lo conocemos hoy, ha sido el resultado de un proceso evolutivo que comenzó con las contribuciones doctrinales de juristas como Thomas M. Cooley, Samuel Warren, Louis Brandeis, y Alan Westin. Estos autores establecieron los principios fundamentales de la privacidad y la autodeterminación informativa, los cuales han sido posteriormente adoptados y desarrollados en diversos marcos normativos y jurisprudenciales a lo largo del siglo XX. La protección de los datos personales es ahora un derecho fundamental que responde a los retos de la era digital, garantizando que los individuos mantengan el control sobre su información personal y su autonomía en la toma de decisiones.

2.2.2. Reconocimiento expreso del derecho a la autodeterminación informativa en la Constitución peruana de 1993

Teniendo en cuenta el proceso histórico mediante el cual la protección de datos personales adquirió relevancia en la sociedad moderna, es necesario ahondar en cómo este proceso se reflejó en el contexto peruano. Así, en el Perú, es la Constitución de 1993 la que incorpora en el catálogo de derechos fundamentales al derecho a la autodeterminación informativa. Esto marcó un hito respecto del reconocimiento de la necesidad de protección de la privacidad frente a la revolución tecnológica. Lamentablemente, a pesar de su inclusión, el contenido y la redacción del derecho presentó varias limitaciones que afectan la eficacia del mismo. En esta parte de la investigación se abordará el análisis sobre la evolución del derecho en el contexto constitucional peruano.

El reconocimiento del derecho a la autodeterminación informativa en la Constitución de 1993 debe entenderse dentro del contexto de cambio de modelo constitucional

que representó esta nueva Constitución. La Constitución de 1979 fue una de corte garantista y se orientaba a la protección de derechos colectivos, económicos y sociales. Sin embargo, en la década de los 90, debido al cambio de modelo político y económico, este enfoque cambió. En efecto, se buscó un enfoque que facilitara la inversión privada y extranjera. Lamentablemente, este cambio se dio a costa de la protección de varios derechos fundamentales protegidos y reconocidos antes en la Constitución de 1979.

La Constitución de 1993 justamente responde a esta transición dado que fue con la misma que se marcó el inicio del enfoque económico liberal en el país. Esta constitución se diseñó con el objetivo de consolidar un modelo económico que diera prioridad a la inversión privada, aunque esto significaba la reducción de garantías sociales. Tal como menciona Ochoa Cardich, el cambio constitucional en 1993 significó una deconstrucción del modelo garantista establecido en la Constitución de 1979, transformando los derechos sociales y colectivos en fórmulas retóricas y minimizando su alcance real (Ochoa Cardich, 2020).

En contraste con esta situación, es de resaltar que la Constitución de 1993 incluyó en el catálogo de derechos fundamentales al derecho a la autodeterminación informativa, lo cual significó un avance en la protección de la privacidad y, en general, de los derechos fundamentales en la sociedad de la información. Cabe aclarar que en la Constitución de 1993 no se utilizó el término “autodeterminación informativa” y la redacción del precepto normativo no evocaba una normal tal como la entendemos hoy.

En efecto, la Constitución de 1993 reconoció el derecho de todo ciudadano a ejercer el control sobre el tratamiento de sus datos personales. Posteriormente, el Tribunal Constitucional peruano denominaría este derecho como autodeterminación informativa, siguiendo el ejemplo europeo. Específicamente, se reconoció este derecho en el artículo 2, inciso 6 de la Constitución, el cual señala lo siguiente:

> Artículo 2, inciso 6: “Toda persona tiene derecho (…) a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”.

Este derecho, aunque de carácter innovador, no alcanzó a ofrecer una protección robusta frente a los desafíos que el manejo de datos personales implica en la sociedad de la información. Si bien, la incorporación de la autodeterminación informativa en la Constitución peruana fue una respuesta a la creciente informatización y al uso masivo de tecnologías de información, que planteaban un riesgo para la privacidad. Lo cierto es que la formulación del artículo y su enfoque limitado fueron objeto de críticas, puesto que su redacción no es lo suficientemente amplia para enfrentar las múltiples vulneraciones a la privacidad derivadas del procesamiento de datos personales. Antes de pasar al análisis de las críticas planteadas al precepto constitucional, desarrollaremos los fundamentos que dieron origen a su planteamiento final.

La inclusión del derecho a la autodeterminación informativa en la Constitución de 1993 se debió al inminente cambio social producido por el avance tecnológico. De hecho, en el debate constitucional en torno al artículo 2.6 de la Constitución de 1993, se hizo mención a que la inclusión del mismo se debió a la entrada de la “Era de la Información” (Diario de Debates, 2011). El paso a esta nueva etapa de la sociedad estuvo marcada no solo por los cambios tecnológicos a finales del siglo XX, sino fue una transformación en las estructuras de poder dentro de la sociedad.

En efecto, debido a la proliferación de los sistemas informáticos, la capacidad de gestión de grandes cantidades de datos produjo una nueva forma de poder basado en el control de dicha información. Este cambio fue tomado en consideración por el Constituyente al momento de decidir la inclusión del artículo 2.6. En los debates constitucionales, se evidencia la preocupación sobre el poder producto del control de la información, al punto de reconocerla como una forma de riqueza (Diario de Debates, 2011).

Es en este contexto que se concluye en establecer expresamente una protección para las personas ante los efectos nocivos del avance tecnológico. Tal como menciona Torres y Torres Lara en los debates constitucionales, con la inclusión de este derecho se intentó establecer “un mecanismo para proteger al ciudadano del desarrollo de la informática, en el sentido de que la informática sirva para el desarrollo de la economía y para el desarrollo de los patrimonios, pero que no vaya contra la intimidad personal o familiar” (Diario de Debates, 2011). Esta visión fue la que fundamentó la inclusión del artículo 2.6 en la Constitución de 1993. No obstante, como se desarrollará a continuación, el objetivo de dotar a los ciudadanos con el control sobre su propia información se vió limitado debido a la redacción del precepto constitucional.

La formulación escogida por el Constituyente para el artículo 2.6 de la Constitución de 1993 presentó limitaciones que redujeron la eficacia del mismo. Tal como menciona Castro Cruzzat, “la fórmula constitucional consagra el derecho a la protección de datos personales de forma sesgada, guardando silencio respecto de los elementos básicos que configuran este derecho” (Castro Cruzatt, 2008). Siguiendo esta misma línea, Eguiguren menciona que “el texto del precepto constitucional fue insuficiente y deficiente, lo cual limitó los alcances de la protección del derecho a la autodeterminación informativa” (Eguiguren Praeli, 2015).

Estas limitaciones se pueden clasificar en tres grandes problemas: (i) la limitación del alcance restringido a las entidades que ofrezcan “servicios informáticos” de suministro de información, (ii) el contenido limitado únicamente a la protección contra la difusión de datos, y (iii) la dependencia al derecho a la intimidad.

i. **Limitación en el alcance:** el texto del artículo 2.6 restringe su alcance al señalar que “toda persona tiene derecho (…) a que los servicios informáticos no suministren informaciones”. En efecto, la referencia a entidades que ofrezcan servicios informáticos resulta imprecisa y limitante. Del precepto

constitucional se interpreta que la protección es aplicable únicamente a entidades cuya actividad principal sea el suministro de información a terceros, “pudiendo quedar excluidos los registros o bancos de datos existentes que no brindan servicio ni acceso al público”(Eguiguren Praeli, 2015).

Asimismo, Castro Cruzzat señala que desde la perspectiva planteada por el artículo 2.6, “se podría concluir que este derecho no es exigible frente a entidades que, sin tener como finalidad principal el suministro de información a terceros, cuentan con registros o bancos de datos personales que utilizan como apoyo a sus funciones” (Castro Cruzatt, 2008). Así, este problema en la redacción del artículo dificulta la eficacia del mismo en sectores que tratan con datos personales, pero que no prestan en sentido literal un servicio informático de suministro de datos.

ii. **Limitación en el contenido del derecho:** la redacción limita el contenido del derecho a la autodeterminación informativa, pues omite casi todas las facultades que integran al derecho. Efectivamente, el texto solo hace alusión a la protección contra la difusión de información, excluyendo otras facultades esenciales del derecho como el acceso, actualización, rectificación, etc (Castro Cruzatt, 2008). Estas otras facultades fueron reconocidas en otras legislaciones y normas internacionales, como se señaló anteriormente, desde mediados del siglo XX. Esta crítica es señalada por Eguiguren, el cual menciona que la norma omitió componentes esenciales del derecho, reconocidos en otras normas constitucionales comparadas (Eguiguren Praeli, 2015). Esto resulta contradictorio con los fundamentos que señalaron los Constituyentes, ya que estas otras facultades resultan imprescindibles para la efectiva protección del derecho a la autodeterminación informativa en la “Era de la información”.

iii. **Dependencia al derecho a la intimidad:** el precepto constitucional presenta un error al mantener la dependencia del derecho a la autodeterminación informativa con el derecho a la intimidad personal y familiar. Esta visión es una restringida pues no reconoce la autonomía del derecho a la autodeterminación informativa. “Si bien este derecho surgió como parte del desarrollo a la intimidad, su evolución lo ha configurado como un derecho autónomo y con ámbito de protección distinto” (Castro Cruzatt, 2008). En ese sentido, el precepto constitucional refleja un enfoque desactualizado del derecho para la época, pues en otras legislaciones mucho antes se dejó en claro la autonomía de este.

Ante esta situación, los legisladores buscaron corregir y precisar la redacción del derecho a la autodeterminación informativa. Esta iniciativa se consolidó con la promulgación del Código Procesal Constitucional en 2004. Esta norma es considerada como el esfuerzo legislativo para intentar superar las deficiencias del precepto constitucional, alineándose a los estándares internacionales. En efecto, Eguiguren menciona que ante las deficiencias del texto constitucional, los que elaboraron el proyecto del Código Procesal Constitucional decidieron “incluir, al regular los alcances del proceso de hábeas data (…) una suerte de desarrollo o mayor precisión del contenido del derecho a la protección de datos personales como una forma de suplir muchas de las carencias u omisiones antes señaladas” (Eguiguren Praeli, 2015).

2.2.3. Desarrollo constitucional por parte del Código Procesal Constitucional en 2004

El Código Procesal Constitucional de 2004 se erigió como una respuesta a las limitaciones que presentaba el artículo 2.6, complementando el marco normativo y dando desarrollo al derecho a la autodeterminación informativa. En este sentido, Orrego destaca la importancia del Código Procesal Constitucional como norma de desarrollo constitucional que produjo “un mejor tratamiento de la configuración del

derecho fundamental de autodeterminación informativa, que complementa lo normado en el texto constitucional" (Orrego, 2013).

En específico, todo ello se concretó en el artículo 61 inciso 2, el cual abordó la regulación del proceso constitucional de hábeas data en relación con el artículo 2.6 de la Constitución. El texto del artículo 61.2 estableció lo siguiente:

> "Artículo 61.- Derechos protegidos. El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: (…)
>
> 2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

A primera vista, es evidente que la formulación del artículo 61.2 amplía significativamente el contenido del derecho fundamental a la autodeterminación informativa, en comparación con el marco constitucional original. Efectivamente, se reconocen las siguientes facultades del titular de los datos: conocer, actualizar, incluir, suprimir y rectificar. A continuación se desarrollaran los aciertos de esta norma. Sin embargo, este no fue el único acierto del Código Procesal Constitucional. Lo cierto es que mediante el mismo intentó corregir las deficiencias del artículo 2.6 de la Constitución.

i. En primer lugar, el artículo 2.6 de la Constitución presentaba una deficiencia de alcance, ya que limitaba dicho alcance a únicamente las entidades que

prestaran “servicios informáticos” de suministro de datos. El Código Procesal Constitucional corrigió esta deficiencia al ampliar el alcance a cualquier entidad que almacene o registre o almacene datos personales (Eguiguren Praeli, 2015). En efecto, la norma señala que la información protegida abarca los datos de las personas que “que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros”.

Asimismo es de destacar que dicha aplicación es acertada pues brinda protección a los datos de las personas en cualquier contexto y no lo limita a entornos digitales. Como menciona Castro Cruzzat, “si bien la protección de datos personales surge como reacción ante el riesgo derivado del tratamiento informatizado de datos personales, ello no supone que el tratamiento de información personal almacenada de manera manual o mecánica no deba ser objeto de tutela” (Castro Cruzatt, 2008).

ii. En segundo lugar, el Código Procesal Constitucional supera la carencia en el contenido del derecho y dota de diversas facultades al titular de los datos personales. Como menciona Eguiguren, “frente a la mención insuficiente al derecho de poder impedir el suministro o la difusión de los datos personales, el Código otorga también al titular los derechos a poder conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona” (Eguiguren Praeli, 2015). Esta precisión fue fundamental para dotar a las personas con un control integral sobre su información personal y alinear al Perú con los estándares de protección reconocidos internacionalmente.

iii. Por último, se supera la dependencia del derecho a la autodeterminación informativa con el derecho a la intimidad personal y familiar. Si bien aún no se reconoce a este derecho como un de carácter autónomo, si se evita la interdependencia exclusiva con el derecho a la intimidad personal y familiar.

> Como señala Eguiguren, el fundamento de la protección no se circunscribe a la preservación de la intimidad, sino el enfoque está puesto en la prohibición de cualquier tipo de injerencia a los datos personales de las personas que puedan afectar derechos constitucionales (Eguiguren Praeli, 2015).

A pesar de los evidentes avances, la norma propuesta por el Código Procesal Constitucional no estuvo exenta de críticas. En especial, se puso en manifiesto dos errores significativos: (i) la confusión entre datos sensibles y datos privados, y (ii) el establecimiento como prerrequisito de la vulneración de otros derecho para ejercer las facultades del titular de los datos personales.

i. **Datos sensibles y datos privados:** la norma menciona lo siguiente " (…) a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales". Si bien a primera vista esto es positivo, pues se por primera vez se regula una protección reforzada para los datos de naturaleza sensible y se los distingue de la categoría general de datos personales. Lo cierto es que la norma genera confusión al introducir una tercera categoría de datos: datos privados. El problema reside en que, de la redacción de la norma, se podría asimilar de manera errónea a los datos sensibles con los datos privados. Lo cual llevaría a concluir que las facultades de cancelación y de reserva se ejercen solo cuando estamos ante datos de categoría sensible o privados. Esta conclusión resulta completamente lesiva pues estas facultades se deben ejercer ante cualquier tipo de dato. Como menciona Castro Cruzzat, hubiera sido preferible que el Código aluda más bien a información o datos personales y no introduzca una noción que puede generar confusión" (Castro Cruzatt, 2008).

ii. **Prerrequisito para el ejercicio de las facultades del titular de datos personales:** la norma no señala una dependencia expresa con el derecho a la intimidad; sin embargo, hace alusión a la necesidad de un prerrequisito a

> los titulares de los datos personales: la vulneración de un derecho. Esto limita que se pueda considerar al derecho a la autodeterminación informativa como un derecho autónomo. Como bien menciona Castro Cruzzat, el ejercicio de las facultades que integran el derecho a la autodeterminación informativa, no deben estar condicionados a que se verifique la violación o amenaza de otro derecho (Castro Cruzatt, 2008).

En este puntoi es preciso mencionar que el 3 de julio de 2021, se publica el Nuevo Código Procesal Constitucional, este siguió la línea planteada en 2004. En este nuevo código, se reguló la protección del derecho a la autodeterminación informativa en el artículo 59[1]. Respecto a los cambios se explicitaron los escenerios en los cuales se podía ejercer la defensa del mencionado derecho. Asimismo, en el

[1] Artículo 59. Derechos protegidos
(...)
También procede en defensa del derecho a la autodeterminación informativa, enunciativamente, bajo las siguientes modalidades:
1) Reparar agresiones contra la manipulación de datos personalísimos almacenados en bancos de información computarizados o no.
2) A conocer y supervisar la forma en que la información personal viene siendo utilizada.
3) A conocer el contenido de la información personal que se almacena en el banco de datos.
4) A conocer el nombre de la persona que proporcionó el dato.
5) A esclarecer los motivos que han llevado a la creación de la base de datos.
6) A conocer el lugar donde se almacena el dato, con la finalidad de que la persona pueda ejercer su derecho.
7) A modificar la información contenida en el banco de datos, si se trata de información falsa, desactualizada o imprecisa.
8) A incorporar en el banco de datos información que tengan como finalidad adicionar una información cierta pero que por el transcurso del tiempo ha sufrido modificaciones.
9) A incorporar información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado.
10) A incorporar al banco de datos una información omitida que perjudica a la persona.
11) A eliminar de los bancos de datos información sensible que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona.
12) A impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada.
13) A que el dato se guarde bajo un código que solo pueda ser descifrado por quien está autorizado para hacerlo.
14) A impedir la manipulación o publicación del dato en el marco de un proceso, con la finalidad de asegurar la eficacia del derecho a protegerse.
15) A solicitar el control técnico con la finalidad de determinar si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.
16) A impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

artículo 53[2] se adopta la definción respecto del banco de datos acorde a la Ley de Proteción de Datos Personales de 2011.

Es preciso mencionar que el Código Procesal Constitucional no solo corrigió los errores presentados por la redacción del artículo 2.6 de la Constitución, sino que complementa y reafirma los avances producidos por el Tribunal Constitucional. Antes de la promulgación del Código Procesal Constitucional de 2004, el Tribunal Constitucional ya había publicado sentencias que desarrollaban el derecho a la autodeterminación informativa.

2.2.4. Desarrollo jurisprudencial por parte del Tribunal Constitucional peruano

El proceso de desarrollo de este derecho fue gradual y, actualmente, se sigue reinventando para poder enfrentar los desafíos tecnológicos que presenta la Sociedad de la Información. Es importante recordar que si bien el derecho fue reconocido en la Constitución de 1993, el precepto constitucional presenta varias carencias que limitaban la eficacia del mismo. En este contexto, los pronunciamientos del Tribunal Constitucional fueron claves para impulsar la evolución del derecho a la autodeterminación informativa, haciendo aportes sustanciales que precisaron su contenido y alcance.

Como señala Olivos, estos pronunciamientos fueron fundamentales, especialmente si consideramos que para la época no existía una ley específica o un órgano de control especializado en la materia (Olivos, 2020). En esta misma línea, Eguiguren comenta que el tribunal Constitucional peruano no fue ajeno a esta temática y realizó aportes para la mejor comprensión y protección del contenido del derecho a la protección de datos personales (Eguiguren Praeli, 2015). Pero la labor del

[2] Artículo 53. Definición del banco de datos
Se entiende por archivo, registro, base o banco de datos a todo conjunto de datos organizado de información personal y que sean objeto de tratamiento o procesamiento físico, electrónico o computarizado, ya sea público o privado, y cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Tribunal Constitucional no se limitó a desarrollar el contenido del derecho a la autodeterminación informativa, sino la labor del mismo fue fundamental para precisar el "objeto de este derecho, su naturaleza relacional, y (…) [marcar] las diferencias entre este y otros derechos humanos como los de la intimidad, la imagen y la identidad personal" (Orrego, 2013). En esta parte de la investigación ahondaremos en los principales pronunciamientos del Tribunal Constitucional que permitieron esta evolución.

2.2.4.1. Sentencia recaída en el Expediente No. 666-1996-HD/TC

El primer pronunciamiento importante en la materia data de 1998, con la publicación de la Sentencia recaída en el Expediente No. 666-1996-HD/TC. En este caso, el Tribunal Constitucional se centró en desarrollar y precisar el ejercicio del proceso de hábeas data como un mecanismo para garantizar las libertades informativas. Así, menciona que para ejercer el hábeas data y proteger las libertades informativas recogidas en el artículo 2.6 de la Constitución, toda persona tiene derecho a "acceder a los registros de información almacenados en centros informáticos o computarizados, cualquiera sea su naturaleza, a fin de rectificar, actualizar, excluir determinado conjunto de datos personales, o impedir que se propague información que pueda ser lesiva al derecho constitucional a la intimidad" (Sentencia del Tribunal Constitucional recaída en el Expediente No. 666-1996-HD/TC, fundamento 2).

Mediante esta sentencia, el Tribunal Constitucional amplía las facultades del titular de los datos personales. En efecto, para este momento, se entendía que las personas contaban con un derecho únicamente contra la difusión de sus datos, este fallo corrige el error del artículo 2.6 y amplía la protección otorgando al titular de los datos personales y control amplio sobre su información. Así mismo, es importante destacar que con este fallo se puso en énfasis "un estadio anterior del propuesto por el artículo 2, inciso 6, es decir, que el ciudadano antes de impedir el suministro de información, puede tener acceso al banco de datos" (Orrego, 2013).

Lamentablemente, a pesar de estos avances, el Tribunal Constitucional comete un error al continuar el vínculo de dependencia del derecho a la autodeterminación informativa con el derecho a la intimidad. Del texto de la sentencia se aprecia que el ejercicio de facultades del titular de los datos tiene un prerrequisito: la lesión al derecho a la intimidad (Sentencia del Tribunal Constitucional recaída en el Expediente No. 666-1996-HD/TC, fundamento 2). Tal como menciona Orrego, "aún los argumentos constitucionales solo ponen como parámetro de protección al derecho a la intimidad" (Orrego, 2013). Cómo se desarrollará posteriormente, el Tribunal Constitucional corrige este error y reconoce la autonomía del derecho a la autodeterminación informativa.

Es interesante cómo en 1998, el Tribunal Constitucional comenzó a abordar de manera integral las facultades del titular de los datos personales, alineando los estándares de protección en Perú con los establecidos en Europa. Esto no solo contribuyó a corregir las deficiencias del texto del artículo 2.6 de la Constitución, sino que sentó las bases para las reformas introducidas en el Código Procesal Constitucional en 2004.

2.2.4.2. Sentencia recaída en el Expediente No. 1797-2002-HD/TC

En el año 2003, el Tribunal Constitucional publica la Sentencia recaída en el Expediente 1797-2002-HD/TC, la cual marcaría un hito importante en la evolución del derecho a la autodeterminación informativa. En dicha sentencia, el Tribunal Constitucional precisa tres aspectos a destacar: (i) adopta la terminología de "derecho a la autodeterminación informativa", alineándose con la nomenclatura europea, (ii) reconoce la autonomía del derecho y lo diferencia de otros, y (iii) ratifica las facultades del titular de los datos personales.

Respecto del primer punto, es importante destacar que la sentencia marca un hito en la jurisprudencia del derecho al referirse a él con la terminología acuñada y popularizada en Europa: derecho a la autodeterminación informativa. La sentencia

menciona lo siguiente: “el derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa”. Hasta ese momento, el derecho a la protección de los datos personales era entendido en vinculación con el derecho a la intimidad. Con el establecimiento de esta nueva nomenclatura el Tribunal Constitucional no solo se alinea con los estándares internacionales, sino que se permite diferenciar el derecho de otros.

En efecto, esta adaptación terminológica estuvo acompañada con un desarrollo conceptual que marcó las diferencias de este derecho con otros como la intimidad, imagen e identidad personal. Tal como menciona Olivos, el Tribunal Constitucional se preocupó por plantear las diferencias del derecho a la autodeterminación informativa con los siguientes derechos: intimidad e imagen; esto con el objetivo de reconocer que este derecho es un independiente (Olivos, 2020). Esto fue fundamental pues “el Tribunal tomó distancia de la identificación entre el derecho a la intimidad y el derecho a la protección de datos personales que venía defendiendo hasta ese entonces” (Castro Cruzatt, 2008).

Para llegar a esta conclusión, el Tribunal Constitucional empieza por señalar que el objeto de protección del derecho a la autodeterminación informativa es “proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC). Sin embargo, hace una precisión fundamental al señalar que aunque su objeto de protección esté relacionado con estos otros derechos, el mismo no puede identificarse o confundirse con estos. Esto se debe a que el derecho a la autodeterminación informativa tiene una naturaleza relacional, “pues las exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

Dejando en claro esto, el Tribunal Constitucional, de manera integral, señala las diferencias existentes entre el derecho a la autodeterminación informativa y los derechos de (i) intimidad, (ii) imagen y (iii) identidad personal:

i. En relación al derecho a la intimidad, se señala que la diferencia con el derecho a la autodeterminación informativa radica en mientras el derecho a la intimidad "protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel [derecho a la autodeterminación informativa] garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen" (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC)

ii. En relación con el derecho a la imagen, el Tribunal Constitucional puntualiza que mientras el derecho a la imagen protege la representación visual de la persona, el derecho a la autodeterminación informativa tiene un enfoque en el control de la información personal. Así, se precisa que "básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad". (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

iii. Finalmente, en relación con el derecho a la identidad personal, este busca garantizar que "la proyección social de la propia personalidad no sufra interferencias o distorsiones" (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC); por su parte, el derecho

a la autodeterminación informativa busca proteger el control de las personas sobre sus datos personales.

Ahora bien, el Tribunal Constitucional en esta sentencia realiza un último aporte: ratifica las facultades del titular de los datos personales. Como menciona Castro Cruzzat, “resulta positivo que en la misma sentencia, siguiendo lo señalado en anteriores pronunciamientos y frente al contenido limitado que le reconoce la Constitución, el Tribunal haya precisado las facultades que integran este derecho” (Castro Cruzatt, 2008). En esta sentencia el Tribunal Constitucional detalló que las facultades que integran al derecho a la autodeterminación informativa son las siguientes:

1. **Acceso a los registros de información:** Al respecto, el Tribunal Constitucional señala que toda persona tienen “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” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

2. **Actualización de datos personales:** En la sentencia se precisa que “el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien 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” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

3. **Rectificación de los datos personales:** Según el Tribunal Constitucional, “un individuo puede rectificar la información, personal o familiar, que se haya registrado” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

4. **Oposición:** En esta sentencia se deja claro que toda persona tiene derecho a “impedir que esta se difunda para fines distintos de aquellos que justificaron su registro” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

5. **Cancelación:** Por último, se señala que toda persona tiene “la potestad de cancelar aquellos [datos] que razonablemente no debieran encontrarse almacenados” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 1797-2002-HD/TC).

2.2.4.3. Sentencia recaída en el Expediente No. 04739-2007-PHD/TC

La siguiente sentencia a destacar data del año 2007, específicamente, la Sentencia recaída en el Expediente 04739-2007-PHD/TC. En este fallo, el Tribunal Constitucional realizó dos aportes significativos para el desarrollo del derecho a la autodeterminación informativa: (i) reafirmó la autonomía del derecho y (ii) estableció la categoría de “datos sensibles”.

Sobre el primer punto, en la sentencia se señala lo siguiente:

> “Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar (…), el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen”. (Sentencia del Tribunal Constitucional recaída en el Expediente No. 04739-2007-PHD/TC).

Así, el Tribunal Constitucional subraya que el derecho a la autodeterminación informativa busca proteger a la persona en sí misma, mediante el control sobre su información. Con ello, se reconoce que el fundamento del control de la información no se limita a la afectación al derecho a la intimidad, sino que el Tribunal reconoce que los riesgos derivados del control indebido de los datos personales puede afectar otros aspectos de vida de las personas, aspectos que trascienden la esfera estrictamente privada.

Por otra parte, la sentencia hace referencia a una categoría especial de datos personales: datos sensibles. El Tribunal Constitucional señala que estos, por su naturaleza, “no deben ser objeto de difusión ni de registro” (Sentencia del Tribunal Constitucional recaída en el Expediente No. 04739-2007-PHD/TC). Es imprescindible mencionar que esta idea será desarrollada mediante la Ley No. 29733 y su reglamento.

En años posteriores, el Tribunal Constitucional reivindicó y amplió los fundamentos desarrollados en estas sentencias. Por ejemplo, en el año 2007, con la Sentencia recaída en el Expediente No. 03052-2007-PDH/TC, se reafirmó la facultad de cancelar la información personal por parte del titular de los datos personales. En ese mismo año, mediante la Sentencia recaída en el Expediente No. 06164-2007-HD/TC, el Tribunal Constitucional desarrolló las tipologías del proceso constitucional de hábeas data y destacó que los titulares de los datos personales contaban con las facultades de rectificación, actualización y exclusión. En el año 2010, mediante la Sentencia recogida en el Expediente No. 0746-2010-HD/TC, se establecieron algunos parámetros para el ejercicio legítimo de este derecho. En el año 2011, con la Sentencia recaída en el Expediente No. 0831-2010-PHD/TC, se ahondó el impacto social del control de la información personal, en específico en contextos laborales y financieros. En el año 2014, se publicó la Sentencia recaída en el Expediente No. 2491-2013-PHD/TC, mediante la cual se subrayó la importancia del derecho de acceso a los datos almacenados y se señaló que la negación de esta

facultad constituía una vulneración directa al derecho a la autodeterminación informativa.

Es importante mencionar que todo este desarrollo jurisprudencial acompañó a la promulgación de la Ley No. 29733 —Ley de Protección de Datos Personales— en el año 2011 y su Reglamento publicado en el año 2013. Mediante estas, se estableció el marco normativo para la protección de datos personales en el Perú. Es evidente que estas normas utilizaron los conceptos desarrollados tanto por la Constitución, Código Procesal Constitucional y por las diversas sentencias del Tribunal Constitucional.

2.3. Desarrollo del derecho a la autodeterminación informativa por parte de la Ley No. 29733 y su Reglamento

El 3 de julio de 2011 y el 22 de marzo de 2013, se publicaron la Ley No. 29733 —Ley de Protección de Datos Personales— (en adelante, "Ley de protección de datos personales" o "Ley") y Decreto Supremo No. 003-2013-JUS (en adelante, "Antiguo Reglamento"), lo cual marcó un hito para el desarrollo del derecho a la autodeterminación informativa en el Perú, pues consolidó el marco normativo para su protección. Es importante mencionar, que el 30 de noviembre de 2024, mediante el Decreto Supremo No. 016-2024-JUS (en adelante, "Nuevo Reglamento" o "Reglamento"), se deroga el Decreto Supremo No. 003-2013-JUS y se aprueba el nuevo Reglamento de Protección de Datos Personales.

Estas normas se concibieron con el objetivo de proporcionar una estructura jurídica robusta y adecuada para garantizar el derecho fundamental a la protección de datos personales, previsto en el artículo 2.6 de la Constitución, en el contexto de la Sociedad de la Información.

En efecto, uno de los más importantes objetivos de la Ley de protección de datos personales y su Reglamento es brindar una respuesta a las necesidades producto

del acelerado avance tecnológico y la globalización. Como bien se señala en la exposición de motivos de la Ley:

> “La informática ha alterado la realidad económica , social y cultural en la que se basa la sociedad anterior, haciendo de la información el elemento clave del poder. A la luz de esta nueva realidad, la sociedad actual ha sido denominada como Sociedad de la Información. (…) urge entonces establecer garantías que tutelen la vida privada de las personas frente a la agresión de la informática (Exposición de motivos de la Ley).

Además de ello, estas normas buscan establecer un marco de protección adecuado para la protección del derecho a la autodeterminación informativa en el Perú frente a la tendencia internacional de regular este derecho. En efecto, de la exposición de motivos de la Ley, se puede inferir que los legisladores tenían el objetivo de evitar que el Perú quedará rezagado ante el avance legislativo en la materia en otros países:

> “Esta exigencia viene encontrando eco en diversas reuniones internacionales, en la legislación de múltiples países - mayoritariamente europeos - y en el desarrollo jurisprudencial de otros. A consecuencia de todo ello aparece la protección de datos personales como una respuesta organizada para el control de la informática.” (Exposición de motivos de la Ley).

Por último, antes de entrar al detalle de la regulación de la Ley de datos personales y su Reglamento, es importante señalar que estas normas tuvieron como eje y base el reconocimiento del derecho a la autodeterminación informativa como un derecho autónomo e independiente del derecho a la intimidad. De la revisión de la exposición de motivos de la Ley, es evidente que los legisladores buscaron enfatizar que el derecho a la autodeterminación informativa es un derecho de naturaleza activa, el

cual busca dotar al titular de los datos personales con el control de sus información, el cual se diferencia de la naturaleza pasiva del derecho a la intimidad:

> "(..) hoy en día, el derecho fundamental a la protección de los datos personales ha cobrado independencia y autonomía ante el derecho a la intimidad. En efecto, al actitud pasiva de simple defensa de nuestros datos personales -propia del derecho a la intimidad, pasa a complementarse con una postura activa, con la posibilidad de ejercer el control sobre el caudal de información que puede existir en los diferentes bancos de datos sobre nuestra persona" (Exposición de motivos de la ley).

Teniendo esto en claro, a continuación se desarrollaran las novedades de la Ley de protección de datos personales y su Reglamento: (i) el ámbito de aplicación, (ii) la definición de los términos en la cadena de tratamiento de datos y (iii) los principios rectores.

2.3.1. Establecimiento del ámbito de aplicación de la Ley de Protección de Datos Personales y su Reglamento

Uno de los aspectos más relevantes de la Ley y del Reglamento de datos personales es la delimitación del ámbito de aplicación de las normas en el Perú. Esto es fundamental pues se definen las circunstancias específicas en las cuales dichas normas son de aplicación y, aún más importante, se señalan los casos excepciones donde las normas no serán de aplicación. A continuación, detallaremos (i) la regla general de aplicación de la Ley y Reglamento de datos personales y (ii) las excepciones al ámbito de aplicación.

i. **Regla general:** La Ley de protección de datos personales establece en su artículo 3 que la misma 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" (Ley de protección de datos personales).

Del texto de la norma se pueden extraer las siguientes conclusiones: (i) la Ley presenta un enfoque en los bancos de datos; (ii) se detalla que la aplicación es tanto para entidades públicas y privadas; y (iii) se especifica que la aplicación la norma se dará siempre y cuando el tratamiento de los datos se de en territorio nacional.

Ahora bien, el Reglamento, acertadamente, amplía los supuestos establecidos por la Ley, proporcionando un enfoque integral y alineado nuestra regulación con los estándares internacionales de protección de datos. En efecto, el Reglamento, en su artículo IV, establece lo siguiente:

> "Artículo IV. Ámbito de aplicación
>
> 4.1 El presente Reglamento es de aplicación al tratamiento de los datos personales, aun cuando no se encuentren en un banco de datos personales.
>
> 4.2 Se aplica a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado, independientemente del soporte en el que se encuentren.
>
> 4.3 La existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones sobre datos personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente Reglamento.

4.4 Lo dispuesto en el párrafo precedente no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales". (Nuevo Reglamento)

Con esto, queda claro que el Nuevo Reglamento (i) plantea como núcleo del ámbito de aplicación el tratamiento de datos personales y no solo a los datos contenidos en bancos de datos, esto es fundamental pues alinea nuestros estándares de protección a los de la normativa norteamericana y europea; (ii) se especifica que la aplicación del Reglamento es tanto para entidades públicas, privadas o personas naturales, sin importar el soporte; es decir, abarca tanto los soportes digitales como los físicos; y (iii) el Reglamento toma en consideración que puede existir normativa sectorial para la protección de datos personales y se asegura de que estas sean compatibles con las disposiciones de la Ley y del Reglamento de datos personales, y en general, la normativa sectorial no debe afectar al derecho fundamental a la autodeterminación informativa.

Por último, es importante mencionar que el Nuevo Reglamento, en el artículo VI, establece un cambio importante: se establece un ámbito de aplicación extra territorial. Este cambio resulta relevante pues tanto la Ley de protección de datos personales como el Antiguo Reglamento de protección de datos antes limitaba su ámbito de aplicación a los bancos de datos y tratamientos de datos que se realizan solo en territorio peruano. Así, podemos concluir que la Ley y el Reglamento actual se aplican a los siguientes contextos:

a. Tratamientos de datos realizados en territorio peruano.

b. Tratamiento de datos personales fuera del territorio peruano, a nombre de un titular de banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento.

c. Tratamiento de datos personales cuyo responsable no esté establecido en el Perú, pero que utilice medios situados en el territorio peruano para el tratamiento de datos, excepto si estos son usados únicamente con fines de tránsito.

d. Todo caso en los que la ley peruana sea aplicable por disposición contractual o normativa internacional.

ii. Excepciones: Tanto la Ley como el Reglamento, son normas claras y puntuales para delimitar los supuestos en los que las mismas no son exigibles. En efecto, comenzando por la Ley de datos personales, está, en su artículo 3, señala explícitamente a qué escenarios no es aplicable.

1. Tratamientos de datos realizados por personas naturales destinados estrictamente a fines relacionados con su vida personal o familiar.

2. Tratamientos de datos realizados por la administración pública cuya finalidad sea imprescindible para el cumplimiento de sus competencias y que estén relacionadas a (i) defensa nacional, (ii) seguridad pública, (iii) actividades que coadyuven a actividades en materia penal.

No obstante estas excepciones, el Nuevo Reglamento, en su artículo V, realiza una importante precisión respecto a los casos de tratamiento de datos por parte de la administración pública: la Ley y Reglamento de datos personales si será aplicable a los tratamientos realizados por entidades pública cuando la finalidad del mismo no esté relacionado con el cumplimiento de sus competencias legales. Con ello, el Nuevo Reglamento amplía el espectro de protección, pues ahora actividades como el archivo administrativo de datos o investigaciones por parte de la administración

pública si estará sujeto a la regulación del marco legal de protección de datos personales.

2.3.2. Establecimiento de definiciones para los términos claves en la cadena de tratamiento de datos

La Ley de protección de datos personales y el Nuevo Reglamento trajeron consigo un glosario de definiciones, lo cual resultó beneficioso para el entendimiento de la misma. En efecto, la protección de datos personales es una materia que requiere un adecuado conocimiento técnico sobre la manera en se desenvuelve la cadena de tratamiento de datos. Tal como señala la Asociación Internacional de Profesionales de la Privacidad, entender la protección de datos implica no solo conocer la regulación sobre la misma, sino tener un entendimiento basto sobre la tecnología y el negocio detrás de la organizaciones que tratan datos personales (Swire & Kennedy-Mayo, 2020). Por lo tanto, la inclusión de este glosario coadyuva al correcto entendimiento e implementación de la Ley y el Reglamento de protección de datos personales.

Dentro de los términos incluidos, resultan indispensables los siguientes: (i) dato personal, (ii) dato sensible y (iii) tratamiento de datos. Ello es así, pues la protección de datos personales involucra el establecimiento de normas que gobiernan su tratamiento. Por lo que entender que constituye un dato personal, dato sensible y el propio tratamiento es clave.

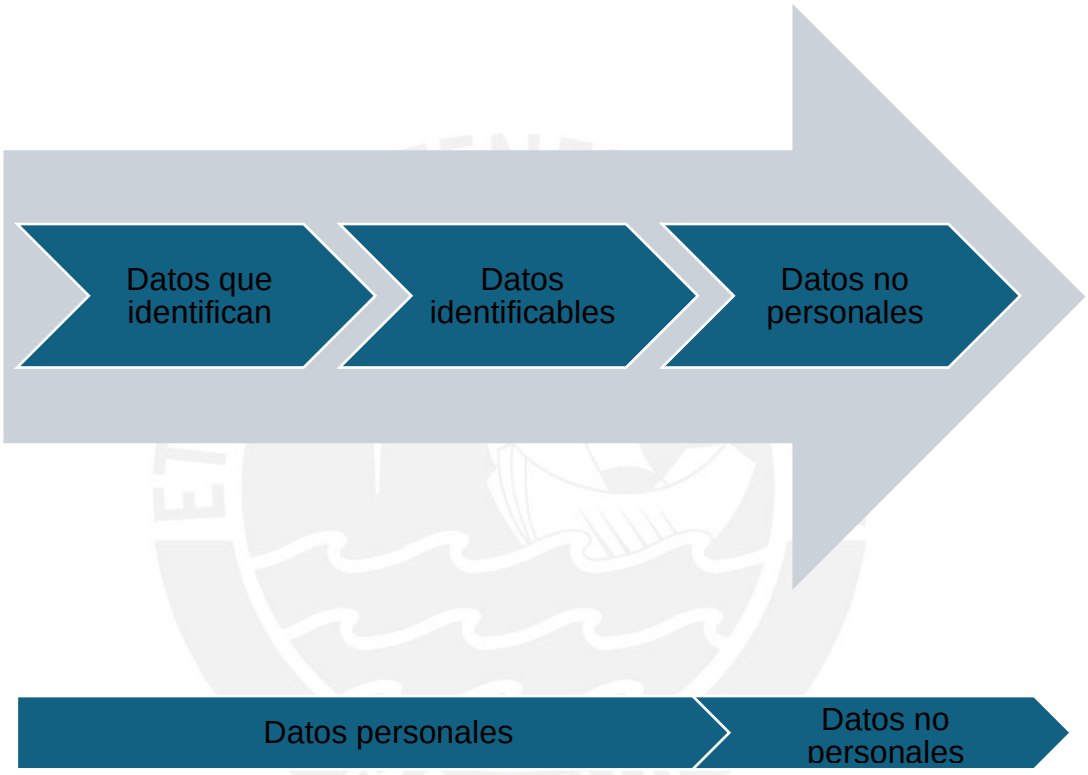
1. **Dato personal:** La Ley de protección de datos personales, en su artículo 2.4, define como dato personal a “toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados”. Por su parte, el Reglamento complementa esta definición al señalar en su artículo III.4 que dicha información puede ser “numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente

a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables".

Por lo tanto, "para entender que estamos frente a un dato personal se requiere que concurra un doble elemento: por una parte, que exista una información o dato; y de otra parte, que dicho dato o información pueda vincularse a una persona física identificada o identificable" (Zamudio, 2021). Queda claro que no todo dato es considerado un dato personal, necesita imprescindiblemente de la cualidad de identificar o hacer identificable a una persona. Una cuestión que es importante mencionar es que los datos no personales; es decir, información o datos que no son considerados como datos personales no están sujetos a regulación. Ahora bien, "si se eliminan los elementos de datos utilizados para identificar al individuo, los datos restantes se convierten en información no personal y las leyes de privacidad y protección de datos generalmente no se aplican" (Swire & Kennedy-Mayo, 2020).

Es necesario preguntarnos ¿cuándo estamos ante un caso de un dato que identifica o en uno donde el dato hace identificable a una persona? El Reglamento de datos personales, en el mismo artículo III.4, se ocupa de este tema: "se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados". Con ello, queda claro que (i) un individuo identificado es aquel cuya identidad puede determinarse con certeza y (ii) un individuo identificable es aquel que puede identificarse indirectamente mediante una combinación de diversos factores. La diferencia reside en que un dato que identifica no requiere de otros factores o datos para identificar a un sujeto; mientras que un dato que hace identificable, por sí mismo, no puede identificar a un individuo, requiere necesariamente de otros factores o datos.

Por otra parte, la Asociación Internacional de Profesionales de la Privacidad señala que “la diferencia entre datos personales y datos no personales depende en si la información es identificable” (Swire & Kennedy-Mayo, 2020). Por todo ello, resulta claro que la relación entre estos tres términos —información que identifica, información identificable y datos no personales— es la de una balanza:



Por último, la Asociación Internacional de Profesionales de la Privacidad precisa que la línea divisoria entre datos personales y datos no personales no es siempre clara y esta depende de cambios por parte de las normas que los regulan, pero sobre todo, depende del cambio tecnológico (Swire & Kennedy-Mayo, 2020).

2. **Dato sensible:** Los datos sensibles son una categoría especial de datos personales reconocida por la Ley y el Reglamento, debido a que los mismos requieren de un nivel de protección adicional debido a que su afectación

resulta extremadamente dañina para el titular de los mismos. Tal como menciona Zamudio, los datos sensibles son datos que requieren de una especial protección, en la medida que el tratamiento indebido de los mismos causa graves daños a la persona (Zamudio, 2021).

En esa línea, el Reglamento presenta un definición clara sobre los datos sensibles; en su artículo III.6, se señala lo siguiente: “Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad”. Asimismo, la Ley de protección de datos personales señala en su artículo 2.5 que los datos sensibles son “datos personales constituidos por datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual ”.

De ambas definiciones, se puede concluir que (i) los datos sensibles son datos personales pero no todo dato personal es un dato sensible y (ii) los datos sensibles gozan de dos niveles de protección: una por ser datos personales y otra exclusiva a los datos sensibles (D. J. Solove, 2023a).

3. **Tratamiento de datos:** La Ley de Datos Personales define al tratamiento de datos personales en su artículo 2.19 como cualquier operación o procesamiento de datos:

> “19. Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión,

> comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales".

De igual manera, el Reglamento se ocupa del término en su artículo III.23 señalando que se refiere a "cualquier operación o conjunto de operaciones, automatizados o no, que se realicen sobre los datos personales o conjuntos de datos personales".

De estas definiciones se concluye que el concepto de tratamiento de datos es uno de carácter amplio (Zamudio, 2021). En efecto, el enfoque adoptado en la Ley y el Reglamento es uno que engloba cualquier procedimiento desde la recolección hasta la eliminación de los datos personales. El tratamiento de datos se refiere a "casi cualquier cosa que alguien pueda hacer con la información personal" (Swire & Kennedy-Mayo, 2020). Este enfoque es afín al modelo europeo de protección de datos, en el artículo 4 del Reglamento General de Protección de Datos (GDPR) se define al tratamiento de datos como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales".

Ahora bien, es necesario hacer una precisión respecto a los procedimientos que incluye el tratamiento de datos. La Asociación Internacional de Profesionales de la Privacidad acuña el término Information Life Cycle o, en español, ciclo de vida de la información para referirse a los principales procesos involucrados en el tratamiento de datos dentro de distintas organizaciones: (i) recopilación, (ii) uso y almacenamiento y (iii) difusión (Swire & Kennedy-Mayo, 2020).

Además de entender los procesos que involucran el tratamiento de datos, es importante analizar a las partes que interactúan en estos procesos: (i) el titular de datos personales, (ii) encargados del tratamiento y (iii) responsable

del tratamiento. En el caso peruano, tanto la Ley como el Reglamento de protección de datos personales proporcionan una definición clara de estas partes.

a. **Titular de datos personales:** La Ley de datos personales en su artículo 2.16 precisa que el titular de los datos personales es aquella "persona natural a quien corresponden los datos". Es decir, es aquella persona cuyos datos son procesados, como por ejemplo un cliente de un banco o un paciente médico. De la redacción de la Ley, se concluye que las personas jurídicas están excluidas de la definición de titular de datos personales.

b. **Responsable del tratamiento de datos:** El Reglamento de datos personales, en su artículo III.22, define al responsable del tratamiento de datos como aquella persona natural o jurídica, privada o pública, que determina la finalidad del tratamiento de datos.

   Esta definición complementa a la Ley de datos personales, la cual no presentaba dentro del glosario de definiciones al responsable del tratamiento. Es necesario mencionar que la Ley presentaba esta definición, pero la asociaba con el titular del banco de datos. Esta correlación no era adecuada ni se alineaba a los estándares internacionales. Efectivamente, el GDPR tiene como definición de responsable a la persona o entidad que determinen los fines y medios del tratamiento.

   De hecho, el propio Reglamento en el artículo III.22 señala que la definición de responsable del tratamiento "no se restringe al titular del banco de datos, sino que incluye a cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales". Bajo este esquema de razonamiento,

puede darse el caso en el que el titular del banco de datos sea a su vez el responsable del tratamiento, pero también, es posible que estas dos figuras sean dos personas o entidad completamente distintas.

c. **Encargado del tratamiento de datos:** Por último, el encargado es aquella persona o entidad que ejecuta el tratamiento, bajo las direcciones y órdenes del responsable del tratamiento de datos. El artículo 2.7 de la Ley señala que el encargado es:

> "7. Encargado de tratamiento de datos personales. Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales".

En ese sentido, de la definición de la Ley podemos concluir lo siguiente: (i) el encargado puede ser una persona natural o una entidad pública o privada; (ii) el encargado realiza el tratamiento por encargo del titular del banco de datos; (iii) el encargado actúa limitado por el vínculo jurídico que tiene con el titular del banco de datos.

Esto tiene coherencia con la definición que presenta la Ley de datos personales sobre el titular del banco de datos, la cual señala en su artículo 2.17, que el titular es quien "determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad". No obstante, como señalamos anteriormente, dicha definición corresponde a la del responsable del tratamiento de datos. De hecho, ello es respaldado por el Reglamento, el cual en su artículo

III.10 precisa que el encargado “es la persona (…) que realiza tratamiento de datos por cuenta u orden del responsable de tratamiento o titular del banco de datos personales”.

Así, el encargado actúa como una extensión operativa del responsable del tratamiento y está ceñido a las órdenes de este último. Ahora bien, es necesario precisar que puede darse el caso que el encargado subcontrate a otra empresa para realizar el tratamiento de los datos. En esta situación, cada empresa u organización que actúen como encargados del tratamiento de los datos personales debe actuar en concordancia con las instrucciones y direcciones del responsable del tratamiento (Swire & Kennedy-Mayo, 2020).

Teniendo en cuenta todo ello, la relación entre estos tres actores puede graficarse de la siguiente manera:

2.3.3. Establecimiento de principios rectores

En principio, la Ley de protección de datos establece 8 principios rectores que orientan el tratamiento de datos personales: (1) principio de legalidad, (2) principio de consentimiento, (3) principio de finalidad, (4) principio de proporcionalidad, (5) principio de calidad, (6) principio de seguridad, (7) principio de disposición de recurso, y (8) principio de nivel de protección adecuado.

Tal como menciona Olivos, dichos principios deben utilizarse como (i) criterios interpretativos que coadyuven a la correcta aplicación de la ley, (ii) parámetros para la creación de nuevas disposiciones y (iii) para suplir los vacíos legales que puedan existir en la ley o el reglamento (Olivos, 2020). Esto a su vez, es respaldado por el artículo 12 de la Ley, el cual expresamente señala que "los principios rectores (…) sirven también como criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia".

Ahora bien, como también se menciona en el artículo 12 de la ley, esta lista de principios es enunciativa. De hecho, con la publicación del Reglamento se añadieron a la lista dos principios adicionales: (1) principio de transparencia y (2) principio de responsabilidad proactiva.

3. CAPÍTULO 2: La incompatibilidad entre el derecho a la protección de datos personales y las prácticas actuales de la sociedad de la información

3.1. El rol del consentimiento en la protección de datos personales

3.1.1. Orígenes del consentimiento y bases filosóficas

El consentimiento tiene un rol central en las interacciones humanas. Ello debido a su efecto transformativo de la moral. Tal como sostiene Hurd, la función principal del consentimiento es la de alterar la moralidad de la conducta de otra persona (Hurd, 1996). Así, por ejemplo, en una conversación, cuando una persona habla y

es interrumpida por otra, resulta un acto reprochable; sin embargo, si dicha persona tenía el consentimiento de la otra, ese mismo acto resulta moralmente aceptable. Lo relevante de este asunto es que el efecto transformativo del consentimiento no solo es aplicable en situaciones triviales como la conversación entre personas, sino que puede incluso ser la clave para determinar si estamos ante un acto ilegal o no.

En efecto, el consentimiento "convierte un allanamiento en una cena, una agresión en un apretón de manos, robo en un regalo, una invasión a la privacidad en un momento íntimo, y una apropiación comercial del nombre en una biografía" (D. J. Solove, 2023b). Tal como menciona Marmor, "usar algo que me pertenece, incluido mi cuerpo (o el manuscrito de mi libro o lo que sea), sin mi consentimiento, está mal y puede ciertamente violar mis derechos; no necesitamos apelar a la privacidad para explicar qué es lo que está mal en ello" (Marmor, 2015).

Hurd denomina a este efecto: la "magia moral" del consentimiento (Hurd, 1996). Bajo esa premisa, el consentimiento permite que una persona pueda realizar actos que sin él serían considerados moralmente erróneos (Schermer et al., 2014). De igual manera, Kleinig agrega que, en términos más amplios, el consentimiento tiene el potencial de transformar las expectativas y reglas sociales (Kleinig, 2010). Esto quiere decir que el consentimiento no solo tiene influencia en las dinámicas sociales entre individuos, sino en también entre grupos sociales. Ello es así, pues el consentimiento confiere legitimidad. Como menciona Solove, el consentimiento otorga legitimidad a los actos, por lo que actos que de otra manera serían considerados inmorales o ilegales, no lo son. Dicha legitimidad, otorga poder (D. J. Solove, 2023b).

Además, el consentimiento actúa como una forma de expresión de la autonomía personal. Rawls señala que la autonomía de una persona se manifiesta cuando la elección de su accionar le pertenece solo a él y dicho accionar es reflejo de su naturaleza racional, libre e igual (Rawls, 1999). En otras palabras, la autonomía no solo reside en la capacidad de tomar decisiones, sino esta implica que dichas

decisiones sean guiadas por tres aspectos fundamentales: (i) racionalidad, (ii) libertad y (iii) igualdad. Así, al ser el consentimiento una expresión de nuestra libertad, es entonces una expresión de nuestra autonomía (Schermer et al., 2014).

Por otra parte, el consentimiento posee una función práctica esencial en la interacción humana: no solo se limita a la obtención de una mera aprobación, este sirve como una señal de alerta. Una solicitud de consentimiento otorga a los individuos un momento de reflexión activa sobre las consecuencias de su decisión; es decir, actúa como "una advertencia de que se producirá una transformación moral potencialmente dañina o legalmente significativa que requiere la atención del individuo" (Schermer et al., 2014). Así, el consentimiento no solo actúa como un catalizador moral y como una expresión de la autonomía personal, sino que asegura que los individuos tomen decisiones de manera consciente.

Ahora bien, el consentimiento es importante en diversas esferas de nuestra vida y resulta una pieza esencial en varías áreas del derecho. Tal como menciona Solove, el consentimiento es un concepto trasversal a todas las áreas del derecho; así, por ejemplo, permea desde la formación de los contratos hasta la consumación de delitos como la agresión sexual (D. J. Solove, 2023b). En estos distintos contextos, el significado y aplicación del consentimiento varía. En la presente investigación, nos centraremos en el consentimiento en el contexto de la protección de datos personales.

El consentimiento en el contexto de protección de datos personales es una base que legitima el procesamiento de los mismos. Es decir, es un forma de autorización autónoma, en la cual el titular de información brinda al responsable del tratamiento la facultad de procesar sus datos (Schermer et al., 2014). Así, en teoría, el consentimiento en materia de protección de datos personales cumple con ser: (i) un acto moralmente transformador; (ii) una forma de expresión de la autonomía personal; y, (iii) ser una señal de alerta. A continuación, se desarrolla cada uno de estos aspectos:

i. Resulta ser un acto moralmente transformador pues el consentimiento transforma lo que es considerado un acto moralmente reprochable como lo es el uso indebido de la información personal, en uno legítimo cuando el titular de dichos datos brinda su autorización. Como menciona Bart, la lógica detrás de las leyes de protección de datos personales es que, mediante un acto moralmente transformador como el consentimiento, se otorgue legitimidad al tratamiento de la información de las personas (Schermer et al., 2014).

ii. Cumple con ser una forma de expresión de la autonomía personal debido a que, mediante el consentimiento, se pretende proteger el derecho a la autodeterminación informativa. En efecto, Westin señaló que el consentimiento en el contexto de datos personales pretende proteger el derecho de las personas a decidir sobre el futuro de su información personal, es decir, pretende proteger el derecho a autodeterminación informativa (Westin, 1968). Así, el consentimiento busca que el individuo tome decisiones sobre sus datos de manera libre, informada y en sintonía con sus propios valores personales.

iii. Por último, cumple el objetivo práctico de ser una señal de alerta, debido a que, en la materia de protección de datos personales, se utiliza el consentimiento como una herramienta para dar alerta a los titulares de los datos personales que su información está siendo tratada. En otras palabras, mediante el consentimiento se pretende otorgar una pausa activa en la cual los individuos pueden reflexionar acerca de las implicancias del tratamiento de datos que se va a realizar.

Hasta este punto deben quedar en claro las siguientes ideas respecto del consentimiento en materia de protección de datos personales: (i) el consentimiento legitima el tratamiento de datos personales, y (ii) al legitimar los tratamientos, su rol

toma un papel central. Teniendo ello en cuenta, es importante introducir la idea de la “autogestión de la privacidad” como paradigma de los sistemas de protección de datos personales. Este paradigma tiene como idea central que las legislaciones de protección de datos personales funcionan en base a la siguiente lógica: se busca el empoderamiento del titular de los datos personales para que este pueda tomar las decisiones respecto de la gestión de su información. En efecto, esta idea es propuesta por Solove, el cual menciona que, en la actualidad, el paradigma que rige la protección de datos personales está basado en que la ley otorgue un conjunto de derechos a los individuos mediante los cuales este pueda ejercer un poder y control sobre sus datos (D. Solove, 2014).

Mediante este paradigma, el enfoque está puesto en el titular de los datos personales. Las leyes de privacidad buscan reforzar sus capacidades para que este pueda ejercer un verdadero control sobre su información. Los países que optan por este modelo de protección tienen al consentimiento como eje central. En efecto, Solove señala que el consentimiento es la base del paradigma de la autogestión de la privacidad, en donde se mantiene neutralidad sobre el fondo del consentimiento y se pone énfasis en si se realiza la autorización o no (D. Solove, 2014). En otras palabras, las normas de protección de datos no califican las prácticas que se pretenden consentir. En lugar de ello, se preocupan en que el consentimiento del titular sea válido. Así, por ejemplo, si un sitio web recopila información acerca del tiempo en pantalla de las personas, la norma no regula si dicha recopilación es buena o mala, sino se preocupa por regular si las personas están informadas y presentaron un consentimiento válido acerca de la recopilación.

Ahora bien, el concepto de la autogestión tiene sus raíces en los *Fair Information Practices Principles* (FIPP) (Gellman, 2014). Estos son principios que tienen como finalidad guiar las practicas de recopilacióm, almacenamiento y tratamiento de las información personal (Dixon, 2006). Estos principios son la base sobre la cual los países han regulado el procesamiento de la información personal; si bien existe variación en sus definiciones debido a la región o país en particular, lo cierto es

existe un similitud en cuanto a los temas centrales y muy pocas excepciones respecto de su aplicación (Swire & Kennedy-Mayo, 2020).

Estos principios han servido como guía en la regulación del tratamiento de la información personal desde la década de 1970 (D. Solove, 2014). Las codificaciones más importantes de los FIPP son: (i) los FIPP del Departamento de Salud, Educación y Bienestar de los Estados Unidos en 1973; (ii) las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre la protección de la privacidad y los flujos transfronterizos de 1980; (iii) la Convención 108 del Consejo de Europa sobre la protección de la información personal de 1981; (iv) el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC) del 2004; y, (v) la Resolución de Madrid sobre los estándares internacionales de protección de datos de 2009 (Swire & Kennedy-Mayo, 2020).

Si bien los principios establecidos en estos cinco cuerpos normativos varía, existe coincidencia en las siguientes categorías: (i) sobre los derechos, (ii) sobre el control de la información, (iii) sobre el ciclo de vida de la información y (iv) sobre el manejo de la información (Swire & Kennedy-Mayo, 2020). Para la presente investigación nos centraremos en los puntos en común sobre los derechos del titular de los datos personales. Así, de una revisión de las normas tenemos que el consentimiento se erige como el punto central para la gestión de la información personal:

Norma	Regulación sobre el consentimiento
Departamento de Salud, Educación y Bienestar de los Estados Unidos en 1973	“Debe existir una manera para que una persona evite que la información sobre ella obtenida para un propósito se utilice o se ponga a disposición para otros fines sin su consentimiento”
Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de 1980	“Debe haber límites a la recopilación de datos personales y dichos datos deben obtenerse por medios legales y justos y, cuando corresponda, con

	el conocimiento o consentimiento del titular de los datos”
Convención 108 del Consejo de Europa sobre la protección de la información personal de 1981	“Los datos personales que sean objeto de tratamiento automático deberán: (a) Obtenerse y tratarse de manera leal y lícita”
Marco de Privacidad del APEC del 2004	“La recopilación de información personal debe limitarse a la información que sea pertinente a los fines de la recopilación y dicha información debe obtenerse por medios legales y justos y, cuando corresponda, con notificación o consentimiento de la persona interesada”
la Resolución de Madrid sobre los estándares internacionales de protección de datos de 2009	“Como regla general, los datos personales solo podrán ser tratados en alguna de las siguientes situaciones: a. Tras obtener el consentimiento libre, inequívoco e informado del interesado”

Fuente: Elaboración propia

Debe quedar claro entonces que el paradigma de la autogestión de la privacidad cuenta con gran aceptación en los sistemas de regulación de protección de datos. Como menciona Solove, las normas que regulan los FIPP varían en cuanto a especificidades como los datos a recopilarse o la forma en la que estos pueden ser usados; sin embargo, los FIPP presentan una clara tendencia a permitir las formas de recolección, almacenamiento, tratamiento y divulgación de datos siempre que medie el consentimiento válido del titular de los datos personales (D. Solove, 2014).

3.1.2. El consentimiento como piedra angular en los diversos sistemas de protección de datos personales

Como se analizó en el apartado anterior, el consentimiento en el marco de la protección de datos personales actúa como una base de legitimación. Sin embargo, es necesario aclarar que el consentimiento no es solo una base cualquiera en el sistema de protección de datos personales; por el contrario, es el eje central en dicho sistema. Las diversas legislaciones a nivel mundial coinciden en un punto: el consentimiento es el requisito mínimo para cualquier tratamiento de datos personales (Olivos, 2020).

A nivel mundial, el desarrollo de los sistemas de protección han variado dependiendo de la región geográfica y el desarrollo económico. No obstante, como menciona la Asociación Internacional de Profesionales de la Privacidad, los diferentes enfoques de protección pueden agruparse en dos categorías: (i) el modelo integral, el cual se caracteriza por que las leyes de protección de datos establecen requisitos aplicables a todos lo sectores de la economía (Swire & Kennedy-Mayo, 2020); y (ii) el modelo sectorial, el cual se caracteriza por que la regulación sobre protección de datos no es uniforme, por el contrario, esta responde a las necesidades de los distintos sectores de la economía, como lo son la salud o las finanzas (Swire & Kennedy-Mayo, 2020).

Es importante mencionar que la aplicación de estas categorías no es excluyente. En la práctica, estos modelos coexisten y los diferentes países combinan elementos de ambos enfoques para la regulación sobre los datos personales. No obstante, la división realizada para esta investigación resulta esencial para ilustrar de manera didáctica las características y principios que subyacen a cada modelo.

Ahora bien, la elección de uno u otro modelo depende de la confianza en las leyes gubernamentales frente a los estándares desarrollados por la propia industria (Swire & Kennedy-Mayo, 2020). Lo cierto es que a pesar de las diferencias de cada uno

de estos enfoques de regulación, en la base de los mismos se encuentra un elemento en común: la confianza en el consentimiento, ya sea este expreso o implícito (D. J. Solove, 2023b). Es por ello que, en la presente sección de la investigación, se desarrollará el funcionamiento de estos modelos de protección, destacando sus diferencias y puntos en común.

3.1.2.1. El modelo integral

El modelo integral se caracteriza por dos aspectos: (i) la existencia y aplicación de una norma de protección de datos que centraliza la regulación a lo largo de los diferentes sectores de la economía, y (ii) la existencia de una autoridad central responsable de la aplicación y cumplimiento de la regulación. En efecto, los países que siguen el modelo integral de regulación tienden a tener leyes de protección de datos personales que regulan el tratamiento de datos personales de manera uniforme; es decir, sin hacer distinción entre los sectores públicos y privados (Swire & Kennedy-Mayo, 2020). Por otra parte, los modelos integrales presentan como elemento característico la presencia de una autoridad o entidad encargada del cumplimiento de las leyes, las investigaciones sobre presuntas infracciones, e incluso, en muchos casos, tiene la función de guiar y educar a la ciudadanía sobre aspectos vinculados a la protección de datos (Swire & Kennedy-Mayo, 2020).

Un ejemplo claro de este modelo es el de la Unión Europea. En este caso, existe una norma que unifica los estándares de protección de datos personales: el Reglamento General de Protección de Datos (RGPD). Bajo este esquema, no existen normas particulares que varían dependiendo de cada sector de economía, el RGPD es de aplicación general (artículo 2). Asimismo, bajo este esquema, existe una entidad encargada del cumplimiento del RGDP: la Autoridad de Protección de Datos (APD) (artículo 51).

Este modelo se caracteriza por legitimar el tratamiento de datos personales en base a distintos elementos. Por ejemplo, en la Unión Europa se establece en el artículo

6 del RGDP que el tratamiento será lícito solo en caso de cumplir con al menos una de las bases de legitimación: (i) consentimiento, (ii) ejecución de un contrato, (iii) obligación legal, (iv) intereses vitales, (v) interés público y (vi) intereses legítimos. Como menciona Solove, si bien en la Unión Europea se utilizan estas seis bases de legitimación, lo cierto es que muchas otras naciones que siguen el modelo regulan como única base de legitimación al consentimiento (D. J. Solove, 2023b).

Ahora bien, este consentimiento es uno de tipo afirmativo. Este tipo de consentimiento es conocido como “opt-in” y requiere una acción clara de parte del titular de los datos personales que exprese una autorización (Swire & Kennedy-Mayo, 2020). En esta misma línea, Solove indica que el consentimiento expreso requiere un acto claro y voluntario que indique aceptación (D. J. Solove, 2023b). Así, por ejemplo, en el caso de la Unión Europea, el RGDP señala en su artículo 4.11 que el consentimiento deberá ser uno libre, específico, informado e inequívoco. Debe quedar claro que este tipo de consentimiento es una de las formas más estrictas que existen en los sistemas de protección de datos (D. J. Solove, 2023b).

3.1.2.2. El modelo sectorial

Por otra parte, el modelo sectorial se caracteriza por lo siguiente: (i) la normativa sobre protección de datos se adapta a cada sector de la economía, y (ii) no existe una sola autoridad encargada del cumplimiento de las normas de protección de datos. La norma en este tipo de modelo se retroalimenta de las necesidades de cada sector de la industria (Swire & Kennedy-Mayo, 2020). De igual manera, la Asociación Internacional de Profesionales de la Privacidad argumenta que, en el modelo sectorial de protección de datos, cada sector del mercado está regulado de manera independiente y el mismo carece de un régimen regulatorio unificado para todos los sectores económicos (Swire & Kennedy-Mayo, 2020).

El ejemplo más claro de este modelo es el caso de Estados Unidos. En efecto, en dicho país son varias las agencias reguladoras las encargadas de la apliación y

supervisión de las normas de protección. Por lo mismo, no exite una sola ley que regule esta materia; es decir, el marco normativo sobre protección de datos está fragmentado en las diversas normas que regulan cada sector particular de la economía. Así, si bien en Estados Unidos, la Comisión Federal de Comercio (FTC) tiene la función de regular y supervisar el tratatamiento de datos personales en el contexto de las practicas comerciales[3], esta coexiste con la Oficina de Protección Financiera del Consumidor (CFPB), encargada de regular el tratamiento de datos en el sector financiero[4], con el Departamento de Salud y Servicios Humanos (HHS)[5], respecto del sector salud, entre otros.

Ahora bien, al igual que vimos en el caso del modelo integral, el consentimiento tiene un rol central en la protección de datos en este modelo. Según Solove, para legitimar el tratamiento de datos personales utilizan el enfoque de "notificación y elección" (*notice-and-choice*), el cual tiene como eje al consentimiento implícito (D. J. Solove, 2023b). Este tipo de consentimiento, también conocido como "opt-out", implica que la autorización para el tratamiento de datos está implícita en el hecho de que la persona no se oponga al uso o divulgación (Swire & Kennedy-Mayo, 2020). Es decir, se presume que una persona ha consentido a menos que la misma exprese explícitamente su desacuerdo.

Así, normalmente, en este tipo de modelo se requiere que las empresas y organizaciones notifiquen a los titulares de los datos personales su política de privacidad. Mediante esta notificación se les brinda la posibilidad de que los mismos se opongan a dicha política, y, en caso de no hacerlo, se concluye que los titulares están consintiendo el tratamiento de su información conforme a lo especificado en la política de privacidad (D. J. Solove, 2023b).

[3] Sección 5 de la Ley del Comisión Federal de Comercio (1938)
[4] Ley Dodd-Frank de Reforma de Wall Street y Protección del Consumidor (2000)
[5] Health Insurance Portability and Accountability Act (1996)

3.1.3. La regulación del consentimiento en el contexto peruano

Teniendo en cuenta lo anterior, surge la pregunta sobre el modelo de regulación en materia de datos personales en el Perú. Es por ello que en este apartado analizaremos si en el Perú se sigue el modelo de regulación sectorial o el modelo integral. Posteriormente, se detallarán los aspectos que caracterizan al consentimiento en el contexto peruano.

En la Ley de Protección de Datos, en su artículo 3, se hace mención expresa de que la misma rige a todo tratamiento de datos, tanto del sector público, como del privado. Esto es corroborado por el Reglamento cuando, en su artículo IV, señala que es de aplicación a cualquier modalidad de tratamiento de datos, "ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado". Asimismo, se recalca que la existencia de normas o regímenes particulares o especiales no excluye la aplicación de la Ley y el Reglamento. Así, resulta claro que la norma que regula el procesamiento de datos en el Perú es una que uniformiza la regulación a través de todos los sectores de la economía. Esta característica acerca al sistema peruano al modelo de regulación integral.

Por otra parte, mediante el artículo 32 de la Ley de Protección de Datos, se crea la Autoridad Nacional de Protección de Datos (ANDP), la cual es la entidad encargada de velar por el cumplimiento del objeto y demás disposiciones de la Ley y de su Reglamento. En 2017, mediante el Decreto Supremo No. 019-2017-JUS, se creó la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD). No obstante, ello no quiere decir que existan dos organismos diferentes encargados del cumplimiento y supervisión del régimen de protección de datos en el Perú. Como bien menciona Olivos, la DGTAIPD es "el órgano de línea del Despacho Viceministerial de Justicia encargado de ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública, así como de ejercer la Autoridad Nacional de Protección de Datos Personales" (Olivos, 2020). En efecto, esto es respaldado por el artículo 2 del Decreto Legislativo No. 1353, el

cual señala lo mismo. Queda claro entonces que en el Perú existe una sola entidad que centraliza el poder cumplimiento y supervisión de la regulación sobre datos personales.

Por lo tanto, es posible afirmar que en el Perú el régimen de protección de datos personales toma el modelo integral de regulación como base:

Modelo Integral	Unión Europea	Perú
1. La existencia y aplicación de una norma de protección de datos que centraliza la regulación a lo largo de los diferentes sectores de la economía.	Reglamento General de Protección de Datos (RGPD).	Ley No. 29733 – Ley de Protección de Datos Personales y su Reglamento.
2. La existencia de una autoridad central responsable de la aplicación y cumplimiento de la regulación.	Autoridad de Protección de Datos (APD).	Autoridad Nacional de Proteción de Datos Personales.

Fuente: Elaboración propia

Ahora bien, en este punto es necesario desarrollar las características que presenta el consentimiento en el régimen de protección de datos personales en el Perú. Para Zamudio, el consentimiento es la piedra angular sobre la que el ordenamiento jurídico peruano recae, pues mediante el mismo se legitima el tratamiento de información personal y es el eje en torno al cual toda la regulación gira (Zamudio, 2021). Esta afirmación guarda coherencia con lo señalado en la Ley de Protección de Datos y en su Reglamento.

En efecto, por parte de la Ley de Protección de Datos, en el artículo 13.5, en relación al tratamiento de datos personales, se señala que “los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al

respecto". Por su parte, en el artículo 14[6] de la norma se establecen los casos excepcionales en los cuales se puede realizar el tratamiento de datos personales sin necesidad del consentimiento del titular de la información. De igual manera, en el artículo 1.1 del Reglamento se establece lo siguiente:

[6] "Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con elpropósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley".

> “1.1 El titular del banco de datos personales o quien resulte como responsable del tratamiento, debe obtener el consentimiento para el tratamiento de los datos personales, de conformidad con lo establecido en la Ley y en el presente Reglamento, salvo los supuestos establecidos en el artículo 14 de la Ley, en cuyo numeral 1 queda comprendido el tratamiento de datos personales que resulte imprescindible para ejecutar la interoperabilidad entre las entidades públicas”

En ese sentido, es claro que el régimen peruano gira en torno al consentimiento del titular. Si bien se establecen supuestos en los cuales es posible realizar el tratamiento de los datos sin que medie consentimiento, estos son establecidos como excepciones. En esta línea, Eguiguren señala que la Ley de Protección de Datos establece una regla general y un régimen de excepción a la misma (Eguiguren Praeli, 2015).

Ahora bien, en la normativa peruana se establecen requisitos para que dicho consentimiento sea válido. Es decir, en el régimen de protección de datos de Perú, el énfasis está en determinar si el consentimiento es válido o no. Con ello, es posible afirmar que la tendencia en el contexto peruano sigue lo planteado por Solove: se mantiene neutralidad sobre el fondo del consentimiento y se enfoca en determinar si la autorización es válida (D. Solove, 2014).

Así, en el artículo 13.5 de la Ley de Protección de Datos se señala que “el consentimiento debe ser previo, informado, expreso e inequívoco”. Por su parte, en el artículo 2 del Reglamento se establecen las características que debe tener todo consentimiento para ser considerado válido:

> “Artículo 2. Características del consentimiento válido
> El consentimiento para el tratamiento de datos personales es válido si se cumplen las siguientes características:

1. Libre
2. Previo
3. Expreso e inequívoco
4. Informado”.

Resulta claro, entonces, que, en el sistema de protección de datos personales en el Perú, el consentimiento es equiparable al caracterizado por Solove: un modelo de consentimiento expreso. Como mencionamos anteriormente, este consentimiento requiere de una acción específica y clara que exprese la autorización por parte del titular de los datos para el tratamiento de los mismos (Swire & Kennedy-Mayo, 2020). Una vez establecido esto, es necesario desarrollar cada una de las características que hacen al consentimiento válido en el Perú.

1. **El consentimiento debe ser libre:** En el Perú, se contempla que se considera libre el consentimiento solo si este es prestado de manera voluntaria y no haya error, mala fe, violencia o dolo. En efecto, en el artículo 3 del Reglamento se señala que “se considera que el consentimiento del titular de los datos personales es libre cuando se otorgue sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales”.

   En esa línea, Gil precisa que la exigencia planteada garantiza que el titular de los datos personales pueda “elegir una opción real” (Gil, 2016). En efecto, mediante este requisito se procura que la voluntad de las personas no esté afectada por factores externos como la presión o coacción (Hidalgo Zamora, 2020), asegurando con ello que el titular tenga un verdadero control sobre las decisiones en torno a sus datos.

   Por otra parte, en el mismo artículo 3 se señalan otros dos aspectos a tomar en cuenta: (i) no se considera libre el consentimiento otorgado cuando este está condicionado a la “prestación de un servicio o la advertencia o la

amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido", y (ii) se considera libre el consentimiento otorgado a pesar de que medie "la entrega de obsequios o beneficios al titular de los dato", excepto en el caso de menores de edad.

2. **El consentimiento debe ser previo:** Esta característica se refiere a que el consentimiento para ser válido debe otorgarse en un momento específico: antes del tratamiento de datos. En efecto, el artículo 4 del Reglamento señala que el consentimiento debe ser solicitado con anterioridad a la recopilación de tales datos. Asimismo, en el scaso de que se plantee un nueva finalidad de uso de datos previamente consentidos, se requerirá de un nuevo consentimiento de parte del titular, autorizando este nuevo uso. Esto planteado por el mismo artículo 4 de la siguiente manera: "el consentimiento debe ser solicitado al titular de los datos personales (…) antes del tratamiento distinto a aquel por el cual ya se recopilaron dichos datos".

   Esto último guarda relación con el principio de finalidad establecido en el artículo 6 de la Ley de Protección de Datos, el cual establece que los datos personales deben ser recopilados para una finalidad determinada y el tratamiento de los mismos no deberá extenderse a otra finalidad que no haya sido la establecida al momento de su recopilación". Como menciona Gil, en caso de cambiar la finalidad del tratamiento de los datos personales, se deberá obtener un nuevo consentimiento (Gil, 2016).

   Por último, es importante señalar que, si bien se ha establecido un momento específico en el cual se debe otorgar el consentimiento, lo cierto es que la revocación del mismo no está sujeta a ningún plazo temporal. Es decir, el titular puede revocar su consentimiento en cualquier momento, ello en concordancia con lo establecido en el artículo 10 del Reglamento.

3. **El consentimiento debe ser expreso:** Además de ser libre y previo, el consentimiento debe expresarse claramente a través de medios que permitan evidenciar la voluntad del titular. El artículo 5 del Reglamento precisa que será necesario que el consentimiento se haya exteriorizado a través de una acción que demuestre una aceptación concreta, directa y explícita respecto al tratamiento de los datos personales.

   Además, el Reglamento adecuadamente señala cuáles son las formas mediante las que se puede expresar el consentimiento: (i) verbalmente, es decir, de manera oral o cualquier tecnología que permita la interlocución oral; (ii) escrita, mediante cualquier documento o medio electrónico con su firma autógrafa, electrónica o digital, huella dactilar, entre otros; (iii) mediante canales digitales, incluyendo cualquier mecanismo electrónico como "la firma electrónica, pulsando un botón o una casilla en un sitio web, o enviando un correo electrónico de confirmación" (Gil, 2016); y (iv) otros conforme a ley, es decir, cualquier otro medio conforme a lo establecido en el artículo 141 del Código Civil.

4. **El consentimiento debe ser inequívoco:** Esta característica implica que el consentimiento debe ser otorgado de manera tal que no exista duda alguna respecto de la intención del titular de los datos personales. En efecto, el inciso 2 del artículo 5 del Reglamento establece que "el consentimiento es inequívoco cuando se pueda apreciar que los actos materiales por parte del titular del dato personal manifiestan la aceptación indubitable respecto a un determinado tratamiento de sus datos personales, sin generar posibilidad de duda o equivocación".

   Al respecto Gil señala que este requisito genera una obligación a los responsables del tratamiento de crear mecanismos y procedimientos rigurosos que aseguren una manifestación indubitable del consentimiento (Gil, 2020). Así, por ejemplo, el uso de casillas pre marcadas no es

compatible con esta característica, pues en el sistema peruano se requiere de una acción afirmativa y clara que demuestre el consentimiento del titular de la información. En efecto, debido a la incertidumbre que genera la inacción, no es posible considerar el hecho de no desmarcar o desplazar un casilla premarcada como una forma de consentimiento.

5. **El consentimiento debe ser informado:** Por último, el artículo 6 del Reglamento señala que el consentimiento para ser informado requiere que al titular de los datos se le comunique claramente y con lenguaje sencillo los alcances, las condiciones y las finalidades específicas del tratamiento[7]. Con ello, se busca que el titular, antes de consentir, comprenda plenamente las ventajas y riesgos asociados al tratamiento de sus datos (Hidalgo Zamora, 2020).

   Igualmente, es importante señalar que esta característica constituye a su vez un derecho del titular de los datos personales (Zamudio, 2021). En efecto, como se establece en el artículo 18 de la Ley de Protección de Datos, "el titular de los datos personales tiene el derecho a ser informado a ser informado en forma detallada, actualizadas sencilla, expresa, inequívoca y de manera previa" sobre las particularidades del tratamiento de sus datos.

[7] "Artículo 6. Consentimiento informado
6.1. Cuando los datos personales son obtenidos directamente del titular de los datos personales se le debe comunicar de forma clara, con lenguaje sencillo, cuando menos lo siguiente:
1. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos, y, cuando corresponda, del representante.
2. La finalidad o finalidades del tratamiento a las que sus datos son sometidos.
3. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
4. La existencia e identificación del banco de datos personales en que se almacenarán, cuando corresponda.
5. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
6. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
7. En su caso, la transferencia nacional e internacional de datos que se efectúen.
8. La existencia de decisiones automatizadas, incluida la elaboración de perfi les, y se transmita información relativa a las consecuencias para el titular del dato personal.
9. El plazo de conservación de los datos personales.
10. Los mecanismos para el ejercicio de los derechos del Título III de la Ley. 6.2. (…)"

> Por último, es necesario mencionar que esta información debe proveerse con independencia de si los datos han sido obtenidos directamente del interesado o a través de terceros. Esto es así pues un dato puede ser obtenido directamente del titular; por ejemplo, cuando este llenó un formulario para registrarse a una red social. Sin embargo, actualmente esta no es la única forma de obtener datos personales; existen situaciones en las que las compañías o entidades adquieren los datos personales de las personas sin la intervención directa de estas. Por ejemplo, mediante bases de datos comerciales o transferencias de datos entre empresas. En estos casos, el nuevo responsable tiene la obligación de informar adecuadamente a las personas sobre el tratamiento a realizar (Gil, 2020). En el inciso 2 del artículo 6 del Reglamento se especifica que "el titular del banco de datos o quien resulte responsable debe estar en condiciones de informar, en el primer contacto y a requerimiento del titular de los datos personales, la fuente de recopilación de los datos personales".

Es importante señalar que estas características deben estar todas presentes para que el consentimiento sea válido. De hecho, en el inciso 3 del artículo 5 del Reglamento se señala que incluso cuando el consentimiento sea expreso, esto no exime del cumplimiento de los otros requisitos. En otras palabras, para considerar que estamos ante un consentimiento válido se exige la concurrencia simultánea de estas cinco características.

Ahora bien, en algunas otras legislaciones, como la de la Unión Europea, se regula expresamente el requisito de especificidad como parte de las condiciones para que el consentimiento sea considerado válido[8]. Sobre esta caracterísa, Gil señala que

[8] Artículo 4: Definiciones
A efectos del presente Reglamento se entenderá por: (…) 11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen (…)"

esta implica lo siguiente: (i) se deben especificar el alcance y consecuencias de tratamiento de datos, lo que signfica que el titular debe conocer exactamente cuales, cuales son los datos a recopilarse y los motivos detrás del procesamiento; y (ii) cualquier cambio en los fines del tratamiento deberá ser comunicado inmediatamente al titular de los datos y deberá exigirse que este brinde nuevamente su consentimiento ante las nueva condiciones (Gil, 2020).

Si bien este requisito no está regulado expresamente en el ordenamiento jurídico peruano, lo cierto es que el mismo forma parte de las condiciones que ha de presentar el consentimiento para ser considerado válido. Ello es así pues este requisito deriva del principio de finalidad regulado en el artículo 6 de la Ley de Protección de Datos:

> "Artículo 6. Principio de finalidad
> Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización".

Finalmente, en situaciones de tratamientos de datos sensibles, la normativa peruana establece una condición adicional: el consentimiento debe ser dado por escrito. En efecto, en el artículo 8 del Reglamento se establece que "tratándose de datos sensibles, además del cumplimiento de los requisitos para el consentimiento válido, este debe ser otorgado por escrito, a través de su firma manuscrita, digital, electrónica o cualquier otra modalidad". El establecimiento de este requisito adicional es "una manifestación del objeto de una protección reforzada a esta categoría de datos personales" (Zamudio, 2021).

3.2. El Big Data

3.2.1. Fases de desarrollo del Big Data

En el primer capítulo de esta investigación se estableció la siguiente idea: actualmente vivimos en la sociedad de la información y, dentro de este contexto, la tecnología del Big Data se ha convertido en una de las formas de procesar datos más populares. Por ello, en este apartado se desarrollará el funcionamiento de esta nueva tecnología con el objetivo de comprender cómo se procesa la información en esta nueva era.

Como menciona Alfonso Sánchez, una característica de la Sociedad de la Información es el esfuerzo por convertir la información en conocimiento; mientras más información es creada, mayor es la necesidad de convertirla en conocimiento (Alfonso Sánchez, 2016). En este punto, el Big Data se crea como una alternativa para solucionar los problemas generados ante la necesidad de procesar y extraer información de la inmensa cantidad de datos generados diariamente (García et al., 2016).

La primera empresa en desarrollar un modelo de Big Data para solucionar el problema del almacenamiento y tratamiento de grandes volúmenes de información fue Google, el cual diseñó el modelo MapReduce en 2003. Ante el problema de procesar información de manera eficiente, debido a la generación incansable de datos provenientes de los sitios web que administraba Google, este decidió desarrollar una solución propia con una estrategia diferente (Niño & Illarramendi, 2015). Este modelo de Big Data se convirtió en la plataforma de datos masivos pionera y el paradigma para el procesamiento de datos masivos (García et al., 2016).

Es importante conocer cómo funciona el MapReduce, pues el mismo sirvió de base para posteriores modelos de Big Data. Así, el modelo MapReduce utilizó dos conceptos fundamentales: (i) la creación de ficheros de información, y (ii) la creación

de un software para el manejo de la información (Niño & Illarramendi, 2015). El sistema de ficheros divide y almacena los datos en múltiples computadores (llamados también nodos) y el sistema de software automatiza los procesos para el tratamiento de datos. En base a esto, el funcionamiento del modelo MapReduce se dividió en dos partes:

1. **Fase Map:** En esta fase, se procesan parejas denominadas “clave-valor”, las cuales son extraídas del sistema de ficheros y se los transforma en datos intermedios según la función elegida por el usuario (García et al., 2016). Así, por ejemplo, imaginemos que deseamos ordenar una caja de legos por colores (función elegida por el usuario). Lo primero que el sistema hará será organizar los pares de información (lego a – color b) y los transformará en dato intermedio fácil de leer y entender. En el ejemplo, el sistema nombrará con el número “1” a los pares de legos rojos y así sucesivamente con los demás colores; esto permitirá que la lista de información sea más sencilla de entender para la siguiente fase. Esto mismo es explicado por Niño al señalar que la función Map es “la que transforma un conjunto de datos de partida en otra serie diferente de datos intermedios en forma de (clave, valor)” (Niño & Illarramendi, 2015).

2. **Fase Reduce:** Una vez creados los datos intermedios, estos se procesan de manera agrupada para producir el resultado final (García et al., 2016). Siguiendo el ejemplo anterior, se tomarán todos los pares similares, como los legos color azul de código 1 para agruparlos en una caja. Es decir, “la función de reducción es aplicada a la lista de valores para general un valor de salida” (Niño & Illarramendi, 2015).

Ahora bien, si bien el modelo MapReduce se popularizó, lo cierto es que no es el único modelo de tecnología de Big Data. Como menciona Niño, se lanzaron modelos como el Sawzall, Bigtable, Dynamo, Dreme, etc (Niño & Illarramendi, 2015). A partir del estudio de estos modelos, se llegó a esquematizar el

funcionamiento de las tecnologías de Big Data. Como veremos a continuación, el esquema deriva del modelo MapReduce establecido por Google en 2003.

Al igual que otros procesos tecnológicos, la ejecución del proceso de Big Data tiene lugar a lo largo de un ciclo de vida donde se selecciona un subconjunto de datos, que no puede modificarse, y se procede a su procesamiento en sucesivas etapas. Si fuese preciso modificar este subconjunto de datos, sería necesario realizar una nueva iteración del proceso. El ciclo de vida a ejecutar se desarrolla en cinco fases o etapas (Alonso Secades, 2015):

1. **Adquisición:** En esta primera etapa, se recopilan los datos que servirán como base del tratamiento. En efecto, como señala Gil, los datos que se recopilen serán base del proyecto de Big Data o de las actividades del tratamiento que hagan uso de esta tecnología, para su posterior explotación (Gil, 2016). Estos datos tienen un origen y una naturaleza variada.

   Respecto al origen de estos datos, los datos pueden provenir de diversas actividades. Como ya se mencionó desde la creación de internet, la dimensión en cuanto a la generación de datos se potenció, lo que hizo imposible el uso de herramientas tradicionales para su procesamiento (Niño & Illarramendi, 2015). Así, los datos que usan las tecnologías de Big Data tienen un origen variado, estos pueden ser capturados a través de sensores, similares, transacciones, entre otras actividades que realiza el individuo (Alonso Secades, 2015).

   Es importante mencionar que las tecnologías de Big Data adquieren los datos mediante un proceso en el cual se infiere la información (Gil, 2016). En efecto, este tipo de datos son obtenidos a partir de otro dato. Así, por ejemplo, una empresa de venta de celulares *online* que recopila información sobre las compras que realiza una persona, mediante el uso de tecnologías de Big Data puede hacer inferencias sobre las preferencias de consumo de una

persona o incluso su nivel socioeconómico. A partir de la compra de un celular, se podría inferir que: (i) la persona tiene un interés en la tecnología; (ii) tiene un nivel intelectual alto que le permite comprender el uso de este tipo de tecnología; y, (iii) dependiendo del historial de compras, se puede inferir qué días prefiere comprar y cuáles son sus tiempos libres.

Es importante mencionar que no todos estos datos son datos personales, por lo que su uso, en principio, no está sujeto a la regulación de la Ley de Protección de Datos. Sin embargo, este ejemplo nos sirve para explicar el origen de los datos que utilizan las tecnologías de Big Data. Como menciona Gil, el proceso de adquisición de datos es dinámico debido a la capacidad que tienen estas tecnologías de generar y obtener datos en tiempo real, así como su posterior retroalimentación (Gil, 2020).

Por último, debemos tener en consideración a los metadatos, los cuales son información que describe y da contexto a otros datos. Es decir, los datos son asociados con otros para describirlos y sistematizarlos (Gil, 2020). Para entender esto tengamos en cuenta un dato gráfico como lo puede ser una fotografía (dato 1). Al momento en que las tecnologías de Big Data procesan la fotografía asocian la misma con otros datos como lo son la fecha (dato 2), la hora (dato 3) o el lugar (dato 4) en los cuales dicha fotografía fue tomada. En este caso, el Big Data asociará los datos 2, 3 y 4 con el dato 1, ello pues los primeros describen al dato 1. Como menciona Gil, estos datos aportan una gran cantidad de información adicional sobre el dato principal, llegando incluso a caracterizarlo sin necesidad de acceder al mismo (Gil, 2016). Lo relevante de esto es que los metadatos serán utilizados posteriormente por las tecnologías de Big Data como datos primarios para hacer procesos de inferencias. Así, lo que en un inicio era considerado como un dato no personal, como la hora o el lugar de una fotografía, puede llegar a convertirse en un dato personal (Gil, 2020).

2. **Limpieza:** Además de la velocidad y la cantidad con la que se generan datos en la actualidad, otro de los problemas que soluciona la tecnología del Big Data es la búsqueda de la veracidad de la información. Es que debido a la cantidad de información que es recolectada, mucha de ella es irrelevante e incluso falsa, lo que puede conllevar a conclusiones erróneas. Justamente, el Big Data tiene como objetivo conseguir datos de alta calidad (IBM INSTITUTE FOR BUSINESS VALUE, 2012). Por lo tanto, "es preciso efectuar una extracción de la información que permita disponer únicamente de la información necesaria y que ésta sea almacenada de forma estructurada" (Alonso Secades, 2015).

3. **Integración:** Si bien las herramientas tradicionales pueden procesar los datos estructurados, estas presentan problemas con los datos semi estructurados y, especialmente, con los no estructurados (Conesa & Gómez, 2015). Ante estos casos, el Big Data extraerá los datos de cada tipo y los cargará en repositorios intermedios de manera organizada (Alonso Secades, 2015). En esta fase, las tecnologías de Big Data transformarán los datos no estructurados en datos estructurados para hacer más sencillo su procesamiento. Asimismo, será en esta fase en la que los metadatos son asociados a los datos principales, lo que servirá para dar contexto a los mismos (Alonso Secades, 2015).

4. **Análisis:** Esta es una de las fases más importantes de todo el proceso de Big Data, pues en esta todos los datos son analizados para encontrar patrones y correlaciones; es decir, crear nuevo conocimiento. En esta fase se utilizan técnicas de inteligencia de negocio, minería de datos y modelos algorítmicos para la generación de nuevo conocimiento que antes se encontraba oculta ante la masividad y variedad de datos (Gil, 2016, 2020).

   Es justamente la diversidad, dinamicidad y heterogeneidad de la muestra de datos con los que trabaja el Big Data que permite la creación de múltiples

patrones y conocimiento hasta ahora desconocidos (Alonso Secades, 2015). Sumado a los datos primarios, como mencionamos anteriormente, esta tecnología trabaja con datos inferidos y metadatos, los cuales son fuente de amplio conocimiento. Como menciona Gil, “los usos secundarios de los datos son la base de un cambio de paradigma” ((Gil, 2016).

5. **Interpretación:** Posterior al análisis de los datos, se descartan los patrones sin valor y se conservan las asociaciones que puedan llegar a tener una mayor utilidad (Alonso Secades, 2015). En esta fase se busca descubrir nueva información e investigar más respecto de las utilidades secundarias que se le puedan dar a los datos (Gil, 2016). Para una mejor comprensión podemos usar el siguiente ejemplo: en una institución educativa que analiza el rendimiento académico de sus estudiantes. A lo largo de los años, se descubre que la probabilidad de que un alumno abandone sus estudios está relacionada con una combinación de factores como la disminución en su participación en actividades extracurriculares (dato 1), una caída en sus calificaciones (dato 2) y un aumento en sus solicitudes de asesoría académica (dato 3). Si bien cada uno de estos elementos por separado no suele ser un indicador fuerte, el análisis cruzado de los datos históricos revela que, en conjunto, estos factores han sido predictores fiables de la deserción escolar.

Es importante tener en cuenta que los datos utilizados para identificar un patrón pueden ser tanto anónimos como personales. En efecto, la tecnología de Big Data no solo usa de fuente datos personales, sino todo tipo de datos. Esto es relevante pues no todos los datos que utilizan los sistemas de Big Data están sujetos a la protección por parte de la Ley de Protección de Datos Personales ni son parte del contenido constitucionalmente protegidos del derecho a la autodeterminación informativa. Ahora bien, en el caso que se lleguen a utilizar datos personales, es importante que estos estén anonimizados o seudonimizados (Gil, 2016, 2020). Según el artículo 14 de la Ley de Protección de Datos, un dato que fue anonimizado

no puede identificar ni hacer identificable al titular de los datos personales. Por su parte, un dato que pasó por un proceso de pseudo anonimización no puede ser atribuido a una persona en específico pues el dato es asociado a un seudónimo (Swire & Kennedy-Mayo, 2020).

Hasta este punto, en el caso de que los procesos de anonimización o seudo anonimización fuesen realmente efectivos, la información generada por los patrones y correlaciones del Big Data no podría ser vinculada directamente con los individuos. Por lo tanto, no existiría una vulneración el derecho a la autodeterminación informativa, ya que las personas segurían en control de su información, sin que los datos generados por el Big Data sean correlacionados con su identidad.

En efecto, el resultado de la etapa de análisis de los procesos que utiliza el Big Data no pueden identificarse directamente con los datos personales de las personas. Esto se debe a que las correlaciones que se realizan se hacen en base a un perfil abstracto. Como menciona la profesora Gil, “el resultado de esta etapa consiste en la definición de un perfil abstracto, el cual se basa en establecer qué combinación de factores genera un resultado específico, determinado con un nivel de confianza y un margen de error determinados”(Gil, 2020). Esta información, si bien es de alto valor, al no ser asociada a una persona en específico no puede ser considerada como datos personales.

Sin embargo, el Big Data presenta una última fase: la aplicación del modelo a una persona determinada. En esta fase, los modelos creados deben ser probados en un individuo para generar conclusiones fidedignas. En efecto, “se recopilan y procesan los datos personales del sujeto con el fin de generar conclusiones basadas en el modelo previamente desarrollado” (Gil, 2016). En esta parte del proceso de Big Data, es necesario contar con el consentimiento del individuo. Antes de esta etapa se utilizaron datos anonimizados o seudo anonimizados; sin embargo, para probar los modelos se requiere del consentimiento del individuo.

3.3. Incompatibilidad del Big Data y el consentimiento

3.3.1. El reinado de las minorías

Las tecnologías de Big Data permiten identificar patrones y realizar inferencias basadas en grandes volúmenes de datos. Ello nos plantea un primer problema: ese potencial de inferencia resulta incompatible con los requisitos del consentimiento establecidos en la Ley de Protección de Datos y en el Nuevo Reglamento. Pero, además, existe uno aún más grave, una de las virtudes de este proceso de inferencia es que con la información recopilada de un grupo reducido de personas se pueden realizar inferencias sobre la información de individuos que no han prestado dicho consentimiento. Esto se agudiza si se toma en consideración que las inferencias generadas pueden incluir datos personales.

En ese sentido, el hecho de que no se requiera el consentimiento del grupo más amplio para realizar estas inferencias supone la vulneración del derecho a la autodeterminación informativa. Ello se debe a que las personas pertenecientes al grupo amplio pierden el control sobre su información personal, pues mediante el Big Data es posible procesar y utilizar su información sin su conocimiento ni aprobación. Es la forma de operar del Big Data, lo que lo hace incompatible con el mecanismo del consentimiento. Lo que conlleva a que los individuos, en el contexto actual, no tienen capacidad real de tomar una decisión que proteja sus datos personales (Nissebaum, 2018). Es por todo ello, que sostenemos que utilizar al consentimiento como principal garante de la protección de la información personal queda obsoleto ante el paradigma de la sociedad de la información, donde el estándar en el procesamiento de datos es el uso de tecnologías como el Big Data.

a. Las tecnologías de Big Data permiten realizar inferencias, las cuales no fueron autorizadas de antemano por el titular de los datos

Como quedó claro en el apartado anterior, las tecnologías de Big Data se caracterizan por su capacidad para recopilar, almacenar, procesar y analizar grandes volúmenes de datos provenientes de fuentes heterogéneas. Gracias al uso de algoritmos avanzados, estas tecnologías permiten identificar patrones ocultos y realizar inferencias que aportan información adicional sobre personas o fenómenos, sin que esta información haya sido proporcionada de manera directa. Este proceso de inferencia se basa en el reconocimiento de relaciones complejas dentro de los datos, muchas veces difíciles de detectar mediante métodos tradicionales estadísticos.

Para comprobar ello, a continuación se demostrará cómo el Big Data realiza los procesos de inferencias sobre datos personales. Como evidencia empírica de ello se utilizará como referencia el estudio empírico realizado por los investigadores Michal Kosinski, David Stillwell y Thore Graepel (2013), en el cual se buscó analizar hasta qué punto los registros digitales simples del comportamiento humano pueden ser utilizados para estimar de manera precisa una amplia gama de datos personales que —en principio— las personas no consintieron.

En su experimento se usaron como muestra los likes de Facebook de más de 58,000 usuarios voluntarios. El primer paso fue justamente la recopilación de estos datos, para luego pasar a la construcción del modelo de Big Data, en el cual todos los datos se organizaron en una matriz usuario-like. Finalmente, se utilizó la fuerza de inferencia de la matriz para realizar una validación cruzada y extraer nuevo conocimiento. Todo ello, es un ejemplo de los pasos descritos en la sección 3.2 de la presente investigación relativos a las fases de las tecnologías de Big Data.

Lo sorprendente de este experimento fueron los resultados, pues **se obtuvieron inferencias precisas tanto en atributos personales específicos, tales como**

orientación sexual, ideología política o religión; así como en variables numéricas continuas, tales como la edad de los usuarios (Kosinski et al., 2013). A continuación, se presentan algunos de resultados con mayor grado de precisión:

Atributo inferido	**Porcentaje de precisión**
Origen étnico (Caucásico vs Afroamericano)	95%
Género (Hombre/Mujer)	93%
Orientación sexual masculina	88%
Afiliación política (Demócrata vs Republicano)	85%
Religión (Cristiano vs Musulmán)	82%
Edad	75%
Orientación sexual femenina	75%
Consumo de cigarrillos	73%
Consumo de alcohol	70%

Fuente: Elaboración propia a partir de los datos presentados en Kosinski, M., Stillwell, D., y Graepel, T. (2013).

Como se puede observar, resulta impresionante no solo la precisión alcanzada por las inferencias, sino también la diversidad de los datos personales obtenidos —incluso algunos de categoría sensible, como la orientación sexual, afiliación política o religión— a partir de un insumo aparentemente trivial como los "likes" en Facebook. Tal como mencionan los propios autores del estudio, “la posibilidad de predecir atributos individuales a partir de registros digitales de comportamiento puede tener implicaciones negativas considerables, ya que puede aplicarse

fácilmente a grandes cantidades de personas sin obtener su consentimiento individual y sin que estas lo noten" (Kosinski et al., 2013).

Todo ello demuestra que las tecnologías de Big Data tiene el potencial de inferir los datos personales sin requerir el consentimiento directo y específico del titular. Lo cual resulta incompatible con el consentimiento, el cual para ser válido requiere de ser (i) libro, (ii) previo, (iii) expreso, (iv) inequívoco y (v) informado.

En especifico, es incompatible pues no resulta posible obtener un consentimiento verdaderamente previo. Si bien el consentimiento es otorgado —formalmente— justo antes del proceso de recolección de los datos base, lo cierto es que las inferencias se generan después del momento de recolección; es decir, no existen aun en el momento de la recolección. Así, el consentimiento no se otorga respecto del tratamiento real —los usos de esas inferencias— sino solo sobre los posibles usos de los datos base. Pero lo cierto, es que esos datos base solo serviran de insumo para las inferencias y los usos posteriores de las mismas.

A primera vista, podría considerarse que el problema radica en la falta de información y especificidad, por lo que bastaría con advertir al titular que sus datos podrían utilizarse para inferencias adicionales. Sin embargo, esta visión es limitada. En los entornos actuales de tratamiento masivo y automatizado, ni siquiera quienes diseñan los sistemas pueden anticipar con precisión qué atributos serán inferidos, qué relaciones emergentes serán explotadas, ni el grado de sensibilidad.

Tal como menciona Hildebrandt, resulta difícil, sino imposible, para los responsables del tratamiento anticipar la creación de perfiles, basados en inferencia (Hildebrandt, 2015). De igual manera, Zarsky señala que el análisis del Big Data implica métodos y patrones que ni la entidad que recopila los datos ni el propio titular consideran o imaginan en el momento de la recolección (Zarsky, 2016). Esta imprevisibilidad estructural hace que el consentimiento se torne una herramienta incompatible con la lógica del Big Data.

b. Estas inferencias alcanzan a los datos personales de terceros; es decir, sobre personas que no han brindado ningún tipo de consentimiento.

Hasta el momento, se ha demostrado cómo el Big Data puede realizar inferencias acerca de los datos personales a partir de insumos aparentemente inocuos, como los likes de Facebook. Así, debe quedar claro como el consentimiento —en su forma tradicional, conforme con los requisitos de validez establecidos en la Ley— no solo resulta incompatible con la naturaleza del Big Data. Ello es así pues la lógica del consentimiento parte de la previsibilidad, especificidad y precisión del tratamiento, mientras que las tecnologías de Big Data operan sobre la base de inferencias emergentes e imprevistas incluso para quienes diseñan estos sistemas. Son justamente esas inferencias, de carácter imprevisible e incompatible con la lógica del consentimiento, las que imposibilitan un control real de la información por parte del titular, lo cual supone una afectación directa a su derecho a la autodeterminación informativa.

Esta situación se agrava si se considera que estas tecnologías permiten generar inferencias sobre terceros; es decir, sobre personas que no han brindado ningún tipo de consentimiento. En efecto, los modelos Big Data pueden operar a partir de los datos de minorías y, a partir de correlaciones, producir inferencias vinculadas a terceros que no son conscientes del tratamiento de su información. Esta capacidad revela —nuevamente— una falla estructural del modelo de protección basado en el consentimiento, pues incluso cuando una persona expresa explícitamente la negativa al tratamiento de sus datos. Lo cierto es que los sistemas de Big Data pueden inferirlos de forma inevitable, lo cual deja desprotegido al titular.

Este potencial de las tecnologías de Big Data no es solo una suposición, sino es una realidad, la cual ha sido demostrada en múltiples investigaciones de carácter empírico. A continuación se presentarán algunas de ellas para evidenciar esta afirmación.

En primer lugar, en el año 2018, los investigadores Neil Zhenqiang Gong y Bin Liu demostraron que, mediante tecnologías de Big Data, es posible inferir los atributos privados de personas que no los han proporcionado, a partir de los datos de otros usuarios en plataformas como Google+ y Google Play. Para ello, utilizaron los datos de 1.1 millones de usuarios de dichas plataformas, de los cuales removieron los datos de los usuario objetivos con el fin de simular un escenario real en el cual dichos datos no estuvieran disponibles. Finalmente, evaluaron el potencial de inferencia mediante el modelo de Big Data llamado SBA (Social-Behavior-Attribute). Los resultados de esta investigación demostraron que **se logró predecir con 57% de precisión la ciudad de residencia de los usuarios objetivo; asimismo, los autores señalaron que su modelo es aplicable a atributos sensibles**, tales como, la orientación sexual, las opiniones políticas, la religión o la afiliación ideológica (Gong & Liu, 2018).

Sin embargo, este no es el único estudio que demuestra el poder de las inferencias sobre terceros de las tecnologías de Big Data. En el mismo año, Nikolaos Aletras y Benjamin Chamberlain desarrollaron un modelo de Big Data con el objetivo de determinar el grado de precisión en la inferencia de atributos socioeconómicos complejos en base al contenido lingüístico y la estructura de la red social de Twitter. Para ello, se utilizó como muestra el perfil de Twitter de 4,625 usuarios británicos. Lo más sorprendente del estudio fue que se evaluó la capacidad de inferencia del modelo para los casos de usuarios que no publicaban contenido alguno; es decir, eliminaron el componente textual del modelo y trabajaron solo con la estructura de su red social (seguidores y seguidos). Los resultados mostraron que, **solo con el uso de la estructura de la red social, se pudo predecir con 54% de precisión la clase ocupacional de los usuarios**; es decir, la categoría profesional a la que pertenecían los usuarios según su empleo (Aletras & Chamberlain, 2018)

Por último, tenemos el experimento realizado por los investigadores Alan Mislove, Bimal Viswanath, Krishna P. Gummadi y Peter Druschel; los cuales, en base a los

principios del Big Data, buscaron determinar si era posible inferir datos personales de usuarios que no los han revelado explícitamente. Para ello, utilizaron los datos de usuarios de la plataforma Facebook pertenecientes a dos comunidades, la Red universitaria de Rice University y Red regional de Nueva Orleans. Para poder simular un escenario real de inferencias sobre datos de terceros, ocultaron los datos de los usuarios objetivos, para simular que estos no habían publicado ningún dato. Luego, en base a correlaciones se trató de identificar la precisión de las inferencias. Los resultados evidenciaron **una alta precisión en las inferencias de los siguientes datos: universidad, año de ingreso, ciudad de residencia y escuela secundaria; por ejemplo, se obtuvo un 95% de precisión en inferencias respecto a qué universidades asistían los usuarios** (Mislove et al., 2010).

Además de ello, parte del estudio se centró en identificar cuál era la proporción mínima de usuarios que debían compartir sus datos para que el sistema pudiera inferir los del resto. Al respecto, l**os resultados mostraron que bastaba con que el 20 % de los usuarios revelará su información para que el sistema pudiera inferir con alta precisión los datos del 80 % restante** (Mislove et al., 2010). Esto evidencia el potencial predictivo del tratamiento de datos mediante el Big Data, el cual opera más allá de la voluntad del titular, o en otras palabras, fuera del consentimiento individual.

La aplicación de las inferencias generadas por el análisis de Big Data plantea serios desafíos legales, en particular en lo que respecta al principio del consentimiento. En este punto cabe preguntarse cuál es la categoría jurídica que corresponde a las inferencias producto del tratamiento de datos mediante Big Data. Al respecto, podemos señalar que el Foro Económico Mundial propuso una clasificación entre el grupo de datos personales: (i) datos voluntarios, (ii) datos observados y (iii) datos inferidos. Respecto de los datos inferidos señaló que estos eran aquellos que se obtuvieron después del análisis de los otros datos (World Economic Forum, 2011). De igual manera, Wachter y Mittelstadt entienden a los datos inferidos como aquella información —que guarda relación con una persona identificada o identificable—

generada a través de procesos deductivos, en lugar de provenir directamente de una mera recolección u observación de datos personales (Wachter & Mittelstadt, 2019).

Ahora bien, es necesario dejar en claro que los datos inferidos no son datos exactos. Como se demostró anteriormente, estos sí pueden alcanzar un alto grado de precisión, pero debido a su naturaleza probabilística no podemos afirmar que, en todos los casos, estos vayan a ser una representación exacta de la realidad. Esto se debe a que las inferencias no son hechos en sentido estricto, sino una son interpretaciones o predicciones formuladas en base a otros datos (Wachter & Mittelstadt, 2019). Al ser generados mediante procesos análiticos, estas adquieren un carácter subjetivo y no verificable, pues son interpretaciones que reflejan lo que el sistema o el analista cree que es una persona (Trovato, 2023).

Lo que sí resulta certero son las consecuencias de los usos en base a estas inferencias. Tal como menciona Trovato, estas inferencias producen efectos concretos sobre los individuos, incluso cuando las mismas se basan en premisas erróneas o no verificables (Trovato, 2023). Ello se debe a que las inferencias en la práctica son tratadas como datos objetivos. Así, el foco de atención no debe estar centrado en cómo fueron obtenidos, sino en el uso que se hace de ellos (Wachter & Mittelstadt, 2019).

La calificación jurídica de este tipo de datos es controversial. Así, Arroyo señala que, actualmente, existe una disputa sobre si los datos inferidos deben ser reconocidos como datos personales (Arroyo Revatta, 2021). En la Unión Europea no se los reconoce expresamente como datos personales; sin embargo, existen avances en el reconocimiento de esto, tal es así que la legislación más avanzada en este tema, es el Consumer Privacy Act (CCPA)[9] de Califonia, Estados Unidos, en la cual se

[9] "(v) (1) "Personal information": (…) (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes".

reconocen a los datos inferidos como información personal (Trovato, 2023). En esa misma línea, el Procurador General de California señaló que “inferencias generadas internamente que una empresa posee sobre un consumidor es información personal según la entiende el CCPA, y debe divulgarse a pedido del consumidor” (California A.G., 2020).

En el Perú, ni la Ley de Protección de Datos, ni el Nuevo Reglamento han establecido expresamente que los datos inferidos son datos personales. No obstante, con el Nuevo Reglamento se hace alusión a este tipo de datos en su artículo 76.4, reconociendo que los datos inferidos pueden ser objeto del derecho de portabilidad. Además de ello, se los define como “aquellos que han sido sometidos, por lo menos, a un proceso de personalización, categorización o elaboración de perfiles”. Si bien esta disposición no otorga un reconocimiento expreso sobre la calidad de datos personales, si representa un avance relevante, en tanto admite que los datos inferidos pueden ser sometidos al régimen de un derecho ARCO: la portabilidad. Así, aunque la regulación en el Perú es de carácter más funcional y parcial, este avance significa una apertura a una protección más amplia a este tipo de datos.

Por todo ello, para los fines de este trabajo de investigación, se optará por considerar a los datos inferidos como datos personales, siempre que estos identifiquen o permitan la identificación de una persona en específico. Negarles esa condición vacía el contenido del derecho fundamental a la autodeterminación informativa, pues el individuo no estaría en pleno control de la información referida a él. Sobre todo si consideramos que esa información puede tener efectos concretos en otros aspectos de su vida como el trabajo, acceso a crédito, salud, etc.

Todo ello, no hace más que reforzar nuestra postura: el consentimiento resulta estructuralmente incompatible con las tecnologías de Big Data. En efecto, si consideramos que las inferencias —en tanto identifiquen o permitan identificar a una persona— son datos personales, entonces, también se debe aceptar que el

consentimiento —tal como se configura actualmente— es insuficiente para protegerlas. Ello debido a la incompatibilidad estructural entre el consentimiento y las tecnologías de Big Data. Como señalamos antes, el consentimiento en estos casos no puede ser realmente previo, pues el proceso inferencial se lleva acabo después del momento de recolección. Asimismo, no es posible que este sea realmente informado ni especifico, pues la finalidad del tratamiento se determina en base a las inferencias.

Además de ello, en el caso de los datos inferidos de terceros, el consentimiento no podrá ser ni libre ni inequívoco. No podrá ser libre, ya que los individuos no aceptaron de forma voluntaria el tratamiento de sus datos inferidos. En estos casos, el titular no ha proporcionado consentimiento alguno, pero aun así resulta ser impactado por el sistema, ya que sus datos pueden ser inferidos en base a los de otros individuos.

En esa linea, tampoco podrá ser inequívoco, pues no existirá ninguna acto claro y afirmativo de manifestación de voluntad. De hecho, en algunos casos puede haber manifestado su negativa al tratamiento de sus datos base y aun así ser parte del tratamiento. Tal como mencionan Wachter y Mittelstadt, el proceso de inferencia se realiza de manera invisibles para el titular; es decir, sin la necesidad de un consentimiento y estas son generadas de manera posterior al momento de otorgar el consentimiento (Wachter & Mittelstadt, 2019).

Así, debe quedar claro que, si bien el principio de consentimiento es uno de los pilares fundamentales en la protección de datos personales, ya que se considera esta es la mejor alternativa para que los individuos tengan control sobre su información. Lo cierto este resulta incompatible con las tecnologías de Big Data, las cuales permiten que las organizaciones tomen decisiones basadas en información inferida, que no ha sido proporcionada directamente por el titular de los datos y, por ende, no ha sido objeto de consentimiento previo.

3.3.2. El cheque en blanco

El segundo problema que demuestra la incompatibilidad entre el consentimiento, como forma de protección de datos personales y el Big Data está relacionado con la especificación de los fines del tratamiento de datos. Como analizamos anteriormente, el derecho a la autodeterminación informativa, en el modelo actual, tiene como principal mecanismo de protección al consentimiento. En ese esquema, es necesario que el consentimiento sea válido; para ello, la Ley de protección de datos señala que este debe ser previo, expreso, informado, inequívoco y específico.

Todo ello implica que los individuos, antes de prestar su consentimiento, estén plenamente informados sobre los fines para los cuales se utilizarán sus datos personales. Como señala Murabak, al momento de solicitarse el consentimiento, el titular de los datos personales debe estar informado de forma expresa e inequívoca sobre la finalidad del tratamiento (Mubarak Aguad, 2017). En otras palabras, el consentimiento no puede ser uno ambiguo o general; de lo contrario, el consentimiento solo otorgaría una ilusión de control a las personas sobre su información.

El objetivo del consentimiento es justamente “entregar a las personas el control respecto de sus datos personales, para que a través de este control puedan decidir por ellas mismas cómo determinar los costos y los beneficios de la recolección, uso y divulgación de su información” (D. Solove, 2014). Este enfoque busca proteger a las personas de tratamientos inesperados sobre los cuales estas no tengan conocimiento. Es por ello que la regulación actual exige que, en caso se plantee un nueva finalidad de uso de datos previamente consentidos, se requerirá un nuevo consentimiento de parte del titular autorizando este nuevo uso (artículo 4 del Reglamento).

Lamentablemente, este enfoque presenta serios problemas en entornos donde se utilizan tecnologías de Big Data. Esto es así pues estas tecnologías desafían la

capacidad de los responsables del tratamiento para definir de manera precisa y exacta las finalidades del consentimiento. Efectivamente, el valor del Big Data reside en la infinidad de usos de la información recolectada (Mubarak Aguad, 2017). Como menciona Gil, “es precisamente en estos usos secundarios donde reside el potencial del Big Data” (Gil, 2016)

Así, a diferencia de los sistemas tradicionales de procesamiento de información, el procesamiento de datos mediante el Big Data se caracteriza por su enfoque dinámico y exploratorio. Aloso Secada explica que, debido la diversidad, dinamicidad y heterogeneidad de la muestra de datos con los que trabaja el Big Data, la creación de múltiples patrones y conocimiento hasta ahora desconocidos es posible (Alonso Secades, 2015). Por lo tanto, el objetivo de este tipo de tecnología no es responder a la pregunta previamente establecida; es decir, el Big Data no es utilizado para reafirmar un presupuesto establecido por el responsable del tratamiento de datos. Por el contrario, el objetivo del Big Data es la generación de nuevo conocimiento mediante el descubrimiento de correlaciones y patrones inesperados

En el esquema actual, se exige que el responsable del tratamiento de datos personales deba conocer las finalidades de las fases de adquisición, limpieza, integración, análisis, interpretación y en la fase de aplicación del modelo. Sumado a ello, el responsable debe estar en condiciones de especificar las finalidades antes de la fase 1 (Gil, 2020). Sin embargo, como desarrollamos previamente, las fases de análisis, interpretación y, especialmente, la de aplicación del modelo resultan ser imprevisibles, lo que imposibilita que el responsable sepa cuáles serán las finalidades del tratamiento.

Teniendo en cuenta ello, cabe preguntarse si es posible evitar la imprevisibilidad que caracteriza el tratamiento de datos mediante Big Data. Lo cierto es que, el funcionamiento técnico de esta tecnología sugiere lo contrario, pues la imprevisibilidad de las inferencias es inherente a los modelos de Big Data. En otras

palabras, la razón por la cual no es posible evitar la imprevisibilidad se debe a razones estructurales, ya que el procesamiento de datos masivos opera bajo el cual el responsable del tratamiento no puede definir de antemano qué conocimiento se generará.

Este enfoque es conocido como bottom-up, el cual consiste en analizar múltiples y diversos datos para generar correlaciones y patrones con el fin de obtener nuevo conocimiento (Wirsch, 2014). Es preciso mencionar, que ese conocimiento no se deriva de planteamientos previos, por el contrario, surge directamente de los datos base. A continuación, se describirá el flujo técnico a fin de entender esta lógica exploratoria.

N°	Fase	Explicación
1	Motivación general	Definición del objetivo general del análisis.
2	Obtención del dataset	Recolección de múltiples datos de diversas fuentes.
3	Exploración y limpieza	Eliminación de errores o inconsistencias.
4	Selección de datos	Identificación de datos relevantes.
5	Selección de modelo	Elección de algoritmos.
6	Entrenamiento del modelo	Entrenamiento del modelo con datos históricos para extraer los primeros patrones.
7	Interpretación	Prueba del modelo para medir precisión.
8	Integración	Aplicación del modelo en un sistema real con nuevos datos.

Fuente: Elaboración propia a partir de los datos presentados en Wirsch, A. (2014).

Resulta evidente, que este proceso se encuadra con las fases características del Big Data descritas en la sección 3.2.1 de la presente investigación. Es importante señalar que la fase 1 descrita por Wirsch no debe ser interpretada como la formulación de hipótesis previas ni a una finalidad de analitica cerrada, sino como un propósito general, como por ejemplo, la mejora de decisiones de un negocio, optimización de servicios, entre otras.

El propósito de este enfoque es crear un sistema automático capaz de ejecutarse con la mínima intervención del operador (Wirsch, 2014). Precisamente esta lógica de funcionamiento es la que dificulta que el responsable del tratamiento pueda anticipar con exactitud qué nuevo conocimiento o información se generará a partir de los datos base. En base a lo anterior, se ha evidenciado que el carácter imprevisible es inherente al tratamiento de datos mediante tecnologías de Big Data.

Ahora bien, es necesario dejar en claro que estas conclusiones no solo son avaladas por los autores citados anteriormente, sino que reflejan la posición mayoritaria de la doctrina especializada en el tema. Como muestra de ello, se utilizará la estudio realizado por los investigadores Wendy Arianne Günther, Mohammad H. Rezazade Mehrizi, Marleen Huysman y Frans Feldberg, los cuales tenían el objetivo de sistematizar la literatura respecto al valor, uso y gestión del Big Data. Para ello, se revisaron 481 artículos académicos, extraídos de las bases de datos científicas Scopus, ScienceDirect, ProQuest y EBSCOhost, enfocados en analizar temas relacionados al Big Data. De análisis de los mismos, se identificaron varias conclusiones respecto a la dirección de la doctrina respecto a este tema, entre ellas:

Conclusión	**Literatura especializada**

Cuando los datos son tratados mediante tecnología de Big Data, estos son reutilizados para finalidades distintas a aquellas para las que fueron originalmente recolectados.	Zuboff, 2015[10]; Constantiou & Kallinikos, 2015[11]; Newell & Marabelli, 2015[12]; Shollo & Galliers, 2015[13]; Aaltonen & Tempini, 2014[14]
Las inferencias emergen sin haber sido definidas por el responsable del tratamiento.	Kim, 2015[15]; Yoo, 2015[16]; Aaltonen & Tempini, 2014; Shollo & Galliers, 2015; Madsen, 2015[17]; Constantiou & Kallinikos, 2015
El tratamiento de datos mediante Bi Data es de enfoque inductivo (bottom-up)	Constantiou & Kallinikos, 2015; Olbrich, 2014[18]; Van den Broek & Van Veenstra, 2015[19]; Bholat, 2015[20]

[10] Zuboff, S., 2015. Big other: surveillance capitalism and the prospects of an information civilization. J. Inform. Technol. 30 (1), 75–89. http://dx.doi.org/10.1057/jit.2015.5

[11] Constantiou, I.D., Kallinikos, J., 2015. New games, new rules: big data and the changing context of strategy. J. Inform. Technol. 30 (1), 44–57. http://dx.doi.org/10.1057/jit.2014.17

[12] Newell, S., Marabelli, M., 2015. Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal effects of datafication. J. Strategic Inform. Syst. 24 (1), 3–14. http://dx.doi.org/10.1016/j.jsis.2015.02.001

[13] Shollo, A., Galliers, R.D., 2015. Towards an understanding of the role of business intelligence systems in organizational knowing. Inform. Syst. J. 26 (4), 339–367. http://dx.doi.org/10.1111/isj.12071

[14] Aaltonen, A., Tempini, N., 2014. Everything counts in large amounts: a critical realist case study on data-based production. J. Inform. Technol. 29 (1), 97–110. http://dx.doi.org/10.1057/jit.2013.29

[15] Kim, H.J., 2015. Big Data: the structure & value of big data analytics. In: Proceedings of the Twenty-First Americas Conference on Information Systems, Puerto Rico, August 13–15. https://core.ac.uk/download/pdf/301365698.pdf

[16] Yoo, Y., 2015. It is not about size: a further thought on big data. J. Inform. Technol. 30 (1), 63–65. http://dx.doi.org/10.1057/jit.2014.30

[17] Madsen, A.K., 2015. Between technical features and analytic capabilities: charting a relational affordance space for digital social analytics. Big Data Soc. 2(1), 1–15. http://dx.doi.org/10.1177/2053951714568727

[18] Olbrich, S., 2014. Madness of the crowd—how big data creates emotional markets and what can be done to control behavioural risk. In: Proceedings of the Twenty-Second European Conference on Information Systems, Tel Aviv, Israel, June 9–11. https://core.ac.uk/reader/301362210

[19] Van den Broek, T., Van Veenstra, A.F., 2015. Modes of governance in inter-organizational data collaborations. In: Proceedings of the Twenty-Third European Conference on Information Systems, Münster, Germany, May 26–29. https://core.ac.uk/download/pdf/301366806.pdf

[20] Bholat, D., 2015. Big data and central banks. Big Data Soc. 2 (1), 1–6. http://dx.doi.org/10.1177/2053951715579469

Fuente: Elaboración propia a partir de Günther et al. (2017)

A partir de lo expuesto, se puede afirmar que la imprevisibilidad de las inferencias en el tratamiento de datos mediante Big Data no es una consecuencia accidental o corregible de dicho proceso, sino es una propiedad estructural de la misma. Así, exigir que el consentimiento del titular sea otorgado de manera previa, expresa, inequívoca e informada, tal como lo establece la norma, resulta incompatible con la dinámica técnica del Big Data. Lo cual refleja una crisis de adecuación entre el modelo regulatorio y los modelos de procesamiento masivo actuales.

Es claro que el propósito de la norma es establecer una obligación a los responsables del tratamiento de anticipar las finalidades de los datos recopilados directamente; sin embargo, surge la pregunta de si también es obligación de los responsables del tratamiento anticipar las finalidades de los datos que se pudieran obtener mediante los procesos del Big Data. Gil menciona que la obligación debe extenderse a ambos tipos de datos, datos primarios y secundarios; sin embargo, ello resulta imposible en la práctica, pues los responsables no pueden prever qué datos serán inferidos mediante los procesos del Big Data (Gil, 2020). En esa misma línea, Culnan y Bruening señalan que uno de los problemas de las tecnologías de procesamiento masivo es la imprevisibilidad de los resultados y con ello la falta de conocimiento sobre los usos de los datos secundarios (Culnan & Bruening, 2018).

Es por ello que la forma en que se concibe el consentimiento en la Ley de protección de datos y en su Reglamento resulta inviable en el contexto del Big Data; es decir, un contexto donde establecer con exactitud las finalidades del tratamiento de datos personales no es posible. Sumado a ello, como señalamos anteriormente, la normativa exige que, ante un uso nuevo de la información, el responsable del tratamiento solicite un nuevo consentimiento. Sin embargo, esto resulta técnicamente imposible, pues el Big Data maneja volúmenes de información masivos y el potencial de análisis por parte de esta nueva tecnología es prácticamente infinito (Gil, 2016).

3.3.3. Otros problemas del consentimiento

Toda la situación descrita anteriormente se agrava si tomamos en cuenta que el consentimiento presenta otros problemas en el contexto de la Sociedad de la Información. En efecto, además de los obstáculos producto directamente de la tecnologías de Big Data, el consentimiento —como principal mecanismo de protección de los datos personales— resulta insuficiente para asegurar el control de la información personal de las personas en la era digital.

Esto es así, pues en la práctica, el consentimiento se ha convertido en una formalidad —un rito— más que en un herramienta real de control de nuestra información. Tal es así, que el reporte de 2019 del Pew Research Center, centro de investigación especializado en tendencias sociales y tecnológicas, concluyó que el 81 % de los ciudadanos estadounidense siente que no tiene control sobre los datos que las empresas recogen (Pew Research Center, 2019). En consecuencia, si bien el consentimiento se presenta como una alternativa legalmente válida de protección de los datos de las personas, lo cierto es que resulta cuestionable si este resulta moralmente transformador (Schermer et al., 2014). A continuación se expondrán algunos de estos problemas.

a. Exceso de solicitudes de consentimiento

En la actualidad las personas lidian con una cantidad excesiva de solicitudes de consentimiento para el tratamiento de sus datos personales, lo que hace que estas se vuelvan insensibles a las mismas y otorguen su consentimiento sin reflexión alguna. Tal como menciona Schermer, “en la práctica, simplemente hay demasiadas solicitudes de consentimiento para que un usuario individual las considere, lo que diluye el efecto psicológico de enfrentarse a una transacción de consentimiento” (Schermer et al., 2014).

Ello se debe a la gran cantidad de sitios web y otras plataformas online a las acceden las personas. Como mencionamos anteriormente, debido al contexto de la Sociedad de la Información, los seres humanos nos vemos expuestos a diario a plataformas online que recaban nuestros datos personales. Lo que conlleva a que tengamos que enfrentarnos a una infinidad de solicitudes de tratamiento de datos personales.

Como muestra de ello, en 2008 las investigadoras Aleecia M. McDonald and Lorrie Faith Cranor publicaron un estudio empírico con el objetivo de calcular el tiempo de lectura promedio de las políticas de privacidad en Estados Unidos. Como parte de su estudio, se determinó la cantidad de sitios web a los que el ciudadano promedio accedía por año, para ello se utilizó datos extraídos de las firmas de análisis de tráfico web: Nielsen/Net Ratings and Pew Internet & American Life data and Census data. En base a todo ello, se concluyó que el usuario estadounidense promedio visitaba entre 1,354 y 1,518 sitios únicos al año, cada uno con su propia política de privacidad (McDonald & Cranor, 2008).

Este primer estudio guarda relación con la estimación propuesta por Henrique Xavier en 2024, quien en base a un análisis del tráfico web a nivel mundial, concluyó que en promedio un usuario visita entre 2.4 y 7.1 dominios web únicos por día (Xavier, 2024). Estos estudios demuestran la exposición masiva y constante a plataformas digitales que procesan información personal, a la que las personas se enfrentan diariamente. Esta dinámica refuerza la sobrecarga de solicitudes de consentimiento a la que nos vemos sometidos en nuestra vida cotidiana.

Ahora bien, no basta con evidenciar la masiva cantidad de solicitudes de consentimiento a la que se ven sometidas más personas en su vida diaria, sino es necesario demostrar que resulta inviable en la práctica que estas puedan leerlas y comprenderlas plenamente. Para ello, nos remitimos nuevamente al estudio presentado por las investigadoras Aleecia M. McDonald and Lorrie Faith Cranor, el

cual como señalamos estaba destinado a calcular el tiempo de lectura promedio de las políticas de privacidad en Estados Unidos.

En dicha investigación, se estimó el tiempo de lectura promedio de una política de privacidad tomando como referencia las políticas de los 75 sitios web más populares de Estados Unidos. Como resultado se estimó que leer una política de privacidad tomaría aproximadamente 10 minutos (McDonald & Cranor, 2008). En base a ello y a la cantidad de sitios web promedio que visita una persona al año (entre 1,354 y 1,518 sitios web), se concluyó que si una persona leyera detenidamente cada política de privacidad, necesitaría entre 181 y 304 horas anuales (McDonald & Cranor, 2008).

Todo ello, evidencia que el modelo de protección de datos personales basado en el consentimiento resulta inviable en la práctica. Ello pues excede la capacidad de atención y tiempo razonable de la persona promedio, lo que pone en entredicho la legitimidad del consentimiento como principal base para el tratamiento de datos personales.

b. La complejidad de las políticas de privacidad

En el apartado anterior, se evidenció que las políticas de privacidad son (i) masivas y (ii) exceden la capacidad de atención y tiempo razonable de la persona promedio. Sumado a ello, estas son de naturaleza compleja, lo cual impide que los usuarios las comprendan. En otras palabras, incluso si los usuarios tuviesen el tiempo para leerlos, la mayoría no tienen los recursos cognitivos para comprenderlos. Como menciona Schermer, “dada la naturaleza altamente compleja del procesamiento de datos y los requisitos legales de transparencia y notificación, los avisos de privacidad suelen ser largos, difíciles y redactados en lenguaje legalista” (Schermer et al., 2014).

Para demostrar ello, tomaremos como referencia el experimento empírico llevado a cabo por las investigadoras Aleecia M. McDonald and Lorrie Faith Cranor, en el cual se estudiaron 75 políticas de seguridad de los sitios web más visitados de Estados Unidos. Como una de sus conclusiones, los investigadores encontraron que el rango de longitud de las políticas de privacidad era de 144 hasta 7,669 palabras (aproximadamente, 15 páginas); estableciendo como media 2,514 palabras por política de privacidad (McDonald & Cranor, 2008). Con ello, resulta evidente que la larga longitud en las políticas de privacidad es la regla y no la excepción.

Como señalamos anteriormente, del estudio de McDonald & Cranor, se concluyó que se necesitan al menos 10 minutos para leer la política de privacidad promedio. Sin embargo, cabe preguntarnos si en la realidad las personas las leen. Para ello, nos remitiremos al reporte de 2019 del Pew Research Center, centro de investigación especializado en tendencias sociales y tecnológicas. Dicho reporte se basó en una encuesta nacional representativa a 4,272 adultos estadounidenses, llevada a cabo entre el 3 y el 17 de julio de 2019, mediante el panel American Trends Panel. Asimismo, la encuesta fue complementada por referencias a los datos del Censo de Estados Unidos, para asegurar que la muestra sea estadísticamente representativa.

Teniendo en cuenta esto, se llegaron a las siguientes conclusiones: solo el 9% de los encuestados afirmó que lee siempre las políticas de privacidad y, —lo que resulta particularmente alarmante— es que el 36% de los encuestado reconoció nunca leer las políticas de privacidad antes de consentir el tratamiento de sus datos (Pew Research Center, 2019). Estas cifras fueron en aumento, pues en el reporte de 2023, se concluyó que el 56% de los encuestados nunca las lee antes de otorgar su consentimiento y el 69% señaló que consideran a las políticas de privacidad como “algo que simplemente deben pasar por alto” para continuar con lo que realmente desean hacer (Pew Research Center, 2023).

Entonces, queda claro que más allá del tiempo y la longitud de las políticas de privacidad, la mayoría de las personas opta por no leerlas. Además de ello, estos datos evidencian que, en la práctica, el otorgar el consentimiento se ha convertido en un acto rutinario y carente de reflexión; percibido como más como un paso previo para el uso de plataformas digitales que como un mecanismo que refleja la decisión informada y voluntaria de las personas.

Por último, cabe responder la pregunta acerca de la complejidad y comprensión de estas políticas. Ello es necesario pues consideramos que “incluso si los titulares de datos leyeran todas las políticas de privacidad, resulta cuestionable si realmente comprenden las posibles consecuencias del procesamiento de datos” (Schermer et al., 2014).

Para comprobar ello, utilizaremos el estudio empírico de los investigadores George Milne, Mary Culnan y Henry Greene, los cuales buscaron evaluar la legibilidad de las políticas de privacidad publicadas en sitios web comerciales líderes. Para ello, se evaluaron 312 sitios web activos de la lista de los 500 sitios Web más visitados según Media Metrix (una firma de análisis de tráfico web), y que contaban con políticas de privacidad accesibles desde su página principal.

Para el análisis se utilizó un software llamado “Readability Calculations” de la empresa Micro Power and Light, el cual aplicaba diferentes índices de legibilidad para evaluar cuán difícil era leer cada política y estimar cuántos años de escolaridad necesita una persona para comprenderlas. Como resultado del estudio se concluyó que el 53.8% de las políticas analizadas estaban redactadas en un nivel de lectura superior al de la educación secundaria; es decir, requieren de una educación de nivel universitario para ser comprendidas (Milne, Culnan, & Greene, 2006).

Además, según datos del censo estadounidense utilizados por los autores, el 47.9 % de la población adulta no cuenta con ningún tipo de educación universitaria, lo que indica que aproximadamente la mitad de los consumidores no tiene el nivel

educativo necesario para comprender la mitad de las políticas de privacidad analizadas (Milne, Culnan, & Greene, 2006). Si trasladamos este análisis al contexto peruano, la situación resulta aún más alarmante, pues solo el 22.9 % de los jóvenes peruanos accede a educación universitaria (INEI, 2018), lo que indica que una proporción aún mayor de la población peruana carece del nivel educativo requerido para interpretar y comprender más del 50% de las políticas de privacidad estudiadas. Todo ello guarda concordancia con los resultados del reporte de 2019 del Pew Research Center, en el cual 63% de los ciudadanos estadounidenses encuestados afirmó que entienden muy poco o nada sobre las leyes y regulaciones actualmente vigentes para proteger sus datos personales (Pew Research Center, 2019).

Ahora bien, la lectura de las políticas de privacidad resultan complicadas incluso para los modelos de lenguaje más avanzados. Así lo comprobaron los investigadores Wasi Ahmad, Jianfeng Chi, Yuan Tian, Kai-Wei Chang, en su estudio de 2020 para desarrollar un sistema de respuestas, PolicyQA, aplicado para comprender las políticas de privacidad. Sin embargo, encontraron que incluso en condiciones controladas, entender el contenido y las consecuencias de las políticas de privacidad era difícil. En efecto, a pesar del uso de modelos de lenguaje avanzados, el rendimiento promedio en comprensión de políticas de privacidad no supera el 56 % F1 score, lo cual implica que incluso sistemas entrenados para leer y comprender tienen graves limitaciones al enfrentarse a textos de privacidad (Ahmad, Chi, Tian, & Chang, 2020).

Con todo ello, queda claro que la utilización del mecanismo de consentimiento en la práctica no cumple su función legitimadora, pues las políticas de privacidad son (i) largas, (ii) complejas y (iii) en la cotidianidad las personas no las leen ni las comprenden. Todo esto, agrava la situación, pues además de los problemas propios del procesamiento de datos mediante tecnologias de Big Data, el consentimiento, en la actualidad, termina siendo un acto meramente formal y se limita a otorgar un ilusión de control sobre los datos personales.

4. CAPÍTULO 3: El establecimiento de un nuevo enfoque y nuevas responsabilidades en la protección de datos personales

En el Capítulo 1 de la presente investigación se analizó el derecho a la autodeterminación informativa en el Perú y se concluyó que el contenido constitucionalmente protegido del derecho a la autodeterminación informativa consiste en el conjunto de facultades que tiene toda persona para ejercer control sobre su información personal a fin de enfrentar posibles abusos. Por su parte, en el Capítulo 2, se analizó el desarrollo normativo del consentimiento como mecanismo de protección de los datos personales y se estableció la existencia de incompatibilidades estructurales entre el consentimiento y las tecnologías de Big Data. Ello se debe principalmente al carácter inferencial, dinámico y exploratorio de esta y, por otro lado, a los estrictos requisitos de validez del consentimiento los cuales quedan obsoletos ante el tratamiento masivo de información.

Ahora bien, con el reconocimiento de todo ello no se pretende, de modo alguno, la aceptación resignada al uso del Big Data, ni una renuncia a la función crítica del derecho. Por el contrario, se parte de la premisa de que el derecho como ciencia social que regula la conducta humana debe adaptarse a los entornos tecnológicos actuales para seguir siendo efectivo, sin por ello abandonar sus principios fundamentales. Tal como menciona Ehrlich, “el centro de gravedad de la evolución del Derecho, tanto el presente como el pasado, no se encuentra en la legislación, ni en la jurisprudencia o en las decisiones judiciales sino que se encuentra en la sociedad misma” (citado en Cebeira Moro, 2008).

La presente investigación no pretende justificar las prácticas del tratamiento masivo de datos, sino regularlas mediante criterios renovados que se adapten a la realidad. Por lo tanto, el replanteamiento del consentimiento propuesto en la presente investigación no responde a un aceptación resignada ante estas nuevas tecnologías, sino debe interpretarse como un ajuste normativo necesario con el objetivo de tutelar adecuadamente el derecho a a la autodeterminación informativa.

4.1. La anonimización como alternativa al consentimiento

Hasta este punto, quedó claro que la normativa de protección de datos está diseñada para regular el procesamiento de información de carácter personal. Por lo tanto, la información considerada “no personal” no está sujeta a la normativa de protección de datos. Es decir, la información que no puede vincularse a una persona en particular queda excluida del marco regulatorio sobre protección de datos personales. Por otra parte, es posible convertir información considerada como personal en información que no pueda vincularse con una persona; es decir, en información no personal. Esto se lleva a cabo mediante un proceso de desvinculación, también llamado anonimización (Swire & Kennedy-Mayo, 2020).

Ahora bien, en la práctica, existen tres métodos para llevar a cabo el mencionado cometido:

1. **La anonimización:** Este método consiste en eliminar todo aspecto de la información que permita identificar a una persona. Ello es realizado de tal modo que la información personal no pueda ser atribuida a una persona incluso si es combinada con otras fuentes de datos (Swire & Kennedy-Mayo, 2020).

2. **La seudo anonimización:** Este método también consiste en retirar aspectos de la información que puedan hacer identificable a una persona. Sin embargo, a diferencia de la anonimización, con esta técnica si es posible revertir el efecto; es decir, es posible volver a un estado en el que la información sí era identificable (Swire & Kennedy-Mayo, 2020).

3. **La encriptación:** A diferencia de los anteriores métodos, la encriptación no consiste en retirar los aspectos identificables de los datos, sino transformar los datos a un formato ilegible mediante técnicas criptográficas

(Christensson, 2014). Este proceso, al igual que el de la seudo anonimización si es posible de ser revertido.

Si bien estos tres métodos son ampliamente utilizados en la práctica, lo cierto es que en el Perú solo se ha regulado expresamente la anonimización. Sin embargo, de manera indirecta, se ha regulado los otros dos métodos. En efecto, el proceso de anonimización está regulado expresamente en los artículos 2.14 y 14.8 de la Ley de Protección de Datos. Así, en el artículo 2.14 se define a la anonimización como un proceso irreversible mediante el cual se impide la identificación del titular de los datos. Por su parte, en el artículo 14.8, se reconoce a la anonimización como una alternativa al consentimiento; es decir, cuando los datos hayan sido anonimizados, el responsable del tratamiento puede hacer uso de ellos sin el consentimiento del titular.

Ahora bien, los otros dos mecanismos, el de encriptación y el de pseudo anonimización, son regulados de manera indirecta en los artículos 2.15 y 14.6 de la Ley y en el artículo 41 del Reglamento. En el artículo 2.15 se define a los procesos de disociación como aquellos procedimientos reversibles que hacen no identificable a una persona. Por su parte, en el artículo 14.6 se señala que cuando son llevados a cabo dichos procedimientos no será necesario contar con el consentimiento del titular. Por último, es necesario mencionar que en el artículo 41 del Reglamento, se señala cuál es el procedimiento para llevar a cabo los procesos de disociación.

Debe quedar en claro que en el Perú se consideran válidos tanto los procesos de anonimización como los de disociación, tales como la seudo anonimización y la encriptación. Siendo la diferencia entre los procesos de anonimización y los de disociación el hecho que unos son considerados irreversibles (anonimización) y otros reversibles (procesos de disociación).

No obstante lo señalado por la norma, debemos tener en consideración que los procesos de anonimización no son una garantía absoluta. Es decir, si bien estos

procesos tienen como objetivo que la reidentificación de las personas sea nula, en la práctica esto no es así, pues siempre existirá el riesgo de que los datos sean re identificados. En efecto, la anonimización absoluta no existe (Gil, 2016). Como menciona Elliot, la anonimización siempre tiene riesgo, lo diferencial con los otros métodos es que el riesgo es tan pequeño que, funcionalmente, se le considera como cero (Elliot, 2015).

Ahora bien, es necesario evaluar qué tan pequeño es ese riesgo a la luz de la nuevas tecnologías, tales como el Big Data. En efecto, cabe preguntarnos si es posible la reidentificación de las personas aun si sus datos han pasado por un proceso de anonimización. Para responder a esa pregunta utilizaremos el estudio empírico de los investigadores Luc Rocher, Julien M. Hendrickx e Yves-Alexandre de Montjoye, los cuales en 2019 buscaron estimar cuál era la probabilidad de una correcta reidentificación en el caso de bases de datos altamente anonimizadas (Rocher, Hendrickx, & de Montjoye, 2019). Así, se utilizó un modelo estadístico que permitió estimar cómo se distribuyen los atributos de las personas, incluso a través de bases de datos reducidas. En otras palabras, el modelo permitió estimar la precisión en la que la combinación de ciertos datos permiten identificar a una persona, incluso en los casos en los que se cuenten con atributos muy reducidos. Los resultados de este estudio demostraron que con tan solo 15 datos es posible reidentificar al 99.98% de los estadounidenses (Rocher, Hendrickx, & de Montjoye, 2019).

Asimismo, otro estudió demostró que la reidentificación es posible utilizando únicamente datos auxiliares anonimizados; es decir, datos que no contienen nombres ni identificadores directos. Nos referimos al estudio de 2008 de los investigadores Arvind Narayanan y Vitaly Shmatikov, en cual se aplicó un algoritmo a los datos anonimizados de Netflix sobre la calificación de películas de los usuarios para medir la precisión de la reidentificación. Los resultados demostraron que (i) con tan solo la calificación de 8 películas es posible la reidentificación del usuario con un 99% de precisión y (ii) para la reidentificación del 68% de usuarios es necesario

solo conocer 2 de las películas que vieron y la fecha de estas (Narayanan & Shmatikov, 2008).

Pero los estudios que demuestran la debilidad de la anonimización datan incluso desde inicios del siglo XXI. En efecto, en el año 2000, Latanya Sweeney demostró que la simple anonimización no garantiza una protección real sobre los datos personales. Para ello cruzó los datos recolectados del censo de Estados Unidos del año 1990 más el padrón electoral de Cambridge, Massachusetts con un conjunto de datos médicos anonimizados. En base a ello, se obtuvieron los siguientes resultados: (i) el 87.1% de la población estadounidense es identificable utilizando la combinación de solo tres atributos —zip code, género y fecha de nacimiento, (ii) 58.4% es identificable mediante el cruce de de los datos de la ciudad a la que pertenecen, género y fecha de nacimiento; y (iii) el 18.1% es identificable utilizando los datos del condado en el que viven, género y fecha de nacimiento (Sweeney, 2000).

Por todo ello, consideramos que la anonimización no es una alternativa completamente eficiente para la protección del derecho a la autodeterminación informativa en el contexto del tratamiento de datos mediante Big Data, debido al alto riesgo de reidentificación producto del avance tecnológico. La evidencia empírica revisada en este apartado ha demostrado que la anonimización es una condición frágil y altamente reversible en contexto tecnológicamente avanzados, en los cuales la reidentificación deja de ser un riesgo pequeño a convertirse en una realidad altamente probable.

4.2. El abandono total del consentimiento: paternalismo

El paradigma actual en el Perú es la autogestión de la privacidad, basado en el consentimiento como método por el cual las personas pueden controlar su información personal. En efecto, a través de este paradigma, la ley busca otorgar a los individuos el control sobre sus datos de tal manera que estos puedan ejercer su

derecho a la autodeterminación informativa. Como menciona Solove, “el núcleo de este control implica dar a la gente la facultad para decidir y dar su consentimiento para la recopilación, uso y divulgación de sus datos (D. Solove, 2014).

Como hemos demostrado en el segundo capítulo de esta investigación, este paradigma presenta serios problemas en el contexto actual, donde el estándar en el procesamiento de la información es el Big Data. Ello debido, principalmente, al uso de los datos secundarios y a la imposibilidad de definir las finalidades del tratamiento. Ante ello, la alternativa obvia es la opuesta: un esquema de regulación en el cual se elimine el consentimiento y se prohíba el uso de tecnologías de Big Data para el procesamiento de datos personales. No obstante, tal como se argumentará a continuación, esta solución es de índole desproporcionada y desconoce los posibles beneficios derivados de dichos tratamientos.

Este tipo de esquemas implican una relación de tutela sobre los intereses del ciudadano objeto de la medida aplicada. En este sentido, una norma de acción o prohibición encuentra justificación siempre y cuando sirva para evitar una lesión en el destinatario de la medida (Garzón Valdés, 1988). A través de las normas paternalistas se nos obliga a hacer determinadas cosas que, incluso, van en contra de nuestra voluntad, con la finalidad de evitar que nos causemos daño a nosotros mismos. Un ejemplo clásico de ello es el de los aportes jubilatorios. De esta manera, “el paternalismo jurídico sostiene que siempre hay una buena razón en favor de una prohibición o de un mandato jurídico cuando ello es necesario para evitar un daño de la persona a quien se impone la medida” (Garzón Valdés, 1988).

Teniendo ello en claro, cabe preguntarnos si, en el caso de la protección de los datos personales, una medida paternalista es la más idónea. Algunos autores han defendido esta posición. Por ejemplo, Allen sostiene que al ser la privacidad un valor esencial para toda sociedad democrática, esta debería imponerse (Allen, 2011). De igual manera, Cohen señala que la privacidad no debe ser intercambiada por otros bienes y que la renuncia a esta debe darse en casos excepcionales (Cohen, 2012).

Es cierto que existen incompatibilidades estructurales entre el consentimiento y las tecnologías de Big Data. Tal como se desarrolló en la sección 3.3 de la presente investigación, esta incompatibilidad, se debe, por un lado, al carácter inferencial, dinámico y exploratorio de esta y, por otro lado, a los estrictos requisitos de validez del consentimiento, los cuales quedan obsoletos ante el tratamiento masivo de información. Todo ello refuerza la idea de que la protección del derecho a la autodeterminación informativa no puede depender exclusivamente del consentimiento individual.

Ahora bien, el reconocimiento de esta situación —desde la perspectiva de esta investigación— no justifica una medida paternalista. En efecto, establecer cuándo un tratamiento de datos personales resultará beneficioso o dañino para el individuo no siempre es claro y dependerá de cada caso en particular. Asimismo, de establecerse una medida paternalista se estarían socavando los beneficios derivados del tratamiento mediante el Big Data. Como menciona Tene y Polonetsky, el uso de técnicas de procesamiento masivo ha permitido el avance en áreas como la salud, seguridad, económicas, etc; ello demuestra que la regulación del tratamiento de datos personales no solo debe considerar los potenciales riesgos derivados del consentimiento, sino los aspectos positivos de este (Tene & Polonetsky, 2013).

Por todo ello, la imposición de una medida paternalista no es la solución, debido a que el consentimiento continúa siendo fundamental para garantizar la autonomía de las personas (D. Solove, 2014). De lo contrario, se les estaría negando la participación a las personas sobre la toma de decisiones respecto de su información personal. Además, considerando que no se ha optado por medidas paternalistas en otros casos de actividades riesgosas, como en el caso del consumo de alcohol, tabaco o la práctica de deportes extremos, no existe justificación suficiente para limitar de manera estricta el tratamiento de datos personales mediante tecnologías de Big Data. Como menciona Solove, solo en los casos en los cuales los riesgos

superan a los beneficios, como por ejemplo el consumo de drogas, se precisa la implementación de una norma paternalista; no siendo el tratamiento de datos personales semejante a dichas actividades (D. Solove, 2014).

Por lo tanto, la sustitución del consentimiento por medidas paternalistas no resulta una opción viable. Lo cierto es que no existe una solución perfecta debido a lo complejo del tema; sin embargo, el consentimiento sigue siendo un elemento central para que las personas tengan cierto grado de control sobre su información personal.

4.3. Nuevos enfoques

Cómo se desarrolló en la sección 3.1 de la presente investigación, el consentimiento es el pilar sobre el cual el sistema regulatorio de protección de datos personales se construye[21]. No obstante ello, a continuación se expondrán una revisión de los principales fundamentos que respaldan esta premisa.

En primer lugar, esta afirmación tiene fundamento en el propio articulado legal. Por una parte, tenemos que la Ley de protección de datos personales establece en su artículo 5 el consentimiento es un principio general aplicable a todo tratamiento de datos personales. Ello, a su vez, es reafirmado por lo establecido en los artículos 13, inciso 5 y artículo 28 inciso 1 del mismo cuerpo normativo, los cuales consagran al consentimiento como regla general para todo tratamiento de datos. Ahora bien, es cierto que la norma establece otras bases jurídicas para el tratamiento de datos, pero estas son configuradas expresamente como excepciones al consentimiento. Lo cual refuerza la premisa de que el consentimiento se consagra como el principal mecanismo de protección de datos personales.

Por su parte, el Reglamento de la mencionada norma dedica íntegramente el Capitulo I del Titulo I al desarrollo al consentimiento, del consentimiento, abordando

[21] Agradezco a la profesora Karina Olano por sus valiosas observaciones y comentarios, los cuales contribuyeron al desarrollo de este apartado.

de manera detallada sus características, requisitos y condiciones de validez. Ninguna otra base de legitimación recibe un desarrollo normativo tan amplio y exhaustivo. Todo ello evidencia la vocación de los legisladores de establecer al consentimiento como la principal base de legitimación para el tratamiento de datos personales. Es importante añadir que esta orientación no es producto de la reforma reciente; por el contrario, esta es establecida desde el Antiguo Reglamento de protección de datos. En efecto, en este se mantuvo la estructura: se dedicó el Capítulo I del Título III íntegramente al desarrollo de la regulación del consentimiento. Así, se consolidó una línea interpretativa constante sobre el rol protagónico del consentimiento, como mecanismo primario de protección de datos personales.

En segundo lugar, la jurisprudencia del Tribunal Constitucional respalda esta hipótesis. En efecto, la primera sentencia en la que se señala expresamente que el consentimiento es la piedra angular del sistema de protección de datos peruano es en la sentencia recaída en el Expediente No. 3700-2010-PHD/TC. En ella se establece, en el fundamento 5, lo siguiente:

> "5. (...) resulta evidente que el actual marco normativo de protección de datos personales ha venido a ampliar la tutela del titular de dichos datos a efectos de resguardar de mejor manera su derecho a la intimidad y a la vida privada, pues no cabe duda que el consentimiento expreso para el tratamiento de datos se constituye, hoy, en la piedra angular para la creación de bases de datos".

Esta sentencia de fecha 7 de agosto de 2014, fue emitida por una anterior composición del Tribunal Constitucional, en un contexto normativo en el que aún se encontraba vigente el antiguo Reglamento de la Ley de protección de datos personales. Sin embargo, el 7 de febrero de 2025, el Tribunal Constitucional —ya con una nueva composición— reafirmó esta interpretación mediante la Sentencia No. 84/2025, recaída en el Expediente No. 01116-2022-PHD/TC. En esta ocasión

se estableció que la regla básica para el tratamiento de datos personales era el consentimiento:

> “9. También es importante precisar que, de manera general, en materia de tratamiento de datos personales (...) el consentimiento se comporta como el principio rector para el análisis de las conductas alegadas lesivas del derecho a la autodeterminación informativa (...)”

> “11. En tal sentido, es claro que para el legislador la regla básica para el tratamiento de datos personales es la existencia del consentimiento del titular del dato, pues de lo contrario, dicho tratamiento resultaría lesivo del derecho constitucional a la autodeterminación informativa y contrario a la Ley 29733”.

El hecho de que tanto la anterior como la nueva composición del Tribunal Constitucional coincidan en esta interpretación evidencia una línea jurisprudencial constante respecto del rol central del consentimiento como base prioritaria en el tratamiento de datos personales. En base a todo ello, queda demostrado que el consentimiento se erige como el principal mecanismo de protección de datos personales.

Ahora bien, este modelo presenta serios problemas en la práctica, en especial, en entornos donde los sistemas de procesamiento de información se llevan a cabo mediante el Big Data. En efecto, tal como se señaló en la sección 3.3 de la presente investigación, el consentimiento —tal como está planteado en la normativa peruana— resulta estructuralmente incompatible con las tecnologías de Big Data. Esta incompatibilidad deriva del carácter inferencial, dinámico e imprevisible inherente a este tipo de tecnologías.

Asimismo, debe quedar claro que ni anonimización, ni el establecimiento de medidas paternalista son solución para este problema. Es por ello, que se debe optar por un nuevo enfoque, el cual garantice el control efectivo de la información

personal de las personas, sin socavar su autonomía. Es importante tener en cuenta, que no existe una solución perfecta debido a lo complejo del tema; sin embargo, es necesario un explorar nuevos enfoques que garanticen el control efectivo de la información personal.

En primer lugar, resulta necesario replantear la estructura normativa actual en la cual el consentimiento es la regla general para el tratamiento de datos personales. Como mencionamos anteriormente, si bien la regulación actual establece excepciones al consentimiento, lo cierto es que las mismas operan como limitaciones puntuales al consentimiento y no están configuradas como verdades bases de legitimación autónomas. Es por ello que se propone transitar a un modelo estructural similar al de la Unión Europea, en el cual el consentimiento es solo una de seis bases de legitimación. Este cambio de enfoque es esencial para evitar jerarquías legales entre las bases legales y, así, otorgar a los responsables no solo la posibilidad de escoger otras bases más adecuadas a cada contexto, sino incentivar el uso de las mismas.

Ahora bien, es importante tener en cuenta que la sola adopción de la estructura del modelo europeo no resuelve el problema de fondo. En efecto, aunque la regulación del Reglamento General de Protección de Datos acierta al no establecer una jerarquía expresa entre sus bases de legitimación, lo cierto es que en la práctica el consentimiento sigue siendo la base de legitimación principal. De hecho, en el estudio realizado en 2019, en el cual se analizaron 1000 de los sitios web más populares en países de la Unión Europea, con el fin de determinar cómo se gestionaba la privacidad en ellos, se concluyó que 62% de estos sitios web utilizaban como base de legitimación al consentimiento (Utz et al., 2019). De igual manera, en el estudio conjunto realizado por OneTrust y la Data & Marketing Association del Reino Unido en 2022, en base a una encuesta a 224 profesionales de marketing, se concluyó que (i) el 56 % de los encuestados utiliza el consentimiento como su principal base legitimación y (ii) esta cifra se eleva al 63% en el caso de las organizaciones que implementan sistemas especializados de

gestión de consentimiento (Consent and Preference Management Platforms) (OneTrust & DMA, 2022).

Cabe entonces, preguntarse a qué se debe esta situación. Consideramos que esto se debe a que el consentimiento es la base que cuenta con mayor desarrollo normativo, lo que incluye requisitos estrictos de validez y estándares interpretativos más exigentes. Todo ello, en teoría la convierte en la base que menos ambigüedad genera en cuanto a la protección del derecho a la autodeterminación informativa. Esta afirmación es respaldada por el Centro de Liderazgo en Políticas de Información (CIPL) —organización global destinada a investigar acerca de la privacidad y las políticas de privacidad— el cual, en su informe técnico del año 2021, concluyó que las organizaciones se inclinaban a utilizar al consentimiento como base jurídica bajo la creencia de que esta otorga a las personas un mayor control y proporcionan mayor seguridad jurídica, ello incluso ante la existencia de otras bases jurídicas más adecuadas (Center for Information Policy Leadership, 2021).

Es por todo ello, que se considera que si bien es necesario replantear la estructura normativa actual —la cual gira en torno al consentimiento— lo cierto es que esta reforma debe ir más allá de la sola inclusión de una igualdad entre las bases de legitimación. Debe incluir un replanteamiento en el enfoque material del consentimiento y el desarrollo normativo de las demás bases.

En segundo lugar, es necesario que la regulación replantee su enfoque normativo. Actualmente, la regulación en materia de protección de datos se concentra en el momento de recolección de los datos, siendo este el momento en el cual se exige el consentimiento para legitimar el tratamiento. Este enfoque tiene como idea base que si el titular es correctamente informado sobre cómo se llevará a cabo el tratamiento y la finalidad del mismo, entonces este podrá libremente autorizar o rechazar dicho tratamiento, en ejercicio de su autonomía. Esta lógica se ve reflejada en los requisitos de validez del consentimiento establecidos en la normativa vigente, según la cual, el consentimiento debe ser (i) libre, (ii) previo, (iii) expreso, (iv)

inequívoco y (v) informado. En consecuencia, la legitimidad del tratamiento parte de la premisa de que el titular comprende las implicancias de sus decisiones y las adopta de forma voluntaria y consciente.

Como se señaló en la sección 3.1.1, este enfoque tiene sus orígenes en los Fair Information Practices Principles (FIPP), los cuales han servido como guía de regulación desde la década de 1970 (D. Solove, 2014). El segundo importante desarrollo que tuvo este paradigma fue introducido mediante la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de fecha 24 de octubre de 1995, en la cual se definió —en su artículo 2, literal "h"— al consentimiento como "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales". Estas características del consentimiento fueron luego interpretadas y ampliadas mediante la Opinión 15/2011 del Grupo de Trabajo del Artículo 29, del 13 de julio de 2011. En 2016, mediante la adopción del Reglamento General de Protección de Datos de la Unión Europea, estos criterios de validez del consentimiento se consolidan tomando como base todo lo desarrollado anteriormente.

En el caso peruano, mediante la Ley de protección de datos personales (Ley N.º 29733) se adoptó este enfoque con clara inspiración en el modelo europeo, tal como se reconoce en su exposición de motivos. El Antiguo Reglamento estableció y desarrolló los requisitos de validez del consentimiento. En esa misma línea, el Nuevo Reglamento reforzó aún más el modelo basado en el consentimiento, introduciendo mayores exigencias en cuanto a las condiciones de validez.

Es evidente entonces, que la tendencia en materia de protección de datos personales fue la de robustecer al consentimiento. Tal como mencionan Custers, De Hert y Van der Hof, con cada desarrollo en materia de protección de datos, las condiciones de validez del consentimiento se han reforzado (Custers et al., 2022). Sin embargo, es necesario tener en cuenta que este paradigma fue concebido en una etapa temprana del desarrollo tecnológico y, en específico, antes del auge del

Big Data. Cómo se desarrolló en el apartado, 3.2.1 de esta investigación, la empresa pionera en el desarrollo tecnologías de Big Data fue Google, mediante el diseño del modelo MapReduce en 2003. En efecto, el paradigma basado en el consentimiento fue concebido para entornos en los cuales el tratamiento de datos personales era más acotado y no se lidiaba con grandes volúmenes de información. Tal como mencionan Pistilli y Trevelin, el consentimiento fue ideado para contextos en los cuales el tratamiento de datos era estable y las finalidades razonablemente predecibles (Pistilli & Trevelin, 2025)

Bajo esas condiciones —previo al auge del Big Data, el consentimiento resultaba un herramienta funcional, pues el ecosistema tecnológico no estaba tan desarrollado y, por el contrario, era limitado. Todo ello, permitirá articular un consentimiento que cumpliese con los requisitos de validez exigidos por la norma con eficacia práctica. En este contexto, resultaba posible:

- Precisar —ex ante— las finalidades del tratamiento, debido a estas se construían directamente de los datos base recolectados.

- Debido a ese componente de previsibilidad, los responsables eran capaces de informar de manera específica y detallada cómo, cuándo y para qué se realizaría el tratamiento.

- Los tratamientos se realizaban sobre datos recolectados u observados de manera directa. Así, la posibilidad de acceder y utilizar datos de terceros —sin una recolección directa— resultaba prácticamente inconcebible.

Sin embargo, todo este escenario cambió radicalmente con la revolución tecnológica seguida de la invención y popularización del Internet en la década de 1970; pero, especialmente, con la irrupción de las tecnologías de Big Data. En efecto, ante el fenómeno de la creación y circulación masiva de información, el Big Data se presentó como la solución para el tratamiento eficiente de grandes y

diversos volúmenes de datos. Esta nueva forma de tratamiento trajo consigo varias innovaciones, siendo la creación de nuevo conocimiento mediante inferencias uno de sus principales atributos. Todo ello, transformó la lógica del tratamiento de datos tradicional, transitando de una enfoque estático, lineal y predecible, a uno dinámico y exploratorio. En este nuevo contexto, se redefinió lo posible:

- Mientras que antes, resultaba posible determinar ex ante las finalidades del tratamiento, con la irrupción del Big Data, esto resultaba incompatible. En efecto, pues las finalidades dependen de las inferencias obtenidas en la fase de procesamiento. Esto provocó que no fuera posible obtener un consentimiento previo, pues las inferencias se generan después del momento de recolección de los datos base.

- Mientras el modelo tradicional se caracterizaba por ser previsible, el tratamiento mediante Big Data se caracteriza por su inherente imprevisibilidad. Esta naturaleza imprevisible del Big Data hace estructuralmente inviable cumplir con el requisito de informar y delimitar de forma precisa las finalidades, pues dichos fines serán planteados a partir de las inferencias.

- Si en el contexto anterior resultaba impensable el acceso y utilización de datos de terceros, sin una recolección directa; con la irrupción de las tecnologías de Big Data esto cambió. En efecto, el Big Data demostró tener la capacidad de inferir datos sobre terceros sin la necesidad de mediar consentimiento.

Entonces, resulta claro que el tratamiento de datos mediante Big Data resulta estructuralmente incompatible con la versión tradicional del consentimiento. Teniendo en claro ello, resulta pertinente preguntarse por qué si la realidad ha cambiado, la normativa continúa aferrándose a un paradigma que ya no responde a esta nueva realidad. Como señalamos anteriormente, la tendencia regulatoria en

materia de protección de datos personales ha sido la de robustecer al consentimiento, sin cuestionar si este mecanismo es capaz de adaptarse a este nuevo contexto.

Sin embargo, no todo ha sido estático, se han introducido algunas modificaciones que muestran el inicio de un cambio de tendencia. En efecto, la incorporación de principios como la transparencia y la responsabilidad proactiva, demuestran que ha comenzado ha hacer un transición en el enfoque: de un sistema en el cual la legitimidad tenía como sustento únicamente en el consentimiento, hacía uno donde la legitimidad del tratamiento de datos dependiera tanto del consentimiento, como del comportamiento activo del responsable del tratamiento de datos. En el Perú, estos dos principios fueron introducidos, expresamente, en 2024, mediante la publicación del Nuevo Reglamento de protección de datos personales.

Además, otro de los avances normativos más significativos está relacionado con la modificación del derecho al tratamiento objetivo de datos personales. Este tiene como base al artículo 23 de la Ley de protección de datos personales, el cual reconoce el derecho del titular a no ser sometido a decisiones que produzcan efectos jurídicos que lo afecten significativamente con base exclusivamente en el tratamiento de datos. Mediante este derecho se busca proteger al individuo de usos abusivos o dañinos basados en el solo tratamiento de datos.

Este fue complementado mediante lo establecido en el artículo 72 del Antiguo Reglamento, el cual establecía que en los casos donde se realizara un tratamiento de datos sin participación del titular, se le debía informar a la brevedad posible. No obstante, consideramos que esta versión tenía un enfoque limitado, no desarrolló qué tipo de decisiones serían consideradas problemáticas y se centró únicamente en establecer una obligación de informar después de la decisión. Este panorama cambia de forma sustancial mediante la modificación introducida por el Nuevo Reglamento. En efecto, en el artículo 87 se señala lo siguiente: (i) se amplia el alcance del derecho, incluyendo a decisiones automatizar que puedan afectar al

titular y (ii) se establecen con mayor claridad qué tipo de decisiones son objeto de este derecho: aquellas que produzcan efectos jurídicos, discriminación o una afectación significativa.

Estas modificaciones reflejan un desplazamiento hacia un enfoque más enfocado en las responsabilidades del responsable respecto de las finalidades del tratamiento. En efecto, desde la perspectiva de esta investigación, este giro normativo representa una parte central de la solución al problema de incompatibilidad estructural entre el consentimiento tradicional y los desafíos que plantea el Big Data. Como señala Gil, el enfoque debe desplazarse hacía el momento de la utilización de los datos personales (Gil, 2016). Es decir, en lugar de establecer requisitos estrictos al consentimiento, se debe buscar formas de regular el uso sobre los mismos. De igual manera, Solove menciona que, actualmente, la regulación es neutral sobre el fondo de los tratamientos de datos (D. Solove, 2014); es justamente, esa neutralidad la que hay que dotar de contenido para asegurar que los titulares tengan un efectivo control de su información y evitar posibles abusos.

Ahora bien, es preciso preguntarnos si este cambio implica adoptar un enfoque paternalista. Desde la perspectiva de esta investigación se sostiene que no. Por el contrario, el propio legislador ya ha introducido elementos que van dirigidos a un cambio de enfoque en el cual la legitimación del tratamiento no de dependa exclusivamente del consentimiento del titular, sino esta se construya en base a las responsabilidades del responsable. Lo cual se evidencia con la introducción de los principios de transparencia y responsabilidad proactiva; pero además, con la imposición de límites al uso de los datos por parte de los responsables, como lo demuestra la regulación del derecho al tratamiento objetivo. En consecuencia, el hecho de reforzar y profundizar este cambio de enfoque supone la continuación de una evolución normativa que ya ha comenzado.

Además de ello, es necesario tener en cuenta que la propuesta no supone un abandono total del enfoque de autogestión de la privacidad. Por el contrario,

reconocemos que el consentimiento es una de las mayores expresiones de autonomía personal y su rol debe ser preservador en el sistema de protección de datos personales, pero con algunos matices considerando la revolución tecnologica y, en particular, el auge del Big Data. Así, el rol del mismo en el esquema de protección de datos no debe ser sobreestimado, pues como se evidencio a lo largo de esta investigación, el mismo plantea incompatibilidades estructurales para regular entornos donde el tratamiento de datos se hace mediante Big Data. Este aspecto se desarrollará con mayor profundidad en el último punto de esta investigación.

En este punto, resulta pertinente analizar por qué esta alternativa es cualitativamente mejor. Para responder a esta pregunta es necesario remontarnos al inicio: a la razón por la cual se protegen los datos personales. Tal como se expuso en el capítulo 1, esa razón la encontramos en el contenido constitucionalmente protegido del derecho a la autodeterminación informativa, entendido como el conjunto de facultades que tiene toda persona para ejercer control sobre su información personal a fin de enfrentar las posibles abusos. Teniendo ello en claro, es necesario reflexionar sobre si el modelo regulatorio actual —basado principalmente en el consentimiento de las personas— garantiza el respeto al contenido del derecho a la autodeterminación informativa, en especial, en los contextos donde el tratamiento se realiza mediante Big Data.

Cómo se desarrolló ampliamente en la sección 3.3 de la presente investigación, existe una incompatibilidad estructural entre el modelo de regulación basado en el consentimiento y las características inherentes del Big Data. Por lo tanto, continuar con un paradigma basado primordialmente en el consentimiento, el cual fue concebido para un contexto diferente —en el cual el tratamiento de datos era lineal, trazable y predecible— implica ignorar la realidad, marcada por el avance tecnológico y el tratamiento de datos mediante Big data, y, sobre todo, desatender los riesgos derivados de ella. Con todo ello, no se pretende presentar una solución definitiva. Sin embargo, lo que sí afirmamos es que resulta imprescindible y urgente

explorar nuevos enfoques regulatorios que permitan (i) adaptarse al avance tecnológico y (ii) devolver a las personas el control de su información en una era marcada por el Big Data.

Por último, es necesario que la norma acepte que el consentimiento no es un mecanismo totalmente idóneo para la protección del derecho a la autodeterminación informativa en la era del auge del Big Data. En efecto, se debe tener en cuenta que el paradigma actual en el cual se busca robustecer al consentimiento, mediante requisitos de validez, conduce a una protección débil de la protección de datos. Como menciona Solove, “en la práctica, el consentimiento es una ficción legal que rara vez se cumple” (D. Solove, 2014). A lo largo de esta investigación se ha hecho hincapié en los problemas que presenta el consentimiento,

Todo ello no implica que el consentimiento deba ser eliminado por completo del sistema de protección de datos personales. Por el contrario, con esto nos referimos a que el consentimiento debe ser revaluado y de manera tal que su rol goce de una verdadera legitimidad en el contexto actual. Así, las cosas el consentimiento tal cual está planteado debe seguir teniendo un rol importante en aquellos escenarios para los cuales fue originalmente concebido —o equivalente; es decir, casos donde el tratamiento sea sencillo y predecible. Tal como Wachter y Mittelstadt, el consentimiento está diseñado para gestionar input data; es decir, datos proporcionados directamente por el titular, no así para datos inferidos (Wachter & Mittelstadt, 2019). En otras palabras, el consentimiento debería reservarse únicamente para aquellos casos en los que el individuo posea efectivamente una capacidad real y plena de decisión sobre sus datos.

Ahora bien, frente a los tratamientos mediante Big Data, mantener como principal mecanismo de legitimación al consentimiento o simplemente simplemente reformarlo, sin un cambio de enfoque no resulta ni efectivo ni real. De hecho, la tendencia de la doctrina refleja ello. Como evidencia, en el estudio realizado por Emmanuel Nti Nkoah y Chandni Sawlani, el cual combinó la revisión de literatura

especializada privacidad y consentimiento —desde 2010 hasta 2024— con entrevista a expertos en la materia. Entre las conclusiones arribadas están las siguientes: (i) a pesar de los intentos en reforzar el consentimiento —como en el sistema de la Unión Europea, persisten desafíos para garantizar el control del titular sobre su información personal; (ii) en contextos digitales, el consentimiento rara vez es informado o voluntario; de hecho, los modelos basados en el consentimiento funcionan más como rituales o formalismos cuyo propósito —parece— estar orientado a eximir de responsabilidad a quienes tratan los datos que a empoderar a los usuarios; y (iii) la dependencia en exceso del consentimiento permite a las empresas cumplir formalmente con la regulación, sin asegurar el respeto a los derechos de los individuos (Nkoah & Sawlani, 2025).

Así, tal como señalamos en el punto anterior, será necesario un cambio de enfoque: transitar a un modelo donde la legitimidad del tratamiento no dependa —principalmente— del consentimiento, sino también de las obligaciones del responsable, así como de las finalidades que se les da a los datos personales, ya sean estos recolectados, observados o inferidos. Como Solove señala será necesaria la imposición de obligaciones a los responsables del tratamiento para que la ficción legal del consentimiento sea válida: (i) deber de obtener el consentimiento de manera adecuada, (ii) deber de evitar frustrar expectativas razonables, (iii) deber de lealtad y (iv) deber de evitar riesgos irrazonables (D. Solove, 2014).

Este cambio de enfoque como respuesta a la revolución digital es respaldado por varios autores. De hecho, otras de las conclusiones del estudio de Emmanuel Nti Nkoah y Chandni Sawlani fueron evidenciaron una consonancia en las siguiente necesidades: (i) las reformas estructurales que transfieran la responsabilidad del individuo hacia las instituciones; (ii) la adopción de limitaciones claras respecto a las finalidades del tratamiento y (iii) la reconceptualización de la privacidad como un derecho colectivo y no solo individual, teniendo en consideración que las consecuencias de los tratamientos de datos afectan a comunidades enteras, trascendiendo al individuo (Nkoah & Sawlani, 2025).

Resulta evidente entonces, que la regulación deberá reducir la amplia legitimidad que se le concede a este; es decir, se deberá optar por un enfoque restringido del consentimiento. Por lo tanto, la normativa deberá procurar mecanismos que hagan que la ficción del consentimiento sea lo más beneficiosa para los individuos. En otras palabras, si la regulación deberá asumir que (i) las personas están consintiendo, pero que (ii) este consentimiento carece de legitimidad total; entonces, la normativa deberá asegurar la implementación de qué mecanismos que hagan que este consentimiento presunto no sea perjudicial para las personas. Así, el hecho que una persona haya prestado o no su consentimiento, no será suficiente si el tratamiento en sí coloca a las personas en situaciones de vulnerabilidad, abuso o explotación.

Todo este cambio en la regulación en el sistema de protección de datos personales, responde a los desafíos que plantea el Big Data y, en general, el avance de la tecnología. Como se demostró en la presente investigación, la regulación actual no garantiza la protección del derecho a la autodeterminación informativa, pues, en la realidad, a pesar del consentimiento de las personas, el control de la información personal es realmente bajo.

5. Conclusiones

La presente investigación tuvo como objetivo principal determinar si el principio del consentimiento garantiza una adecuada tutela del derecho fundamental a la autodeterminación informativa en el marco de la sociedad de la información contemporánea. A partir del desarrollo y análisis realizado a lo largo de la investigación, se concluye que la regulación actual peruana sobre protección de datos personales basada en el principio de consentimiento no resulta eficaz para la protección del derecho a la autodeterminación informativa. A continuación se expondrán las ideas principales que sustentan esta conclusión:

1. El paradigma de organización social actual es el de la llamada “Sociedad de Información”, el cual se basa en la producción de conocimiento e información. En el contexto de la sociedad de información se produjo un fenómeno: la creación y circulación masiva de información. Ante ello, se creó un nueva tecnología capaz de procesar y extraer conocimiento ante la ola masiva de información: el Big Data.

2. Paralelamente, se desarrolló el derecho fundamental a la autodeterminación informativa como respuesta al desarrollo de la Sociedad de la Información, del Big Data y, en general, de las nuevas tecnologías desde 1970. En efecto, este derecho es reconocido a partir de las preocupaciones sobre la privacidad, intimidad y el control de la información personal.

3. Este derecho fue desarrollado principalmente en Europa y Estados Unidos. Los antecedentes del mismo los encontramos en la Ley de protección de datos (*Datenschutzgesetz*) en el Estado alemán de Hesse de 1970 y, en Estados Unidos, en el *Privacy Act* de 1974. Por su parte, respecto al desarrollo constitucional del derecho, se tiene como base a la sentencia del Tribunal Constitucional Aleman de 1983 (1 BvR 209, 269, 362, 420, 440, 484/83) y a las sentencias del Tribunal Constitucional Español 290/2000 y la 292/2000, las cuales establecieron que el derecho a la autodeterminación informativa: *(i)* forma parte del catálogo de derechos fundamentales; *(ii)* protege a los individuos contra la recopilación, almacenamiento, uso y difusión no autorizados de sus datos personales; y, *(iii)* goza de autonomía e independencia en relación al derecho a la identidad, derecho a la imagen y derecho a la intimidad.

4. En el Perú, se reconoció el derecho a la autodeterminación informativa en la Constitución de 1993, en el artículo 2.6. Posteriormente, los legisladores buscaron corregir y precisar la redacción del derecho a la autodeterminación informativa mediante la promulgación del Código Procesal Constitucional en 2004. En efecto, el artículo 61 inciso 2 del Código Procesal Constitucional de

2004 amplió el alcance y dotó de contenido al derecho a la autodeterminación informativa.

5. La precisión del contenido del derecho a la autodeterminación informativa se consolidó mediante la jurisprudencia del Tribunal Constitucional. Específicamente, en las sentencias recaídas en los Expedientes No. 666-1996-HD/TC, No. 1797-2002-HD/TC, y No. 04739-2007-PHD/TC. En estas decisiones, el máximo Tribunal estableció lo siguiente: *(i)* el contenido del derecho a la autodeterminación, el cual consiste en el conjunto de facultades que tiene toda persona para ejercer control sobre su información personal a fin de enfrentar las posibles abusos; *(ii)* la autonomía del derecho, diferenciándolo del derecho a la intimidad, imagen e identidad personal; y, *(iii)* las facultades del titular de los datos personales (acceso, actualización, rectificación, oposición y cancelación).

6. El desarrollo del derecho a la autodeterminación informativa se consolida con la publicación y entrada en vigencia de la Ley No. 29733 – Ley de protección de datos personales y su Reglamento. En estas normas se precisó el ámbito de aplicación, se establecieron definiciones claves para entender la cadena de tratamiento de datos, y se precisaron los principios rectores, entre ellos el principio de consentimiento.

7. El consentimiento es el principio rector más importante para la protección de datos personales. En efecto, tanto a nivel global, como nacional, se verificó que el consentimiento es la 'piedra angular' de todo el sistema de protección de datos personales. En efecto, si bien existen diferencias en las formas de consentimiento, tanto los modelos integrales como los sectoriales de protección de datos basan su regulación en el principio de consentimiento. Ello es así pues el consentimiento posee un atributo transformador de la moralidad: mediante el mismo, actos considerados inmorales o, incluso ilegales, se transforman en actos moralmente aceptables. Así, en los

sistemas de protección de datos personales, este es utilizado para otorgar legitimidad al tratamiento de datos.

8. En el Perú, el sistema de protección de datos personales se asemeja a los modelos de protección integrales, en los cuales: *(i)* existe y se aplica una norma general de protección de datos que centraliza la regulación a través de los diferentes sectores de la economía (Ley No. 29733 – Ley de Protección de Datos Personales y su Reglamento); y, *(ii)* existe una autoridad central responsable de la aplicación y cumplimiento de la regulación (Autoridad Nacional de Protección de Datos Personales).

9. Los modelos de protección integrales se basan en el consentimiento de tipo afirmativo[22] para legitimar el procesamiento de datos, esta característica también está presente en el modelo peruano. En efecto, de la lectura en conjunto de los artículos 13.5[23] y 14[24] de la Ley de Protección de Datos y del artículo 2[25] del Reglamento, se establece que el régimen peruano de protección de datos personales gira en torno al consentimiento, estableciéndolo como la regla general para el procesamiento de datos. Este consentimiento presenta características para ser válido: (i) libre, (ii) previo, (iii) expreso, (iv) inequívoco, e, (v) informado.

10. Ahora bien, en la Sociedad de la Información, el Big Data es el sistema de procesamiento estándar pues es capaz de hacer frente a los problemas de masificación de la información. Esta tecnología funciona a través de un ciclo de procesamiento compuesto por diferentes fases: (i) adquisición, (ii)

[22] El consentimiento de tipo afirmativo (también conocido como *opt-in*) es aquel que necesita de una acción voluntaria y explícita por parte del titular que exprese una autorización. Por su parte, el consentimiento de tipo implícito (también llamado *opt-out*) opera de manera tal que se presume que el titular de la información consiente el tratamiento de sus datos, salvo que este expresamente señale lo contrario.

[23] "Artículo 13. Alcances sobre el tratamiento de datos persona.- 13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco (…)".

[24] "Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales (…)"

[25] "Artículo 2. Características del consentimiento válido.- El consentimiento para el tratamiento de datos personales es válido si se cumplen las siguientes características: 1. Libre 2. Previo 3. Expreso e inequívoco 4. Informado"

limpieza, (iii) integración, (iv) análisis, (v) interpretación, y, (vi) aplicación del modelo. Mediante estas fases, el Big Data no solo analiza datos primarios, sino que su principal virtud recae en la generación de patrones y correlaciones. En efecto, mediante el Big Data es posible la inferencia de información personal, sin la necesidad de que esta sea brindada directamente por el titular de los datos.

11. Esta nueva forma de procesamiento de información personal desafía el modelo actual de protección de datos personales basado en el consentimiento. Ello debido a dos razones:

    i. **El reinado de las minorías:** Mediante la tecnología del Big Data es posible inferir información personal de un grupo amplio de personas sin la necesidad de contar con su consentimiento. Este fenómeno ocurre debido a que el Big Data utiliza datos de una minoría para establecer patrones que permiten inferir la información personal de un grupo de personas más amplio. Ello demuestra que incluso si un individuo decide no brindar su consentimiento para el procesamiento de su información, su derecho a la autodeterminación informativa puede verse vulnerado debido a que mediante el Big Data se puede inferir su información a partir de datos proporcionados por otras personas de su entorno. En ese sentido, es claro que el consentimiento pierde su función legitimadora, pues el procesamiento de datos personales puede efectuarse aun si el individuo no prestó su consentimiento.

    ii. **El cheque en blanco:** El Big Data tiene como uno de sus atributos principales el análisis de datos para descubrir y generar nuevo conocimiento a partir de ellos. Para esto, se utilizan patrones y correlaciones que permiten la generación de información inferida. Todo ello ocasiona que las finalidades del tratamiento sean imprevisibles, pues no se sabe con certeza cuáles son los datos que

serán generados por el Big Data. Sin embargo, ello genera una contradicción con el principio de consentimiento, el cual para ser válido (como vimos antes) debe ser: (i) libre, (ii) previo, (iii) expreso, (iv) inequívoco, e, (v) informado. En efecto, resulta irracional exigir un consentimiento con dichas características si los modelos de procesamiento se basan en la imprevisibilidad de los resultados. Es por ello que la forma en que se concibe el consentimiento en la Ley de Protección de Datos y en su Reglamento resulta inviable en el contexto del Big Data; es decir, un contexto donde establecer con exactitud las finalidades del tratamiento de datos personales no es posible.

12. Ante ello, es necesario establecer alternativas jurídicas al consentimiento. Este nuevo paradigma de protección deberá:

i. Abandonar la dependencia al consentimiento y adoptar un modelo basado en otras bases de legitimación, sin jerarquía entre estas. Un ejemplo de ello, es la regulación adoptada en la Unión Europea. En efecto, en el Reglamento General de Protección de Datos (RGPD)[26] se establecen múltiples bases de licitud para el tratamiento de datos personales, de las cuales el consentimiento es solo una de ellas y no es considerado como la regla general para el procesamiento de datos.

[26] "Artículo 6. Licitud del tratamiento
1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

ii. Incluir un cambio de enfoque, es decir, la regulación no debe centrarse en el momento de la recolección, sino en el control del uso de la información.

iii. Incentivar a las empresas a optar por modelos de privacidad por defecto[27].

iv. Reducir la amplia legitimidad que otorga el consentimiento, para ello se debe asumir que el consentimiento es una ficción. La regulación debe asumir que si bien las personas están consintiendo, lo cierto es que este consentimiento carece de legitimidad; por lo tanto, la normativa deberá asegurar la implementación de mecanismos que hagan que este consentimiento presunto no sea perjudicial para las personas. Así, el hecho que una persona haya prestado o no su consentimiento, no será suficiente si el tratamiento en sí coloca a las personas en situaciones de vulnerabilidad, abuso o explotación.

13. La presente investigación abordó otros dos enfoques como alternativa al consentimiento; sin embargo, ninguno de estos enfoques presenta una alternativa realista que (i) proteja efectivamente el derecho a la autodeterminación informativa y (ii) no vulnere la autonomía de las personas.

i. Anonimización: La normativa peruana lo establece como un mecanismo alterno al consentimiento[28], ello debido a que mediante el

[27] El modelo de privacidad por defecto son aquellos que incorporan un enfoque de protección de datos personales desde la arquitectura misma de la organización. Tal como señala la Agencia Española de Protección de Datos, la privacidad por defecto "implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso)" (Agencia Española de Protección de Datos, 2019). Mediante el mismo, la protección de los datos personales pasan a ser parte fundamental de toda organización que trate datos personales y no una mera exigencia legal.

[28] "Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales

mismo es posible desvincular la información personal de su titular, de manera tal que la información no pueda vincularse a una persona en particular. No obstante, los procesos de anonimización no son una garantía absoluta, debido al riesgo de reidentificación, el cual se agudiza en los contextos de uso de Big Data. En efecto, el Big Data, al trabajar con grandes volúmenes y variedades de datos, es capaz de crear modelos casi exactos de la realidad. Así, mediante las fases de análisis y de aplicación del modelo es posible inferir datos personales.

ii. **Abandono total del consentimiento:** En este esquema de regulación se adoptaría un modelo de protección de datos paternalista, en el cual se establecería de manera expresa los supuestos en los cuales el tratamiento de datos estaría permitido, obviando por completo la voluntad de los individuos. No obstante, una medida paternalista no resulta ser la solución, ello debido a que esta limitaría en extremo la autonomía de las personas. El uso del consentimiento es fundamental para garantizar la autonomía de las personas. Además, el establecer cuándo un tratamiento de datos personales resultará beneficioso o dañino para el individuo depende de cada caso en particular, lo que hace inviable el establecimiento de una medida paternalista.

14. Lo cierto es que no existe una solución perfecta debido a lo complejo del tema; sin embargo, es necesario un explorar nuevos enfoques que garanticen el control efectivo de la información personal de las personas. Lamentablemente, la regulación peruana se ha inspirado pasivamente en la regulación de la Unión Europea, sin adoptar una postura crítica respecto del enfoque planteado en dicha normativa. Como se evidenció en esta

---

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos: (…)
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación (…)"

investigación tanto los sistemas integrales como los sectoriales de protección de datos se basan —en mayor o menor medida— en el consentimiento como principal base de legitimación respecto de los tratamientos de datos personales. Es esto lo que constituye el problema central, si bien cada legislación ha introducido ajustes, la base —el consentimiento— del sistema de protección de datos no ha variado. Las aproximaciones planteadas en esta investigación estan basadas en análisis doctrinales, pues las legislaciones a nivel internacional no han variado sustancialmente desde la década de 1970.

6. Bibliografía

Agencia Española de Protección de Datos (2019). Guía de Privacidad desde el Diseño. https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

Ahmad, W. U., Chi, J., Tian, Y., & Chang, K.-W. (2020). *PolicyQA: A reading comprehension dataset for privacy policies*. In Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP) (pp. 7417–7431). Association for Computational Linguistics. https://doi.org/10.18653/v1/2020.findings-emnlp.66

Aletras, N., & Chamberlain, B. P. (2018). Predicting Twitter user socioeconomic attributes with network and language information. In *Proceedings of the 29th ACM Conference on Hypertext and Social Media*. ACM. https://doi.org/10.48550/arXiv.1804.04095

Alfonso Sánchez, I. (2016). La Sociedad de la Información, Sociedad del Conocimiento y Sociedad del Aprendizaje. Referentes en torno a su formación. *Bibliotecas. Anales de investigación*, *12*(2), 235–243.

Allen, A. (2011). *Unpopular PrivacyWhat Must We Hide?* Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195141375.001.0001

Alonso Secades, V. (2015). Big Data: la eclosión de los datos. *Cuadernos Salmantinos de Filosofía*, *42*(1), 315–330. https://doi.org/10.36576/summa.39755

Arroyo Revatta, L. V. (2021). *La protección de datos personales en el contexto del big data: una propuesta desde los derechos humanos* [Tesis de Licenciatura] Repositorio Institucional PUCP

Bustamante Alonso, N. B., & Guillén Alonso, S. T. (2017). Un acercamiento al Big Data y su utilización en comunicación. *Mediaciones Sociales*, *16*, 115–134. https://doi.org/10.5209/MESO.58112

California Office of the Attorney General. (2020). *Opinion No. 20-303*.

Cárdenas Cárdenas, R. M. (2019). Big Data el nuevo orden de la información y la comunicación. *Publicaciones e Investigación*, *13*(2), 93–99. https://doi.org/10.22490/25394088.3653

Castells, M. (2006a). *La era de la información: economía, sociedad y cultura* (4a ed.). Alianza.

Castells, M. (2006b). *La sociedad red: una visión global*. Alianza Editorial.

Castro Cruzatt, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *IUS ET VERITAS*, *18*(37), 260–276.

Cebeira Moro, A. (2008). *Pluralismo jurídico y Derecho vivo: la concepción sociológica de Ehrlich*. En *Paradigma. Revista de investigación jurídica* (pp. 79–98). Instituto Internacional de Sociología Jurídica de Oñati.

Cervera Fantoni, Á. L. (2008). *Comunicación total* (4a ed.). ESIC Editorial.

Center for Information Policy Leadership. (2021). *How the "legitimate interests" ground for processing enables responsible data use and innovation*.

Christensson, P. (2014). *Encryption*. Technical Terms.

Cohen, J. E. (2012). *Configuring the networked self.* Yale University Press.

Conesa, J., & Gómez, J. (2015). *Introducción al Big Data*. UOC.

Culnan, M. J., & Bruening, Paula. (2018). Privacy Notices Limitations, Challenges, and Opportunities. En *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press.

Custers, B., Fosch-Villaronga, E., van der Hof, S., Schermer, B. W., Sears, A. M., & Tamò-Larrieux, A. (2022). The role of consent in an algorithmic society: Its evolution, scope, failings, and re-conceptualization. In E. Kostas, R. Leenes, & I. Kamara (Eds.), *Research handbook on EU data protection*. Edward Elgar Publishing. https://doi.org/10.4337/9781800371682.00027

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, 25(2), 238–249. https://doi.org/10.1509/jppm.25.2.238

Dixon, P. (2006). *A Brief Introduction to Fair Information Practices*. World Privacy Forum. https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/

Eguiguren Praeli, F. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. *Themis Revista de Derecho*, *67*, 131–140.

El Emam, K., & Alvarez, C. (2015). A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques. *International Data Privacy Law*, *5*(1), 73–87. https://doi.org/10.1093/idpl/ipu033

Elliot, M. (2015). To be or not to be (anonymous)? Anonymity in the age of big and open data. *Computers, Privacy & Data Protection on the Move (CPDP)*.

Flores Torres, J. L. (2020). La sociedad y la comunicación desde la perspectiva de Manuel Castells de sociedad red. *Sintaxis*, *1*(5), 85–102. https://doi.org/10.36105/stx.2020n5.05

García, S., Ramírez-Gallego, S., Luengo, J., & Herrera, F. (2016). Big Data: Preprocesamiento y calidad de datos. *Novática*.

Garzón Valdés, E. (1988). ¿Es éticamente justificable el paternalismo jurídico? *Doxa. Cuadernos de Filosofía del Derecho*, *5*, 155. https://doi.org/10.14198/DOXA1988.5.08

Gellman, R. (2014). Fair Information Practices: A Basic History. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2415020

Gil, E. (2016). *Big data, privacidad y protección de datos* (1a ed.). BOE.

Gil, E. (2020). *El interés legítimo en el tratamiento de datos personales masivos.* [Tesis de Doctorado]. Universidad CEU San Pablo.

Gong, N. Z., & Liu, B. (2018). Attribute inference attacks in online social networks. *ACM Transactions on Privacy and Security, 21*(1), 1–30. https://doi.org/10.1145/3154793

González, F. (2019). Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales. *Cinta de moebio*, *65*, 267–280. https://doi.org/10.4067/s0717-554x2019000200267

Gonzalez, L. D. (2018). Control de nuestros datos personales en la era del big data: El caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, *21*(1). https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941

Günther, W. A., Mehrizi, M. H. R., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems, 26*(3), 191–209. https://doi.org/10.1016/j.jsis.2017.07.003

Hidalgo Zamora, Y. (2020). *EL PARADIGMA DEL DERECHO GLOBAL PARA LA PROTECCIÓN DE DATOS PERSONALES EN REDES SOCIALES* [Tesis de Licenciatura]. UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing.

Horvát, E.-Á., Hanselmann, M., Hamprecht, F. A., & Zweig, K. A. (2012). One Plus One Makes Three (for Social Networks). *PLoS ONE*, *7*(4), e34740. https://doi.org/10.1371/journal.pone.0034740

Hurd, H. M. (1996). The Moral Magic of Consent. *Legal Theory*, *2*(2), 121–146. https://doi.org/10.1017/S1352325200000434

IBM INSTITUTE FOR BUSINESS VALUE. (2012). *Analytics: el uso del big data en el mundo rea*. IBM Global Business Services.

Instituto Nacional de Estadística e Informática (INEI). (2018). *Estadísticas de la educación 2018* (Capítulo 9: Educación superior). https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1680/cap09.pdf

Kitchin, R., & McArdle, G. (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951716631130

Kleinig, J. (2010). The nature of consent. En F. G. Miller & A. Wertheimer (Eds.), *The Ethics of Consent: Theory and Practice* (1a ed., pp. 3–24). Oxford University Press.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Marmor, A. (2015). What Is the Right to Privacy? *Philosophy & Public Affairs*, *43*(1), 3–26. https://doi.org/10.1111/papa.12040

Mislove, A., Viswanath, B., Gummadi, K. P., & Druschel, P. (2010). You are who you know. *Proceedings of the third ACM international conference on Web search and data mining*, 251–260. https://doi.org/10.1145/1718487.1718519

Monleon-Getino, A. (2015). El impacto del Big-data en la Sociedad de la Información. Significado y utilidad. *Historia y Comunicación Social*, *20*(2), 427–445. https://doi.org/10.5209/rev_HICS.2015.v20.n2.51392

Moore, N. (1997). La sociedad de la información. En *Informe mundial sobre la información 1997/1998*. UNESCO-CINDOC.

Mubarak Aguad, L. (2017). El Internet, el Big Data y el tratamiento de datos personales. *Advocatus*, *036*, 205–223. https://doi.org/10.26439/advocatus2018.n036.4753

McDonald, A. M., & Cranor, L. F. (2008). *The cost of reading privacy policies*. I/S: A Journal of Law and Policy for the Information Society, 4(3), 543–568.

Narayanan, A., & Shmatikov, V. (2008). *Robust de-anonymization of large sparse datasets*. In 2008 IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2008.33

Niño, M., & Illarramendi, A. (2015). ENTENDIENDO EL BIG DATA: ANTECEDENTES, ORIGEN Y DESARROLLO POSTERIOR. *DYNA NEW TECHNOLOGIES*, *2*(3), [8 p.]-[8 p.]. https://doi.org/10.6036/NT7835

Nissebaum, H. (2018). Stop thinking about consent: it isn't possible and it isn't right. *Harvard Business Review*.

Nkoah, E. N., & Sawlani, C. (2025). *Beyond consent: Rethinking data privacy in the digital era*. *International Journal of Research Publication and Reviews, 6*(5), 2462–2466.

Ochoa Cardich, C. (2020). *El Estado Social en la Constitución de 1993: evolución, interpretación y proyección garantista en el Perú* (1a ed.). Palestra Editores.

Olivos, M. (2020). EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ. *IUS: Revista de investigación de la Facultad de Derecho*, *9*(1), 83–100. https://doi.org/10.35383/ius-usat.v9i1.338

OneTrust & Data & Marketing Association. (2022). *Consent management by the numbers: 2022 DMA report summary*. OneTrust. https://www.onetrust.com/blog/consent-management-by-the-numbers-2022-dma-report-summary/

Orrego, C. (2013). Una aproximación al contenido constitucional del derecho de autodeterminación informativa en el ordenamiento jurídico peruano. *Anuario de Derecho Constitucional Latinoamericano*, 311–330.

Pew Research Center. (2019). *Americans and privacy: Concerned, confused, and feeling lack of control over their personal information*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Pew Research Center. (2023). *How Americans view data privacy*. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Pistilli, G., & Trevelin, B. (2025). Can AI be Consentful? In *arXiv [cs.CY]*. https://doi.org/10.48550/ARXIV.2507.01051

Puyol, J. (2015). *Aproximación jurídica y económica al Big Data*. Editorial Tirant Lo Blanch.

Rawls, J. (1999). *A Theory of Justice*. Harvard University Press. https://doi.org/10.4159/9780674042582

Recio 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*, 1–24.

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). *Estimating the success of re-identifications in incomplete datasets using generative models*. Nature Communications, 10, 3069. https://doi.org/10.1038/s41467-019-10933-3

Santos Divino, S. B. (2019). Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos. *Derecho PUCP*, *83*, 179–206. https://doi.org/10.18800/derechopucp.201902.006

Schermer, B. W., Custers, B., & Van der Hof, S. (2014). The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-014-9343-8

Solove, D. (2014). Autogestión de la privacidad y el dilema del consentimiento. *Revista Chilena de Derecho y Tecnología*. https://doi.org/10.5354/0719-2584.2013.30308

Solove, D. J. (2023a). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4322198

Solove, D. J. (2023b). Murky Consent: An Approach to the Fictions of Consent in Privacy Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4333743

Sweeney, Latanya (2018). Simple Demographics Often Identify People Uniquely. Carnegie Mellon University. Journal contribution. https://doi.org/10.1184/R1/6625769.v1

Swire, P., & Kennedy-Mayo, D. (2020). *U.S. Private-Sector Privacy: Law and Practice for Information Privacy Professionals*. International Association of Privacy Professionals.

Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*.

Trejo, R. (1996). *La nueva alfombra mágica. Usos y mitos de Internet, la red de redes*. Fundesco.

Trovato, M. (2023). *Protección legal de datos personales inferidos*. Fundación Vía Libre.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field." In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 973–990.* https://doi.org/10.1145/3319535.3354212

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*, 2019(2), 494–620. https://ssrn.com/abstract=3248829

Westin, A. F. (1968). Privacy And Freedom. *Washington & Lee Law Review*.

Wirsch, A. (2014). *Analysis of a top-down bottom-up data analysis framework and software architecture design.* [Tesis de Maestría]. Massachusetts Institute of Technology. https://hdl.handle.net/1721.1/107346

World Economic Forum. (2011). *Personal data: The emergence of a new asset class*.

Xavier, H. (2024). *The Web unpacked: A quantitative analysis of global web usage*. En *Proceedings of the 20th International Conference on Web Information Systems and Technologies (WEBIST)* (pp. 183–190). SciTePress. https://doi.org/10.5220/0012905900003825

Zamudio, M. (2021). *El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. Límites y propuestas.* [Tesis de Maestría]. PUCP.

Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of Big Data. *Seton Hall Law Review, 47*(4). https://scholarship.shu.edu/shlr/vol47/iss4/2/