

**UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO**

ESPECIALIZACION EN DERECHO DE LA ECONOMÍA

**PRINCIPIOS PARA LA GESTIÓN DE LOS DATOS DE LOS USUARIOS DE
REDES SOCIALES EN VENEZUELA**

**Trabajo Especial de Grado, para optar al Título de Especialista en Derecho de la
Economía, presentado por:**
Ballester Martínez, Ana Julia, CI. V-25.235.800

Asesorado por:
Mag.. Guerrero Albornoz, Litsay

Caracas, enero del año 2025

AUTORIZACIÓN

Yo, Ana Julia Ballester Martínez, mayor de edad, domiciliado(a) en Caracas, portador(a) de la cédula de identidad número V-25.235.800, autor(a) del trabajo especial de grado titulado **“Principios para la gestión de los datos de los usuarios de redes sociales en Venezuela”** presentado ante la Universidad Monteávila para optar al título de Especialista en Derecho de la Economía, otorgo mi autorización a la Universidad para comunicar públicamente mi obra en su Repositorio Institucional.

Esta autorización es válida para que el trabajo especial de grado sea usado, divulgado y prestado, en formato impreso, digital, electrónico, virtual y para usos en redes, internet, intranet y en general por cualquier formato conocido o por conocer, donde se garantizará:

- El reconocimiento de mi autoría sobre la obra.
- La conservación de la obra entregada a través del Repositorio Institucional.
- La reproducción y/o transformación a cualquier formato, que permita su legibilidad en las diferentes herramientas ofrecidas por las tecnologías de información y comunicación.
- La visibilidad en internet a través de motores de búsqueda, directorios y demás medios de difusión del conocimiento interoperables con el Repositorio Institucional.

Caracas, 28 de enero de 2025.





Universidad
Monteávila



CARTA DE CONFIRMACIÓN DEL TUTOR

Quien suscribe, **Litsay Guerrero Albornoz**, C.I. N° 12950939, CONFIRMO QUE EL **TRABAJO ESPECIAL DE GRADO** presentado por el estudiante **Ana Julia Ballester Martinez**, C.I. V-25.235.800, cursante de la **Especialización en Derecho de la Economía** titulado **"Principios para la gestión de los datos de los usuarios de redes sociales en Venezuela"**, a la cual me comprometí en orientar desde el punto de vista académico que siguió los lineamientos y sugerencias que se le realizaron, de acuerdo con los requisitos exigidos por el Reglamento de Postgrado de la Universidad Monteávila.

A los 22 días del mes de enero de 2025.


Firma del Tutor

DATOS DEL TUTOR:

Nombre y Apellido: Litsay Guerrero Albornoz

Cédula: 12950939

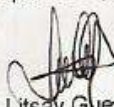
E-mail: lguerrero@profesor.uma.edu.ve

**Comité de Estudios de Postgrado
Especialización en Derecho de la Economía**

Quienes suscriben, profesores evaluadores nombrados por la Coordinación de la Especialización en Derecho de la Economía de la Universidad Monteávila, para evaluar el Trabajo Especial de Grado titulado: "PRINCIPIOS PARA LA GESTIÓN DE LOS DATOS DE LOS USUARIOS DE REDES SOCIALES EN VENEZUELA", presentado por la ciudadana: BALLESTER MARTINEZ, ANA JULIA, cédula de identidad N° V- 25.235.800, para optar al título de Especialista en Derecho de la Economía, dejan constancia de lo siguiente:

1. Su presentación se realizó, previa convocatoria, en los lapsos establecidos por el Comité de Estudios de Postgrado, el día **28 de enero de 2025**, de forma presencial en la sede de la Universidad.
2. La presentación consistió en un resumen oral del Trabajo Especial de Grado por parte de su autor, en los lapsos señalados al efecto por el Comité de Estudios de Postgrado; seguido de una discusión de su contenido, a partir de las preguntas y observaciones formuladas por los profesores evaluadores, una vez finalizada la exposición.
3. Concluida la presentación del citado trabajo, los profesores evaluadores en vista de lo novedoso en el abordaje del tema y que deja evidencia de la interdisciplinariedad del Derecho y la Economía, así como, el aporte que a la práctica de nuestra área realiza, decidieron otorgar la calificación de Aprobado "A" por considerar que reúne todos los requisitos formales y de fondo exigidos para un Trabajo Especial de Grado, sin que ello signifique solidaridad con las ideas y conclusiones expuestas.

Acta que se expide en Caracas, el día 28 del mes de enero de 2025.



Prof. Litsay Guerrero
C.I. 12.950.939



Prof. Alida Sabrina Matheus
C.I. 14.454.077



Dedicatoria

A mi mamá,
My Love, My Life.

Agradecimientos

A mi madrina,
por ser la luz en la oscuridad.

A mi papá,
por acompañarme sin preguntar ni juzgar.

A mis tíos,
por ser mis confidentes y consejeros.

A mi abuela,
por su amor incondicional.

A mi amor,
por aparecer y no soltarme.

A mis amigas,
compañeras de experiencias y risas.

A la profesora Litsay Guerrero Albornoz,
porque sus palabras, enseñanzas y su sinceridad fueron fundamentales
para la preparación de este trabajo.

A la profesora Alida Sabrina Matheus,
porque sus palabras de aliento me dieron
la motivación que necesitaba.

A todos los profesores de la
Especialización en Derecho de la Economía de la Universidad Montávila,
por ser una fuente constante de inspiración.

Principios para la gestión de los datos de los usuarios de redes sociales en Venezuela

Autor: Abog. Ana Julia Ballester Martínez

Asesor: Econ. Litsay Guerrero

Año: 2025

RESUMEN

En la sociedad actual, la tecnología es fundamental para la vida del ser humano, pues facilita la conexión entre individuos y diversos temas. Como producto de esta conectividad, surgen las redes sociales, estructuras creadas para vincular intereses comunes. Este Trabajo Especial de Grado aborda la creciente problemática de la gestión de datos de los usuarios por parte de las empresas que ofrecen servicios de redes sociales, en un entorno caracterizado por el auge de estas plataformas y la ausencia de una legislación específica sobre protección de datos en Venezuela. Se propone analizar el uso de los datos de los usuarios de redes sociales y las diversas implicaciones que conlleva compartir información con estas plataformas. Tomando como base el estudio del caso *Bundeskartellamt vs. Meta Platforms Inc.* (anteriormente Facebook, Inc.), se proponen principios adaptados al contexto venezolano, considerando sus particularidades legales, sociales y culturales, con el objetivo de orientar hacia una gestión ética y legal de los datos en redes sociales y subsanar el vacío legal existente, promoviendo así un entorno digital más seguro y respetuoso para los usuarios venezolanos. La investigación concluye con recomendaciones para la implementación de estos principios y futuras líneas de investigación.

Palabras Clave: *Derecho y Economía, Gestión de Datos, Redes Sociales, Protección de Datos, Privacidad, Usuarios y Consumidores.*

Principles for the management of social network user data in Venezuela

ABSTRACT

In today's society, technology is fundamental to human life, as it facilitates the connection between individuals and different subjects. As a product of this connectivity, social networks arise, structures created to link common interests. This Special Degree Project addresses the growing problem of the management of user data by companies that offer social networking services, in an environment characterized by the rise of these platforms and the absence of specific legislation on data protection in Venezuela. It is proposed to analyze the use of social network users' data and the various implications of sharing information with these platforms. Meta Platforms Inc. (formerly Facebook, Inc.), principles adapted to the Venezuelan context are proposed, considering its legal, social and cultural particularities, with the aim of guiding towards an ethical and legal management of data in social networks and filling the existing legal gap, thus promoting a safer and more respectful digital environment for Venezuelan users. The research concludes with recommendations for the implementation of these principles and future lines of research.

Line of work: *Law and Economics, Data Management, Social Networks, Data Protection, Privacy, Users and Consumers.*

ÍNDICE GENERAL

CARTA DE CONFIRMACIÓN DEL ASESOR

Carta de Aprobación del Trabajo Especial de Grado

Dedicatoria

Agradecimientos

Resumen

Abstract

Índice General

Introducción

CAPÍTULO I: EL PROBLEMA

Planteamiento del Problema.

Objetivos

Objetivo General

Objetivos Específicos

Justificación e Importancia

Alcance y Delimitación del Trabajo

CAPÍTULO II: MARCO TEÓRICO

Antecedentes

Bases Legales

Bases Teóricas

Nociones Generales sobre la Protección de Datos Personales.

Las Redes Sociales

Los Datos

Los Datos personales

Derecho a la Privacidad

Confidencialidad, Relación Contractual en las Redes Sociales y Contrato de Prestación de Servicios.

Tratamiento de datos personales

Uso de datos personales

Abuso de datos

Derecho al olvido

Derecho de la intimidad

Consensualidad

Contrato Informático

Contrato por Medios Electrónicos

Habeas Data

CAPÍTULO III: MARCO METEDÓLOGICO

Línea de Investigación

Tipo de Investigación

Diseño de Investigación

Técnicas y Herramientas de Recolección y Procesamiento de Datos.

Entrevistas Estructuradas

Resultados

Entrevista al Profesor Juan Esteban Korody Tagliaferro. Realizada el 4 de abril de 2024.

Análisis de la Entrevista realizada al Profesor Juan Esteban Korody Tagliaferro.

Entrevista al Profesor Daniel Betancourt Ramírez. Realizada el 5 de junio de 2024

Análisis de la Entrevista realizada al Profesor Daniel Betancourt Ramírez.

CAPÍTULO IV: LA TUTELA DEL CONSUMIDOR

I. Definición y relevancia de la Tutela del Consumidor

Usuario y Consumidor

Protección Jurídica de los usuarios y consumidores

Importancia en la Protección de los Derechos de los Consumidores.

II. El Paradigma de la Tutela del Consumidor.

Teoría Neoclásica del Consumidor.

III. Caso Bundeskartellamt vs Meta Platforms Inc (anteriormente Facebook, Inc)

CAPÍTULO V: PROPUESTA: Los Principios Rectores para la Protección de datos del Usuario en el ámbito de las Redes Sociales en el Ordenamiento Jurídico Venezolano.

Principio Del Consentimiento Informado

Principio del Empoderamiento del Consumidor y Usuario.

Principio de Recopilación Necesaria.

Principio de Autorregulación.

Principio de Educación.

Principio de Auditabilidad.

Principio de Colaboración.

Conclusiones

Referencias

Introducción

La necesidad de conexión entre seres humanos es una característica fundamental de nuestra especie, impulsándonos a comprendernos a nosotros mismos y al entorno que nos rodea. La Real Academia Española (RAE) define "conectar" como "Unir o poner en comunicación dos cosas o dos personas, o una con otra" o "Establecer comunicación entre dos lugares, o entre un lugar y otro" (RAE, s.f.). De estas definiciones se desprende el concepto clave de "comunicación", entendida por la RAE como la acción y efecto de comunicar o comunicarse, y como un trato o correspondencia entre dos o más personas. Esta necesidad innata de comunicación impulsa al ser humano a transmitir mensajes, experiencias y sentimientos, dando sentido al contexto social y cultural.

Con la innovación tecnológica, el internet y dispositivos como las computadoras y el fax, surgió el fenómeno de las redes sociales. En la década de 1990, la empresa Six Degrees, basada en la teoría de "Los seis grados de separación" que postula la conexión entre cualquier persona a través de una cadena de conocidos no mayor a seis individuos (BBC News Mundo, 2019), ofreció un servicio web pionero que permitía a los usuarios crear listas de contactos y enviar mensajes. Six Degrees fue precursora en la gestión de círculos sociales en línea. Posteriormente, surgieron empresas como Friendster (2002), enfocada en conectar personas con intereses comunes, la cual fue sucedida por MySpace y, finalmente, por Facebook.

Facebook, creada en 2004, se consolidó como una plataforma para conectar usuarios, compartir información, intereses y actividades en línea. Con 2.079,8 millones de usuarios activos mensuales (Statista, 2024), se ha convertido en una de las redes sociales más populares a nivel mundial. Sin embargo, su gestión de datos de usuarios ha generado un intenso debate en torno a la privacidad y la protección de derechos individuales.

La recopilación y el uso de datos personales (nombres, ubicación, preferencias, etc.) por parte de las redes sociales han sido objeto de escrutinio global. Organizaciones de defensa del consumidor, agencias gubernamentales y expertos en seguridad informática han expresado preocupación por la cantidad de información que los usuarios revelan y el uso que las empresas dan a estos datos. Los usuarios, atraídos por los beneficios de estas plataformas,

a menudo subestiman el valor de su información personal y, al aceptar los términos y condiciones, otorgan un amplio acceso a sus datos sin comprender plenamente las implicaciones. Esto plantea interrogantes cruciales: ¿Qué hacen las empresas con estos datos? ¿Cómo garantizan su seguridad? ¿Cuáles son los riesgos asociados a la recopilación masiva de datos?

Este problema es particularmente relevante en Venezuela, donde la regulación en materia de protección de datos aún está en desarrollo y la conciencia ciudadana sobre estos temas es limitada. La ausencia de un marco legal sólido crea un vacío que facilita prácticas potencialmente abusivas. Ante este escenario, es urgente desarrollar lineamientos claros para proteger la privacidad de los usuarios venezolanos en el entorno digital.

Esta investigación aborda la problemática desde la perspectiva del Derecho de la Economía, disciplina que estudia la interacción entre el sistema legal y el económico, buscando regular la actividad económica y proteger el interés público. El Derecho de la Economía, siguiendo los criterios metodológicos de las ciencias naturales, utiliza modelos formales basados en matemáticas y lógica para realizar predicciones verificables (Posner, 2015, citado en Osorio, 2021). Este enfoque permitirá analizar las implicaciones económicas de la gestión de datos y proponer soluciones que consideren tanto los derechos de los usuarios como el funcionamiento del mercado digital.

Esta tesis se estructura de la siguiente manera: el primer capítulo plantea la problemática, los objetivos y el alcance de la investigación. El segundo capítulo delimita las bases conceptuales y legales, analizando posturas doctrinales y jurisprudenciales nacionales e internacionales relativas a la protección de datos en redes sociales, y revisa los instrumentos normativos venezolanos relevantes. El tercer capítulo analiza el caso *Bundeskartellamt vs. Meta Platforms Inc.* en Alemania, desde la perspectiva del Derecho de la Economía, para extraer lecciones aplicables al contexto venezolano. Este caso ofrece un precedente valioso para comprender cómo las prácticas de gestión de datos pueden afectar la competencia y los derechos de los usuarios. El cuarto capítulo define el concepto de consumidor y el paradigma

de la tutela del consumidor. El quinto capítulo explora la racionalidad del individuo a la luz de las teorías económicas neoclásicas y analiza el uso y abuso de la gestión de datos.

En este sentido, la presente investigación busca explorar herramientas y mecanismos jurídicos, desde la óptica del Derecho de la Economía, para regular eficazmente la gestión de datos personales en redes sociales en Venezuela, fortaleciendo la protección de los derechos de los usuarios y el interés público. Se espera que los hallazgos y propuestas contribuyan al desarrollo de un marco normativo más robusto y adaptado a los desafíos del entorno digital venezolano.

CAPÍTULO I

EL PROBLEMA

En esta “era”, algunas de las acciones, conductas y problemáticas que se presenten en la vida cotidiana de los individuos pueden ser resueltas a través de herramientas digitales, un ejemplo de ello es la inteligencia artificial, que puede indicarle al individuo los lineamientos o bases para ejecutar tareas simples. Por ende, las plataformas digitales están creciendo aún más, y la influencia en las opiniones de políticas, cultura o temas digitales podrían ser fácilmente influenciadas con ciertos usos de las tecnologías digitales, tales como las redes sociales consideradas como “(...) *plataformas que permiten compartir información, entablar relaciones con diversos usuarios y ver información de ellos*” (Boyd y Ellison, 2007, citado por Gomez, Juan, 2021)

En un contexto global de creciente interconexión, los individuos generan un rastro de datos al interactuar con plataformas tecnológicas, datos que las empresas de redes sociales utilizan para conocer sus preferencias y hábitos. Esta evolución ha transformado las redes sociales, que han pasado de ser meras plataformas de socialización a convertirse en espacios donde la información de los usuarios se recopila y se explota con fines económicos. Este interés económico se nutre tanto de los comportamientos de los usuarios dentro de la plataforma como de la información que proporcionan al registrarse. Además, la

incorporación de funcionalidades de compra y venta directa ha permitido a las empresas monetizar aún más su presencia en estas plataformas.

Asimismo, las normativas a nivel global que tratan los temas del uso de los datos o información privada de los usuarios de las redes sociales intentan enfocar dichas normas en tratar problemas que la misma globalización ha provocado, tales como: la vulneraria que tiene el usuario de su propia seguridad o identidad al exponer sus datos personales dentro de aplicaciones tales como Meta (anteriormente Facebook), TikTok o Instagram, y, el enfoque en el cómo y para qué específicamente las mencionadas aplicaciones utilizan los datos de los usuarios.

Es por ello que la información que utilizan las redes sociales para identificar al usuario, tales como el nombre, apellido, país en el que reside, correo electrónico, edad, género, intereses y preferencias, es sumamente valiosa y sensible. Por ende, es necesario que los consumidores o usuarios manejen la mayor cantidad de información posible sobre cómo las empresas de redes sociales gestionan sus datos personales.

Un aspecto crucial a considerar es que las principales empresas que ofrecen servicios de redes sociales operan desde jurisdicciones extranjeras. Esta realidad plantea importantes desafíos para la aplicación de la legislación venezolana en materia de protección de datos, dificultando la efectiva tutela de los derechos de los usuarios ante posibles abusos o irregularidades.

Por lo cual, se encuentran las siguientes interrogantes: 1) ¿qué valor tienen los datos personales de los usuarios de las redes sociales?; 2) ¿dentro de los “Términos y Condiciones” de las redes sociales, los usuarios realmente tienen conciencia de la implicación que tiene compartir sus datos personales con la empresa?; 3) ¿en Venezuela, la legislación existente en materia de uso y protección de datos personales es suficiente y eficiente o si se deben establecer nuevos lineamientos sobre el tema?; 4) ¿qué datos específicos recopilan las redes sociales? ¿el usuario entiende que tiene derechos sobre el acceso y uso de sus datos personales?

Objetivo General:

Proponer principios de protección legal y eficaz para la gestión de datos personales de los usuarios de redes sociales en Venezuela, inspirados en el caso de *Meta Platforms, Inc.* (anteriormente *Facebook*) en Alemania.

Objetivos específicos:

1. Revisar la racionalidad del individuo mediante el estudio de la teoría neoclásica económica para determinar cómo valorar los datos de los usuarios de las redes sociales.
2. Estudiar la Teoría de la Tutela del Consumidor mediante la revisión doctrinaria para determinar su alcance en las redes sociales.
3. Evaluar las prácticas implementadas por *Meta Platforms, Inc.* (anteriormente *Facebook*) para la recopilación, almacenamiento y procesamiento de los datos personales de los usuarios para proponer principios que protejan los derechos de los usuarios en Venezuela.

Justificación e Importancia

Las redes sociales, en la era digital, se han convertido en un pilar fundamental de la interacción humana. Definidas por la Real Academia Española como “*Servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo*”.

Entonces, es fundamental que un servicio que se usa diariamente sea regulado bajo un marco normativo, es decir, las empresas que ofrecen servicios de redes sociales que recopilan y usan la información de los usuarios para obtener ganancias, diseñar estrategias de negocio o cualquier otro beneficio económico que obtengan de esos datos personales, deben ser reguladas a través de normativas, principios o políticas que supongan que el usuario

como titular de su propia información reciba la mayor protección y resguardo suficiente en un marco legal específico, y que dentro de su capacidad racional pueda entender por completo los “Términos y Condiciones” que establezcan dichas empresas, con la finalidad de tomar decisiones sobre qué información autoriza y desea que se comparta de él.

Es por ello que, el propósito de estudiar estas circunstancias en las que se encuentran los usuarios es explorar el cómo las empresas que ofrecen los servicios de redes sociales gestionan el uso de los datos personales de los usuarios. Asimismo, dicho estudio se hará a través del análisis del caso de *Bundeskartellamt vs Facebook, Inc*, donde este último recopilaba los datos de los usuarios a través de sus dispositivos, en conjunto con la información de sus cuentas de Facebook para ser utilizadas en los servicios corporativos de *WhatsApp, Oculus, Masquerade e Instagram*, todo ello sin el consentimiento de los usuarios (*Bundeskartellamt*, 2019).

Dicho comportamiento de *Meta Platforms Inc* (anteriormente *Facebook, Inc*), considerada como una de las plataformas sociales más influyentes de la era digital para la interacción social y la comunicación (Corcho, 2023, como se citó en Gavilanes, 2024), se revisará bajo los criterios que la doctrina y jurisprudencia de la protección de datos que la Unión Europea proporciona, ya que, no toda plataforma que recolecte datos lo estará haciendo “a cambio” del servicio que presta, pudiendo simplemente ser el caso de que la plataforma recopile esos datos para mejorar los servicios prestados a sus consumidores finales (Barrionuevo, E, 2019, como se citó en Caña, 2023)

Asimismo, junto al caso de *Meta Platforms Inc*, y el análisis de la normativa de la Unión Europea es posible entender o concluir si la misma verdaderamente protege al usuario ante cualquier vulneración de su derecho fundamental a la protección de sus datos, también permitirá identificar qué principios o lineamientos siguieron las autoridades europeas para determinar si existió un abuso de la gestión de los datos personales de los usuarios por parte de la mencionada red social.

Alcance:

Este proyecto, a partir del análisis del caso Bundeskartellamt vs. Facebook, Inc., busca proponer un conjunto de principios para la gestión de los datos de los usuarios de redes sociales en Venezuela. Para la elaboración de estos principios, se tomará como base la siguiente normativa, que incluye instrumentos de derechos humanos, la legislación venezolana y la jurisprudencia internacional, con el fin de identificar posibles áreas de mejora en la regulación actual:

1. Reglamento General de Protección de Datos de la Unión Europea (UE) 2018/1725.
2. Constitución de la República Bolivariana de Venezuela, publicada en la Gaceta Oficial Nro. 36.860 de fecha 30 de diciembre de 1999.
3. Ley Orgánica del Tribunal Supremo de Justicia publicada en la Gaceta Oficial Nro. 6.684 Extraordinario del 19 de enero de 2022.
4. Ley de Delitos Financieros publicada en la Gaceta Oficial Nro. 37.313 del 30 de octubre de 2001.
5. Ley de Infogobierno publicada en la Gaceta Oficial Nro. 40.274 del 17 de octubre de 2013.
4. Plan de la Patria 2019-2025 de Venezuela.

La idea principal de este Trabajo Especial De Grado se fundamenta en la necesidad que existe de proteger los derechos de los usuarios de redes sociales a través de una normativa y/o legislación específica sobre la gestión y uso de los datos personales de los usuarios de redes sociales en Venezuela.

CAPITULO II

MARCO TEÓRICO

Antecedentes.

El surgimiento de lo que se conoce como gestión o uso de datos de los usuarios ha puesto en movimiento constante al mundo del Derecho, que de por sí se caracteriza por ser dinámico y ajustable a los esfuerzos intelectuales de los individuos. En pocas palabras, el derecho busca evolucionar a medida que la sociedad avanza, y dentro de esa percepción se encuentra la tecnología, sus herramientas, y específicamente los servicios que ofrece, ya que estos últimos han sido objeto de múltiples trabajos académicos a lo largo de los últimos años que pretenden servir de antecedentes al objetivo principal, el cual es desarrollar unos principios de protección legal y eficaz a los usuarios de las redes sociales en Venezuela, Cedeño (2021) menciona que “En Venezuela carecemos de una legislación especial en materia de protección de datos personales y privacidad, como comentamos en el primer ensayo de esta serie, lo que implica preguntarnos en cuáles fuentes debemos apoyarnos para abordar este proceso legislativo” (p. 3).

Uno de los tantos trabajos que se pueden encontrar sobre protección de datos es "El acceso a la información de Datos Personales y derecho a la privacidad en los usuarios del Sistema Financiero" de Díaz Solari (2018). La autora se centra en el acceso a la información de los datos personales de los usuarios del Sistema Financiero. Díaz Solari destaca que, a pesar de la existencia de una normativa específica para la protección de datos, aún persisten vacíos legales que permiten a las entidades financieras acceder a la información de sus clientes sin su consentimiento previo. Este estudio resulta relevante para la presente investigación debido a que aborda un aspecto fundamental: el tratamiento y gestión de los datos personales por parte de las empresas. Aunque Díaz Solari se enfoca en el sector financiero, su análisis puede extenderse a otros ámbitos, como las redes sociales. Al comparar ambos contextos, se puede analizar la racionalidad del consumidor al proporcionar sus datos personales y evaluar el grado de conocimiento que los usuarios tienen sobre el manejo de su información en estas plataformas.

Un segundo trabajo de la autoría de Sebastián Cañas O (2023) en su obra “Abusos explotativos de posición dominante en precios en plataformas digitales y su aplicación a la explotación de datos” analizó lo siguiente:

En los mercados intermediados por plataformas digitales son vulnerables a la concentración del mercado, tales como: 1) Economía de escala y alcance; 2) Efectos de red positivos; 3) Acumulación de datos personales; 4) Integración vertical; 5) Costos de cambio elevados para los consumidores.

Es así, como se ha tomado en cuenta la obra previamente mencionada para el presente Trabajo Especial de Grado en virtud a la mención del manejo o gestión de los datos como “*factor distintivo de las plataformas digitales*” y las reflexiones en cuanto al caso de Bundeskartellamt vs Facebook, Inc.

En tercer lugar, otra autora interesada en las políticas de privacidad y protección de datos es Carolina D. Gavilanes (2024), cuyo proyecto de investigación se titula “Los riesgos contractuales de las plataformas digitales: caso Meta-Facebook”, el cual se enfoca en:

Abordar de manera detallada las complejidades y repercusiones de las políticas de privacidad implementadas por Meta-Facebook, considerando su impacto en los derechos digitales y la privacidad de los usuarios. Se examina minuciosamente cada cláusula de los términos y condiciones, destacando su extensión y complejidad, lo que dificulta su comprensión para la mayoría de los usuarios.

Asimismo, se han publicado una serie de artículos sobre la protección de datos y el tratamiento de los datos personales de los usuarios en diversas revistas académicas, en especial el artículo de las autoras Yadira Nieves-Lahaba y Gloria Ponjuan-Dante sobre el “Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia” donde realizan un trabajo de campo con la metodología de encuestas a estudiantes de distintas carreras, llegando a la conclusión de que:

El principal resultado fue que los estudiantes conceden gran importancia a tener derechos sobre los datos personales y en especial a poder oponerse o cancelar que estos se obtengan o se usen, pero por otra parte no son muy cuidadosos con la privacidad de estos pues comparten en su mayoría datos personales con amigos y conocidos.

Por otro lado, se publicó en el año 2023, un artículo del Centro de Competencia de Chile del autor mencionado previamente, Sebastián Cañas O., sobre la *“Explotación de datos personales como precio excesivo: Una revisión del caso Bundeskartellamt c. Facebook”*, dicho artículo expone que, en el año 2019 la autoridad de competencia alemana multó a la empresa Facebook por obligar a sus usuarios a ceder sus datos personales sin ninguna restricción, y comenta que algunos expertos consideran que la empresa también podría haber sido sancionada por cobrar precios excesivos a sus usuarios.

Como se ha podido observar a lo largo del desarrollo de este punto, existe una diversidad en cuanto a las investigaciones dedicadas al estudio y análisis de la situación planteada con respecto a la gestión y uso de los datos de los usuarios, así como a la privacidad y a los derechos de los usuarios en la era de la Big Data, en las distintas legislaciones nacionales o internacionales. Por lo cual, el presente Trabajo Especial de Grado cumplirá con la finalidad de proponer una serie de principios que reúna una forma de proteger el uso y evitar el abuso de las empresas a los datos personales de los usuarios de las redes sociales, con el propósito de que dichos parámetros sean factibles y se puedan aplicar dentro de una normativa venezolana especializada en el uso de los datos personales en las redes sociales.

Bases Legales

Se ha tenido la concepción de que el tema sobre la protección de datos de los usuarios surge con la llegada del internet, sin embargo, la necesidad que tienen los individuos de resguardar su privacidad ha sido evolutiva y en conjunto con la tecnología, de ello nace el derecho que tienen los individuos a su intimidad, y es así como en el artículo 12 de la Declaración Universal de Los Derechos Humanos proclamada por la Asamblea General de las Naciones Unidas en París, en fecha 10 de diciembre de 194, establece que: *“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”*.

Posteriormente, el artículo 8 del Convenio Europeo de Derechos Humanos firmado en Roma el 4 de noviembre de 1950, y entrado en vigor en fecha 3 de septiembre de 1953, trata

específicamente sobre el Derecho al respeto a la vida privada y familiar, determinando lo siguiente:

Artículo 8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Es ampliamente reconocido que las nuevas tecnologías, como las redes sociales, pueden representar una amenaza para el derecho a la intimidad de las personas. Esto se debe a que su vida personal puede quedar registrada en sistemas y plataformas de redes sociales, y dichos datos podrían ser transmitidos a otros servicios o utilizados sin el conocimiento de los usuarios. En respuesta a esta problemática, el 7 de octubre de 1970 surgió la primera ley especializada en materia de protección de datos, conocida como la Ley de Protección de Datos (Datenschutzgesetz), aprobada por el Land de Hesse en Alemania. Inicialmente, esta normativa se centraba en la protección de las personas físicas frente al tratamiento automatizado de datos personales por parte de entidades gubernamentales.

Posteriormente, las normativas en cuanto a la protección de datos de los usuarios se fueron creando en toda Europa y en U.S.A., algunos ejemplos de esas legislaciones fueron la Constitución de Portugal del año 1976 en su artículo 35 sobre la Utilización de la informática:

Artículo 35.1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.

2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.

3. Se prohíbe atribuir un número nacional único a los ciudadanos”.

Después se introdujo en la Constitución española de 1978 en el Capítulo Segundo sobre los Derechos y Libertades, específicamente en el artículo 18, numeral 4, se estipula lo siguiente:

Artículo 18. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”

En el mismo período, es decir, en el año 1978, se aprobó en Francia la Ley Nro. 78-17 sobre el procesamiento de datos informáticos, los archivos y la libertad.

Por su parte, Estados Unidos en cuanto a la protección de datos, comenzó con las publicaciones de los juristas americanos Samuel D. Warren y Louis Brandeis quienes publicaron un trabajo sobre el derecho a la privacidad, este fue el inicio hacia la regulación sobre la privacidad, ya que hacían referencia a los chismes y escándalos sexuales publicados en la prensa, así como a la denominada intrusión en el círculo doméstico (Polo, A, 2022), posteriormente, a través de diversos fallos o decisiones, se crean las leyes federales que forman parte del sistema legal de Estados Unidos, ya que cada estado también tiene sus propias leyes que quizás puedan regular los mismos temas que estas leyes federales, pero de una forma distinta.

Ahora bien, las leyes de Estados Unidos destacadas sobre la protección de datos sería la Ley de Protección de la Privacidad de Menores en Internet (COPPA) de 1998, la cual se aplica sobre la recopilación de información personal de niños menores de 13 años, también se encuentra la *Gramm-Leach-Bliley Act* (Ley de Modernización de Servicios Financieros) de 1999, la cual tiene como objetivo regular la privacidad y seguridad de la información financiera, y la Ley de Protección de Privacidad en Comunicaciones Electrónicas (ECPA) de 1986 dedicada a proteger la libertad de las comunicaciones electrónicas, tales como el correo

electrónico, conversaciones por llamadas telefónicas, ya que prohíbe la interceptación y el acceso y divulgación que no estén autorizadas sobre comunicaciones electrónicas.

Por su parte, otra legislación importante que se debe destacar dentro de este Trabajo Especial de Grado es la Ley Fundamental de la República Federal de Alemania de 1949, también llamada Ley Fundamental de Bonn, la cual acogió los conceptos de la dignidad humana y el libre desarrollo de la personalidad. Por otra parte, diversos países de Latinoamérica poseen un marco regulatorio sobre la protección de datos personales, por ejemplo, Argentina en su reforma constitucional de 1994 en su artículo 43 introduce el concepto del “habeas data”, posteriormente fue reconocida la Ley de Protección de Datos Personales Nro. 25.326 que establece la figura del habeas data y complementa el derecho a la autodeterminación informativa (Peruzzotti, M, 2024).

Hay que mencionar, además, que en Latinoamérica también existen diversas regulaciones sobre la protección de datos, por ejemplo, en la Constitución de la República de Ecuador, publicada en el Registro Oficial Nro. 449.20 de octubre de 2008, en su artículo 66, específicamente en el numeral 19 se establece lo siguiente:

Artículo 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley”.

Asimismo, Ecuador también posee una Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento Nro. 459, de fecha 26 de mayo de 2021, en el Artículo 10 contiene un catálogo de principios que regulan el ejercicio del derecho de privacidad y no divulgación, los más destacables de estos son:

Artículo 10. “1. Lealtad: El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así

como las formas en que dichos datos son o serán tratados. En ningún caso los datos personales podrán ser tratados a través de medios para fines, ilícitos o desleales”.

2. Transparencia: El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

3. Finalidad: Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida final. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación del tratamiento ulterior prevista.

4. Calidad y exactitud: Los datos personales que sea objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sea inexactos con respecto a los fines para los que se tratan.

En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales. Siempre que el

responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen su dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

A) Hubiesen sido obtenidos por el responsable directamente del titular.

B) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable.

C) Fuesen obtenidos de un registro por el responsable.

5. Confidencialidad: El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las casuales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.

Por otra parte, Colombia también posee una regulación de protección de datos personales, especialmente en la Constitución en el Artículo 15 “De los Derechos, las Garantías y los Deberes Artículos”, en el cual se recoge el derecho al Habeas Data, exponiendo lo siguiente:

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan

recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Reglamento General de Protección de Datos de la Unión Europea (“RGPD”)

A medida que el mundo avanzaba, también las normativas sobre la protección de datos se desarrollan y actualizan con la finalidad de proteger la privacidad y el alcance del uso de los datos de los individuos, es por ello que surge el Reglamento General de Protección de Datos de la Unión Europea denominado Reglamento (UE) 2016/679 dirigido a proteger las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

De acuerdo a la Comisión Europea “*El Reglamento es una medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital. Además, la existencia de una norma única pone fin a la fragmentación en distintos sistemas nacionales y a las cargas administrativas innecesarias*”.

Asimismo, el mencionado Reglamento se enfatiza en el tratamiento de datos por medio de un proceso de análisis de riesgos, exponiendo lo siguiente en sus Disposiciones Generales:

Artículo 1. Objeto.

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales”.

Pacto Internacional de Derechos Civiles y Políticos

Este Pacto es identificado como un tratado multilateral general que reconoce los derechos civiles y políticos, que establece los mecanismos para su protección y garantía, el mismo fue adoptado por la Asamblea General de las Naciones Unidas en fecha 16 de diciembre de 1966 y entró en vigencia en fecha 23 de marzo de 1976, este es legalmente vinculante y el Comité de los Derechos Humanos en el artículo 28 indica que supervisa la ejecución del mismo. En dicho Pacto, dentro de la Parte III, se establece en el Artículo 17 lo siguiente:

Artículo 17.

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

El mencionado artículo refleja el derecho a la privacidad del individuo, incluyendo su intimidad física y personal, también resalta el derecho a la confidencialidad de la información personal y que la toma de las decisiones de un individuo no interfieran con la colectividad ni las normativas establecidas. Ahora bien, como se ha podido

observar a lo largo de este punto, las normativas dedicadas a regular la protección de datos de los usuarios se han enfocado en su mayoría al derecho de la intimidad del individuo, no obstante, no es el caso en Venezuela, debido a que el mismo no posee un Marco Normativo exclusivo a la protección de los datos personales de los ciudadanos.

Normativa de la protección de datos en Venezuela.

Regular la protección de datos de los usuarios se ha enfocado en su mayoría al derecho de la intimidad del individuo. No obstante, no es el caso en Venezuela, debido a que el mismo no posee un marco normativo exclusivo a la protección de los datos personales de los ciudadanos, sino que dicha materia se encuentra regulada en diversos instrumentos jurídicos que la respaldan como una entidad y existencia propia dentro del ordenamiento jurídico.

Es así como de la necesidad de proteger la identidad del individuo la Constitución de la República Bolivariana de Venezuela de 1999 incorpora en su artículo 28 la figura del “Hábeas Data”, la cual es definida como *“El derecho que tiene toda persona de acceder y controlar la información personal restringida en bancos de datos públicos o privados”* (Quiroz, 2016, como se citó en Silva, 2024)

Asimismo, dentro del Artículo 28 de la Constitución se expone sobre los Datos Personales, a saber:

Artículo 28. Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de éstos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés por comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley

Seguidamente, el Artículo 60 de la Carta Magna se consagra el derecho sobre la protección del honor y privacidad, así como otros valores inherentes a los personales, tales como la buena fama y la intimidad, dicho Artículo expresa lo siguiente:

Artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos

Posteriormente, encontramos el Artículo 167 en la Ley del Tribunal Supremo de Justicia, que desarrolla la "Demanda de habeas data". En este se expone lo siguiente:

"Toda persona tiene derecho a conocer los datos que a ella se refieran, así como su finalidad, que consten en registros o bancos de datos públicos o privados; y, en su caso, exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos cuando resulten inexactos o agraviantes. El habeas data solo podrá interponerse en caso de que el administrador de la base de datos se abstenga de responder el previo requerimiento formulado por el agraviado dentro de los veinte días hábiles siguientes al mismo, o lo haga en sentido negativo, salvo que medien circunstancias de comprobada urgencia."

Por otro lado, la protección de datos también es reconocida y regulada a través de la Ley de Delitos Informáticos publicada en la Gaceta Oficial Nro. 37.313 del 30 de octubre de 2001, cuyo objetivo es brindar protección de los bienes jurídicos ante cualquier conducta delictiva que se manifieste a través de la tecnología de la información y la comunicación. Específicamente en su Artículo 20 el cual expone que:

Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas

a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

De modo similar sobre el uso de la tecnología se tiene la Ley de Infogobierno publicada en la Gaceta Oficial Nro. 37.313 del 30 de octubre de 2001, la cual regula el uso de las tecnologías de información por parte de todos los órganos del Poder Público en la gestión pública y en los servicios que brinda y en sus relaciones con los administrados y ciudadanos (Zubillaga, 2022). En definitiva, dicha normativa contempla un conjunto de derechos fundamentales que tienen los ciudadanos en relación con sus datos personales, específicamente sobre el acceso, la rectificación, cancelación y oposición que dichos datos personales sean tratados para determinados fines.

En cuanto a jurisprudencia venezolana sobre la protección de datos, se debe mencionar la Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia de fecha cuatro (04) de agosto de 2011, en la cual se fija el criterio de interpretación vinculante sobre el derecho a la protección de datos personales. En la mencionada sentencia, el demandante José Mandarín Hernández y otros, solicitó un recurso de nulidad por inconstitucionalidad contra el Artículo 192 del Decreto Nro. 1.526 de la Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras publicada en la Gaceta Oficial Nro. 5.555 del 13 de noviembre de 2001.

Con el mencionado caso, la Sala Constitucional *“(…) desarrolló ampliamente el ámbito de esos principios, incorporando por esta vía los derechos ARCO, e incluso, ciertas exigencias consagradas posteriormente en el RGPD, como, por ejemplo, la de contar con un “con- sentimiento previo, libre, informado, inequívoco y revocable”* (Zubillaga, 2022)

Asimismo, se procede a mencionar tales principios vinculantes:

1. El Principio de la autonomía de la voluntad: Lo cual comporta la necesaria existencia de un consentimiento previo, libre, informado, inequívoco y revocable para el uso o recopilación de datos personales.

2. El Principio de legalidad: La recopilación de datos personales comporta que la limitación a la autodeterminación informativa, sea el resultado de normas de rango legal. Así, cualquier limitación al derecho a la "autodeterminación informativa" es admisible en la medida que resguarde un interés general superior que la ley tutele directamente o se fundamente en la Constitución, advirtiéndose en todo caso que las restricciones deberán ser objeto de interpretaciones estrictas, por constituirse en normas restrictivas de derechos.
3. El Principio de finalidad y calidad: La recopilación de datos personales debe responder a finalidades, motivos o causas predeterminadas, que no sean contrarias al ordenamiento jurídico constitucional y sectorial, lo cual se constituye además en un requisito necesario para obtener un consentimiento válido de conformidad con lo indicado en el principio de autonomía de la voluntad.
4. El Principio de la temporalidad o conservación: La conservación de los datos se extiende hasta el logro de los objetivos para las cuales han sido elaborados, vale decir, que justificaron su obtención y tratamiento.
5. El Principio de exactitud y de autodeterminación: Los datos deben mantenerse exactos, completos y actualizados, respondiendo a la verdadera situación de la persona a la que se refieran, ya que toda actividad que comporte la recopilación de datos personales puede ser objeto de control, el cual posee cada ciudadano frente a la información que les concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, dignidad y su libertad ante las injerencias en la zona espiritual íntima y reservada de una persona o un grupo, especialmente de una familia, la cual comprende no sólo sus relaciones afectivas o sexuales, sino también la esfera de confianza que abarca toda la información de un sujeto como afinidad o parentesco, entre otras.
6. Principio previsión e integralidad: La tutela de los derechos fundamentales vinculados con la recopilación de datos personales, debe plantearse inicialmente en relación con la protección del individuo contra la recopilación, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona en los términos antes expuestos, pero el análisis de la posible afectación de sus intereses o derechos, no puede hacerse en todos los casos aisladamente -vinculado a registros de

información determinados-, sino necesariamente debe tomar en consideración los datos que integran otros registros y su posible vinculación, ya que si bien éstos pueden carecer en sí mismo de interés, alcanzan un nuevo valor o significado de referencia, en relación con otros sistemas de registro de datos, más aún si se tienen presentes los actuales avances tecnológicos, por lo que no puede afirmarse que algunos datos carezcan per se de interés o relevancia jurídica.

7. Principio de seguridad y confidencialidad: Corolario de los anteriores principios, es la necesaria garantía -según los casos- de confidencialidad, de no alteración de datos por terceros y del acceso a tales datos por parte de las autoridades competentes de conformidad con la ley. Por lo tanto, deberán adoptarse las medidas técnicas y organizativas que resulten necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.
8. Principio de tutela: Al respecto, cabe reiterar que:

En sentido amplio el derecho a acceder a la información y al conocimiento del fin (...) se trata de derechos que han de ser ejercidos previamente (incluso extrajudicialmente y tal vez hasta por vía administrativa en algunos casos) ante el recopilador real o supuesto, por lo que la lesión al titular de los derechos nace de ese ejercicio extrajudicial fallido. Si se le niega extrajudicialmente el ejercicio, porque no se le da acceso a la información, se le da errónea, o no se explica legalmente para qué se registra, se le infringe su situación jurídica que nace directamente de la Constitución. (Cfr. Sentencia de esta Sala N° 332/01).

9. Principio de Responsabilidad: La violación del derecho a la protección de datos personales debe generar de conformidad con el ordenamiento jurídico aplicable, sanciones de tipo civil, penal y administrativas, según sea el caso.

Finalmente, es importante señalar que el Plan de la Patria 2019-2025 de Venezuela, si bien establece las líneas generales del proyecto político del Estado venezolano, no contempla medidas o acciones específicas para proteger los datos personales de los usuarios. Aunque el documento menciona de manera general el impulso a políticas y marcos legales, no existe ningún apartado específico que aborde o profundice en materia

de protección de datos personales o privacidad. Esta omisión representa una oportunidad perdida para establecer un marco legal sólido y actualizado en esta materia.

Es fundamental considerar que, hasta la fecha, el marco legal venezolano carece de un dispositivo específico que aborde la protección de datos en el ámbito de las redes sociales. Esta situación genera una serie de desafíos, tanto para los usuarios, quienes ven comprometida su privacidad, como para las autoridades, que enfrentan dificultades para hacer cumplir sus derechos. Además, es necesario establecer un sistema de sanciones claras y efectivas para disuadir a las empresas de violar la normativa vigente y garantizar el cumplimiento de las medidas de protección de datos.

Bases teóricas

Nociones Generales sobre la Protección de Datos Personales.

Según la autora Marianela Zubillaga (2022) “No hay actividad alguna del quehacer humano que no esté sujeto a la irrupción tecnológica. El derecho se enfrenta a tal realidad y luce un tanto lento e inoperante, frente a los nuevos fenómeno” (p. 227).

Esta reflexión representa el origen de la necesidad de proteger los datos personales y que hoy en día tienen un valor económico para las empresas que ofrecen servicios de redes sociales, sin embargo, no es precisamente el dato de la persona sino su tratamiento e interacción con otras aplicaciones o si esa información es valiosa para crear un proyecto o negocio, en pocas palabras, es el uso que se le da a la información del individuo y si esa información se puede transformar en un producto útil para la empresa.

Desde una perspectiva de Derecho y Economía, la protección de datos personales puede analizarse a través de la teoría de la elección racional. Esta teoría postula, principalmente, que los individuos establecen una relación de preferencia entre diversas situaciones, toman decisiones y eligen de forma que se maximice su beneficio, es decir, es aquella situación en la que un agente (económico, político, social, empresa, etc.) tiene preferencias transitivas y estas le dan la mayor utilidad posible (Vidal, 2008, citado en Gutiérrez Cruz & Moreno Brid, s.f.).

En este contexto, los individuos, al decidir compartir sus datos personales, realizan un cálculo costo-beneficio en el que sopesan los beneficios esperados (como una experiencia de usuario más personalizada o acceso a servicios gratuitos) frente a los costos potenciales (como la pérdida de privacidad o el riesgo de fraude). No obstante, esta racionalidad individual se ve limitada por la asimetría de información existente entre los usuarios y las empresas, lo que dificulta una evaluación precisa y completa de los riesgos asociados a la divulgación de datos personales.

Asimismo, la protección legal de los datos personales busca nivelar el juego entre individuos y entidades que manejan información personal. En este contexto, el derecho a la protección de datos se erige como un mecanismo fundamental para garantizar que los ciudadanos puedan ejercer un control efectivo sobre su información, este derecho protege a los individuos contra el uso no autorizado de sus datos personales, que podría generar perfiles que afecten negativamente su vida personal, social o profesional (Rodríguez, 2004, como se citó en Silva, 2024)

- **Las Redes Sociales:**

Las redes sociales exhiben una dualidad económica fundamental. Desde la perspectiva de los usuarios, estos actúan como consumidores que buscan satisfacer sus necesidades de interacción social y acceso a contenido digital, a menudo impulsados por incentivos como la validación social a través de mecanismos como los "me gusta". Simultáneamente, las empresas que operan estas plataformas se comportan como productores en un mercado digital, cuyo objetivo primordial es la maximización de sus beneficios económicos. Esta interacción genera un ecosistema complejo donde las motivaciones de usuarios y empresas pueden converger o divergir, planteando interrogantes sobre el equilibrio de poder y la protección de los derechos de los usuarios en este contexto económico particular.

También es importante destacar que, las redes sociales han emergido como actores principales en la transformación digital, proporcionando plataformas para la interacción social en línea. Estos espacios virtuales han creado comunidades virtuales donde los usuarios comparten información, opiniones y experiencias de manera instantánea. La capacidad de

conectarse con amigos, familiares y comunidades de intereses comunes ha redefinido las dinámicas sociales (Hugo et al., 2019, como se citó en Gavilanes, 2024).

Asimismo, de acuerdo a Mariliana Rico Carrillo (2012), se tiende a asociar las empresas *Meta Platforms Inc* (anteriormente *Facebook*) con las redes sociales, sin embargo, estas empresas “presentan los servicios para la instalación de la plataforma electrónica donde funciona la red social; en su condición de prestadores de servicios de la Sociedad de la Información, estas empresas están sometidas a un régimen jurídico específico.

La protección legal de los datos personales, como ya se ha visto, busca garantizar que los individuos puedan tomar decisiones informadas sobre el uso de sus datos. Sin embargo, en la práctica, la interacción social en línea, facilitada por las redes sociales, plantea nuevos desafíos. Como señala Mariliana Rico Carrillo (2012), la actividad de los individuos en estas plataformas es una de las principales fuentes de problemas en el ámbito de la protección de datos. Esta dinámica, caracterizada por la generación constante de contenido y la interacción entre usuarios, crea un entorno en el que la privacidad puede verse comprometida de múltiples formas.

Otro concepto que se desprende de la definición anterior y que es fundamental para la presente investigación es la denominada “Web 2.0”, cuya definición la hace Fernando Ureña (2008) y expone que es la transición que se ha dado de aplicaciones tradicionales hacia aplicaciones que funcionan a través de la Web enfocadas al usuario final. Se trata de aplicaciones que generen colaboración y de servicios que reemplacen las aplicaciones de escritorio.

Sumado a esto, Raúl Santiago Campión (2012) establece que: Los resultados de un número relativo importante de estudios y análisis de la Web 2.0 coinciden en definirla como un conjunto de herramientas que promueven la participación online, en lo que a la creación de contenidos y participación social se refiere.

- **Los Datos**

Ahora bien, otro elemento medular en el presente trabajo de investigación son los datos personales, no obstante, primero se debe delimitar la definición de “datos” y la Real Academia Española (RAE) precisa lo siguiente: “1. *Información sobre algo concreto que permite su conocimiento exacto o sirve para reducir las consecuencias derivadas de un hecho.* 3. *Información dispuesta de manera adecuada para su tratamiento por una computadora*”.

Por otro lado, otra definición bastante extensa sobre los datos indica lo siguiente:

Los datos son el elemento vital del desarrollo económico: constituyen la base de muchos nuevos productos y servicios, lo que conduce a un aumento de la productividad y una mayor eficiencia en el uso de los recursos en todos los sectores de la economía, lo que permite, a su vez, que haya productos y servicios más personalizados y se mejore no solo la elaboración de políticas sino también los servicios públicos. Es un recurso esencial para las empresas emergentes y las pequeñas y medianas empresas (pymes) a la hora de desarrollar productos y servicios. La disponibilidad de datos es fundamental para entrenar a los sistemas de inteligencia artificial” (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, 2020, como se citó en Zubillaga, 2022)

- **Los Datos personales:**

Los “datos personales” o de carácter personal son toda información que pertenece a una persona, independientemente si esta es natural o jurídica, que permita identificar directa o indirectamente a dicha persona. (Díaz y Zambrano, 2024)

Los datos personales son definidos legalmente como aquella información relativa a los individuos ya sea numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. (Porven H, Y, Morejón, Y Pérez V, 2021)

Por otra parte, los datos personales son todos aquellos que identifican a una persona, como por ejemplo su nombre, número de cédula, dirección, y cualquier otro que permita

saber que esa persona se encuentra constando como tal en un determinado territorio dentro de un Estado. Por tal razón cuando nace una persona se le registra en el Registro Civil, para que no sea un fantasma para sociedad y el Estado y desde aquí nace el primer banco de datos de un ser humano, ya que consta en esta institución. (Silva, 2024, pp 46-47)

Según los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la Organización de los Estados Americanos (OEA, 2021), el término 'datos personales' abarca una amplia gama de información que puede identificar a un individuo de manera directa o indirecta, incluyendo datos biométricos, de localización, y aquellos relacionados con características físicas, psicológicas, económicas, culturales o sociales. En otras palabras, cualquier información que pueda asociarse a una persona específica, ya sea en formato digital o físico, constituye un dato personal. Sin embargo, es importante destacar que la definición excluye la información que no permite identificar a un individuo de manera razonable.

En cuanto al tratamiento de datos o la gestión de datos habría que delimitar ambos conceptos, por una parte, el tratamiento de datos acorde a los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la Organización de los Estados Americanos (OEA), mencionado previamente, establece que el “Tratamiento de Datos” es uno de los Principios y “(...) *se usa en un sentido amplio y abarca toda operación o conjunto de operaciones realizado con Datos Personales, incluyendo, de manera enunciativa más no limitativa, la recopilación, acceso, organización, adaptación, indexación, aprovechamiento, registro, almacenamiento, recuperación, divulgación o transferencia*”.

Asimismo, los Datos Personales incluyen los identificados como el nombre real, alias, dirección postal, identificador personal único, identificador en línea, dirección de protocolo de internet, dirección de correo electrónico, nombre de cuenta, número de seguridad social, número de licencia de conducir, número de pasaporte u otros identificadores similares, o información comercial, información biométrica, información de internet u otra actividad de redes electrónicas (como historial de navegación, historial de búsqueda e información sobre la interacción de un Titular con un sitio web, aplicación o anuncio, datos de geolocalización, información de audio, electrónica, visual, termal, olfatoria u otra similar, información

profesional o relacionada al trabajo, información educativa e inferencias derivadas de lo anterior para crear un perfil de las preferencias, características, tendencias psicológicas, predisposiciones, comportamiento, actitudes, inteligencia, habilidades y aptitudes del Titular de datos, entre otras. (OEA, 2021, p. 24)

En este sentido, acorde a diversos ejemplos de la Comisión Europea, los datos personales pueden ser:

- “nombre y apellidos,
- domicilio,
- dirección de correo electrónico, del tipo nombre.apellido@empresa.com,
- número de documento nacional de identidad,
- datos de localización (como la función de los datos de localización de un teléfono móvil) (*),
- dirección de protocolo de internet (IP),
- el identificador de una cookie (*),¹
- el identificador de la publicidad del teléfono,

los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona.

- **Derecho a la Privacidad**

¹ (*) Cabe señalar que, en algunos casos, existe una legislación sectorial específica que regula, por ejemplo, el uso de los datos de localización o el uso de las «cookies»: la Directiva sobre intimidad y comunicaciones electrónicas (Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 (DO L 201 de 31.7.2002, p. 37) y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004 (DO L 364 de 9.12.2004, p. 1) ”.

La Comisión Económica para América Latina y el Caribe (CEPAL) al definir Privacidad lo delimita desde el “Derecho a la privacidad” que se refiere al estar libre intrusiones o perturbaciones en la vida privada o en los asuntos personales. Toda investigación debe esbozar estrategias para proteger la privacidad de los sujetos involucrados, y también sobre cómo el investigador tendrá acceso a la información. Los conceptos de privacidad y confidencialidad están relacionados, pero no son lo mismo. La privacidad se refiere al individuo o al sujeto, mientras que la confidencialidad se refiere a las acciones del investigador.

- **Confidencialidad, Relación Contractual en las Redes Sociales y Contrato de Prestación de Servicios.**

La Comisión Económica para América Latina y el Caribe (CEPAL), en la sección de su página web de Bibliografías define la Confidencialidad de la siguiente forma:

La confidencialidad se refiere al acuerdo del investigador con el participante acerca de cómo se manejará, administrará y difundirá la información privada de identificación. La propuesta de investigación debe describir las estrategias para mantener la confidencialidad de los datos identificables, incluidos los controles sobre el almacenamiento, la manipulación y el compartir datos personales.

Ahora bien, en relación a la relación contractual, García (2020) indica que:

Debe distinguirse claramente el consentimiento contractual del consumidor de su consentimiento para el tratamiento de sus datos personales, lo que con frecuencia no suele producirse en el contexto de los contratos de suministro de contenidos y servicios digitales en los cuales los clausulados ligan ambos consentimientos.

Es importante destacar que, el acuerdo de confidencialidad se encuentra inmerso dentro de la relación contractual que se produce entre el usuario y la empresa que ofrece los servicios de red social. Es así, como los autores Sánchez Cano, M, y, Matute, Romero (2021) afirman que, la relación jurídica que surge entre el usuario y la empresa que gestiona la red social podría calificarse como un contrato de prestación de servicios.

Asimismo, atendiendo a lo anterior, el contrato de prestación de servicios comprende una noción económica más que jurídica y, en consecuencia, ha de interpretarse en términos económicos, dejando de lado las obligaciones que derivan del contrato en virtud de la ley aplicable al mismo. De este modo, cabría interpretar que el contrato de prestación de servicios sería aquel cuyo objeto principal es la realización de una actividad consistente en dar, hacer o no hacer una cosa, a título oneroso, gratuito o lucrativo. (Calvo, Carava, Carrascosa González, 2018, como se citó en Sánchez Cano, M, y, Matute, Romero, 2021)

- **Tratamiento de datos personales**

Entre los considerandos del Reglamento de la Unión Europea (UE) 2016/679 se especifica que, el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Asimismo, dentro de la esfera del tratamiento de los datos personales se destaca el consentimiento informado del titular de la información, la cual debe de ser libre, específica, inequívoca e informada, no solo para el acceso de sus datos sino además para saber cuál será su finalidad, es decir, el conocer a detalle el uso que se le va a dar a los datos personales, e implica que este consentimiento no resulta la renuncia de su titular. (Arteaga, 2024)

- **Uso de datos personales**

Siguiendo las delimitaciones anteriores y las implicaciones de las acciones que implica recolectar, almacenar, procesar, divulgar, transmitir o eliminar datos, el uso de los datos personales se podría definir como una acción que recae directamente sobre los datos personales de una persona natural o jurídica que sea identificable, con el propósito de proveerle un servicio, personalizar su experiencia de usuario, realizar estudios de mercado o cumplir con obligaciones legales.

Además de ello, es importante destacar que, el uso de los datos personales se basa en el consentimiento expreso del usuario y se debe llevar a cabo bajo las más estrictas medidas de seguridad con el fin de garantizar la confidencialidad en la relación.

- **Abuso de datos**

Dentro de las definiciones y sobre la protección de datos, se puede conseguir el límite del uso de esos datos, que sería el Abuso de Datos, el abuso es descrito según la Real Academia Española (RAE) en sus primeras definiciones es delimitado como “*Hacer uso de algo de modo excesivo o indebido*”. Ahora bien, como el propósito del presente Trabajo Especial de Grado se centra en el uso y abuso de los datos personales, el término “abuso” está relacionado a los derechos fundamentales infringidos o tratados de una incorrecta en ese ámbito.

- **Derecho al olvido**

En el contexto digital, la jurisprudencia ha reconocido el derecho al olvido como un elemento importante del derecho a la intimidad. Este criterio implica el derecho de los individuos a solicitar la eliminación de información personal obsoleta o irrelevante que pueda afectar su privacidad (Allán, 2023, como se citó en Gavilanes 2024)

El Derecho al Olvido (DO) representa una garantía de normas y principios que otorgan la potestad de olvidar cierta información en particular, si bien en el momento de la emisión correspondiente generó importancia, ahora afecta al individuo al tener los datos publicados en la red. Frente a esta problemática surge el DO como una institución desarrollada en el ámbito del hábeas data, cuyo sustento expresa que la existencia de información publicada en internet que no tenga importancia por el paso del tiempo o que sea negativo para la persona, se elimine u oculte en el marco de la protección de datos. (Puchana, 2020, como se citó en Avellán, Y, Mendoza, 2022)

- **Derecho de la intimidad**

El derecho a la intimidad es una faceta fundamental de los derechos individuales que abarca la esfera privada de una persona, protegiendo su capacidad de controlar y resguardar información personal y experiencias íntimas. Este derecho se considera esencial para el desarrollo humano y la autonomía, reconociendo la importancia de mantener ciertos aspectos de la vida fuera del escrutinio público. Su inclusión en diversas declaraciones de derechos humanos y constituciones resalta su carácter universal y su relevancia en sociedades democráticas (Valenzuela, 2020, como se citó en Gavilanes, 2024).

El derecho a la intimidad personal se ha catalogado como derecho de la personalidad, esto refiere a características, rasgos y cualidades que conforman la manera de ser de una persona que la diferencia de las demás. Es un derecho primordial innato que nace con la persona, sin que sea necesario acto jurídico alguno que origine la adquisición de este derecho, pues éste, imputa al titular una potestad y amplia disposición para proteger todo lo concerniente a la propia persona y las cualidades que la definen. La personalidad es determinada por el nacimiento y se extingue con la muerte, porque legalmente, es una condición connatural de la persona. (Baño C, Y, Reyes E, 2020)

Por su parte, al titular de este derecho se le atribuye la capacidad de limitar que cualquiera se inmiscuya o pueda disponer de información en algunos de los ámbitos protegidos de su vida privada, y, faculta a su titular la potestad de impedir el conocimiento ajeno sobre cualquier información que puede incluirse dentro de su esfera privada. (Gibelalde A, 2022)

El derecho a la intimidad es el que protege la esfera personal y privada de un individuo contra intrusiones no deseadas. Este derecho implica que las personas tienen el control sobre su información personal, así como el derecho a mantener ciertos aspectos de su vida fuera del escrutinio público. El derecho a la intimidad puede abarcar aspectos como la privacidad en el hogar, la correspondencia personal, la información médica, los datos financieros, entre otros. Este derecho varía en alcance y aplicación según las leyes y regulaciones de cada país, pero es un componente fundamental de los derechos humanos reconocidos internacionalmente. (Cuellar, 2016, como se citó en Arteaga, 2024)

- **Consensualidad**

Acorde al Reglamento de la Unión Europea (UE) 2016/679 en su Artículo 11 numeral 4 estipula que, el consentimiento del interesado se define como 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.

Ahora bien, en fecha 10 de abril de 2018, el Grupo de Trabajo de la Unión Europea, en el Artículo 29 (GT29) adoptó las Directrices en cuanto al consentimiento en el sentido del Reglamento 2016/679 y estas fueron aprobadas por el Comité Europeo de Protección de Datos en la primera reunión plenaria, en dicha reunión se discutieron los elementos para un consentimiento válido, explicando que según la definición mencionada en el párrafo anterior, esa manifestación de libertad debe ser 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.

Por su parte, el Reglamento 2016/679 (Artículo 7, numeral 1) también establece condiciones adicionales para obtener consentimiento válido: (...) Cuando el tratamiento se lleva a cabo con el consentimiento del adoptadas interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento.

El responsable del tratamiento debe garantizar que el interesado pueda retirar su consentimiento en cualquier momento y que será tan fácil retirarlo como lo fue darlo. (Artículo 7, numeral 3). Además de las anteriores concepciones, el consentimiento es definido por Rebolledo (2019) en Polo (2020) como una facultad de la libertad del individuo para decidir acerca de sus datos, constituye la capacidad de autodeterminación del individuo y equivale en el mundo de las comunicaciones, a extender la capacidad de decisión de la persona con el fin de proteger su libertad y sus derechos en el mundo tecnológico.

- **Contrato Informático**

Este tipo de contrato comprende bienes físicos o lógicos -*hardware* o *software*- o, incluso, la prestación de servicios que sirven de apoyo y complemento de la actividad informática, como los de mantenimiento, corrección, desarrollo, certificación, entre otros. Aunque

mantiene dependencia electrónica por ser este el medio más común para su ejecución, su esencia no se encuentra en el medio por el cual se manifiesta la voluntad. Sino en el objeto sobre el cual recae el contrato. Existen diversos de ejemplos de este tipo de contrato, un ejemplo de estos contratos pueden ser la compra de un ordenador o un virus, la elaboración de software, etc. (Benavides et al., 2021)

Sin embargo, otro ejemplo muy común de un contrato informático en la actualidad es el que aceptamos al utilizar redes sociales u otras aplicaciones. Al crear una cuenta y aceptar los términos y condiciones, estamos celebrando un contrato con la empresa que provee la plataforma. En este acuerdo, se establecen los derechos y obligaciones tanto del usuario como de la empresa, incluyendo aspectos como el uso de la información personal, la responsabilidad por el contenido publicado y las condiciones de uso de la plataforma.

- **Contrato por Medios Electrónicos:**

Este tipo de relación contractual consiste en un acuerdo de voluntades que tiene lugar por medios electrónicos. Es decir, la existencia de este depende de la oferta y/o aceptación realizada a través de medios electrónicos, los cuales ejercer una influencia decisiva o real en la formación de la voluntad, el desarrollo o la interpretación del contrato. Son los más utilizados en internet ya que estos crean transacciones con bienes tangibles o intangibles. (Benavides et al 2021)

- ***Hábeas Data***

Acorde a la Constitución de la República Bolivariana de Venezuela de 1999, el “*hábeas data*” es una acción constitucional, consagrado en el Capítulo III De Los Derechos Civiles, específicamente en el Artículo 60, delimitando que:

Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

Asimismo, dentro de varias reflexiones que hace el autor Silva Gustavo (2024), en su obra “La naturaleza jurídica del Habeas Data y el Derecho a la protección de datos personales”, este delimita lo siguiente sobre esta acción constitucional en conjunto con la protección de datos:

“El hábeas data nace como un mecanismo para proteger el derecho a la protección de datos personales, y que la palabra protección no solo indica ocultar, si no también acceder, modificar y en ciertos casos eliminar; la segunda, no todos los datos personales son de carácter reservado, si no que existen ciertos datos que son de dominio público por lo la mayoría de personas con la que se ha interactuado alguna vez, va a tener conocimiento de esto; tercero, los datos sensibles no siempre son susceptibles de ser de carácter reservado, como pasa con el pasado judicial, ya que esto no está oculto y puede estar a la vista de todos; por último, no se puede alegar que los datos sensibles es información reservada y pretender con esto cohibir el derechos de las otras personas a acceder a la información pública” (p. 46).

El habeas data es una garantía jurisdiccional que constituye un mecanismo procesal que permite la protección constitucional de ciertos derechos frente al impacto que ha tenido las nuevas tecnologías de la información y comunicación. (Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., & Santillán Molina, A. L. (2022)

El objeto del hábeas data es proteger a las personas frente al tratamiento, especialmente electrónico, de sus datos personales, ofreciendo una defensa procesal contra la discriminación y otras violaciones de derechos fundamentales que puedan resultar de la divulgación de información privada o íntima, motivada por el avance tecnológico. De esta forma, el hábeas data protege los derechos fundamentales de tercera generación, como la intimidad y la privacidad, ante las posibles violaciones derivadas del acceso y la divulgación de información y datos de todo tipo. En consecuencia, el hábeas data consagra la posibilidad de rectificar, actualizar, eliminar o anular datos personales contenidos en cualquier base de datos (Arce, 2009, como se citó en Gárate, Reina, Samaniego, & Loyola, 2021)

En este capítulo se han explorado los distintos términos, conceptos y términos que son fundamentales para poder comprender la gestión de datos de los usuarios en las redes sociales. Además de ello, se han identificados las regulaciones internacionales y naciones que recogen los principios fundamentales para regular el tratamiento de datos. Sin embargo, la implementación efectiva de las regulaciones y de los mencionados principios presenta desafíos significados en el ámbito legal de Venezuela. Por lo cual, se consideró que, los futuros legisladores deben profundizar en el análisis del impacto de las nuevas normativas en la protección de datos, así como en el desarrollo de herramientas tecnológicas para mejorar la privacidad de los usuarios.

CAPÍTULO III

MARCO METODOLÓGICO

Línea de Investigación.

Derecho de la Economía.

Tipo de Investigación.

Para la ejecución del presente Trabajo de Investigación, se establece una investigación de tipo proyectiva, la cual según el autor Hurtado (2024), en su obra “Investigación Cualitativa: Fundamentos Epistemológicos, Teóricos Y Metodológicos”, se define como:

“Aquella que se ocupa de la creación de propuestas, inventos y programas, entre otras cosas, para dar respuesta a una situación, a partir de un proceso de indagación metódica que genera conocimiento nuevo. Este concepto abarca tres procesos: en primer lugar, la investigación, pues la propuesta se construye a partir de los hallazgos de un proceso investigativo -no de un mero proceso de documentación-. en segundo lugar, la creatividad, porque implica la generación de algo que no existe, o que tiene características novedosas, y, en tercer lugar, la planificación y el diseño, porque requiere de la creación de algo nuevo.”(pp 16-17).

Esto se debe a que se pretende aportar una propuesta que pueda otorgar una solución al planteamiento de la problemática explicada en el primer capítulo. Dicha propuesta se fundamentará en los resultados obtenidos de la aplicación de los instrumentos seleccionados, junto con sus debidos análisis y conclusiones.

Diseño de la Investigación.

Ahora bien, enmarcada en la metodología documental, busca identificar y analizar las principales propuestas y enfoques teóricos desde el Derecho y la Economía para abordar la problemática del uso de datos de usuarios en las redes sociales venezolanas.

Además de ello, el presente Trabajo Especial de grado se basa en una investigación cualitativa, definida como:

La investigación cualitativa es un paradigma emergente que sustenta su visión epistemológica y metodológica en las experiencias subjetivas e intersubjetivas de los sujetos, cuya práctica se orienta hacia la sociedad construida por el hombre, donde interactúan las versiones y opiniones del ser pensante, respecto a los hechos y fenómenos de estudio, para construir la realidad de manera cooperativa y dinámica. (Corona, 2018, p 75)

Todo ello quiere decir que, a través de un análisis de la literatura especializada, se pretende contribuir al debate sobre posibles soluciones normativas y regulatorias que garanticen la protección de los derechos de los usuarios y promuevan un uso responsable de los datos personales en este contexto. Por lo cual, para poder llegar a los resultados se pretende la revisión de los conceptos y análisis existentes en la materia mediante los métodos basados en la búsqueda y revisión de información en fuentes documentales previas con el objetivo de obtener un apoyo a las soluciones que serán planteadas a la problemática del presente Trabajo de Investigación.

Técnicas y Herramientas de Recolección y Procesamiento de Datos.

Para este trabajo de investigación, se ha seleccionado la técnica de entrevista estructurada, definida como:

Aquella que se basa en un guion de preguntas, fundamentalmente abiertas (en contraste con las preguntas que aparecen en un cuestionario, que son principalmente cerradas o de opción múltiple). A todos los entrevistados se les hacen las mismas preguntas con la misma formulación y en el mismo orden. De esta manera el estímulo es igual para todos los entrevistados y se garantiza que la variedad en la disposición de preguntas no altera las respuestas. Los entrevistados, sin embargo, tienen plena libertad para manifestar su respuesta. (Tejero, 2021, p. 67)

En pocas palabras, las entrevistas estructuradas serán el principal medio de recopilación de datos. Estas entrevistas se llevarán a cabo mediante un intercambio de información entre el entrevistador y los participantes. Con el fin de asegurar la efectividad del proceso, se ha diseñado un cuestionario previamente, el cual será aplicado con la colaboración de expertos en la materia. De esta manera, se espera obtener resultados óptimos que aporten información valiosa para el desarrollo del estudio.

También es importante destacar que se aplicará la observación documental sobre el caso “*Bundeskartellamt c. Meta Platforms Inc*”, en Alemania y la Unión Europea (“UE”), con el propósito de usar este caso como punto de partida para el análisis de principios para la gestión de datos personales en las redes sociales en Venezuela.

Resultados

Entrevistas estructuradas

Entrevista al Profesor Juan Esteban Korody Tagliaferro.

Realizada el 4 de abril de 2024

1. ¿Usted considera que en las redes sociales hay un consumidor o un usuario?

Definitivamente hay un consumidor, el concepto de consumidor y usuario en el mundo de la economía digital, en mi opinión, se está difuminando o fusionando uno en el otro, tu consumes contenido, consumes tiempo o información que recibes en las redes sociales y a cambio de eso das tu tiempo y das información sobre ti. Entonces,

definitivamente hay un intercambio económico muy claro, ellos te ofrecen conectividad, interconexión, información y tú das la información.

2. ¿Qué rige el paradigma de la tutela del consumidor?

En mi opinión, a pesar de que existen muchas teorías, el paradigma de la tutela del consumidor parte de un hecho de que el consumidor “a pie” o el ciudadano común no está en una posición de poder de una manera individual frente a un prestador de servicios o un vendedor de gran escala que tiene una posición si se quiere decir “privilegiada” en esa relación comercial, entonces ante esa diferencia que puede afectar las decisiones del mercado y generar una falla del mercado, le es necesario esa falla de mercado porque esa diferencia de posiciones de poder pudieran hacer que las decisiones que está tomando el agente económico en el mercado no las está tomando con entera libertad, no las está tomando totalmente informado ni con el fin de hacer una conducta que pueda variar definitivamente en el tipo de oferta o el precio, en consecuencia, al reconocer económicamente que hay una deficiencia o desigualdad desde el punto de vista del poder, se hace necesario para garantizar o equilibrar esa desigualdad que el agente económico individual pueda buscar en alguien más fuerte la protección de sus derechos o la protección de sus bienes.

La tutela de protección del consumidor se justifica en la medida en que se resuelvan las fallas del mercado y en la medida en que estos consumidores puedan tener acceso a bienes y servicios de mejor calidad al precio que el mercado defina que es el adecuado o el que se encuentra en el punto de equilibrio.

3. ¿Qué críticas se pueden hacer a la aplicación de la teoría neoclásica a la gestión de los datos de los usuarios de redes sociales?

Es necesario una evolución y una revisión de los paradigmas que se han tenido para revisar el contenido de las redes sociales, la economía digital va más allá de la venta de bienes o la prestación de servicios, la economía digital está incluso proyectada en “presencial digital” y la misma está cambiando la forma de vivir, la forma en que se relacionan los individuos y en consecuencia, la forma en la que toman decisiones los agentes económicos, así como la psicología entró a cuestionar al “*homo economicus*”, un hecho social relevante

como es el mundo digital, ha generado, en mi opinión, un cambio importante del paradigma de concepción de nuevos negocios o de nuevas formas de relacionamiento económico-social, psico-social del individuo y del agente económico, y por lo tanto, debe ser superada la teoría neoclásica para dar pasos a nuevos paradigmas o lo que me gusta a mí pensar, englobar estas nuevas formas de relacionamiento sociales o de economía en los conceptos clásicos y básicos.

4. ¿Cuándo considera usted que ocurre el abuso y uso de los datos en las redes?

Es muy difícil determinar un patrón infalible cuando se habla de abuso, creo que la concepción está, para mí, en primero lugar en el abuso del derecho, en segundo lugar, en la dignidad, en tercer lugar, en la decisión libre de los agentes económicos, esto quiere decir: ¿Qué fue lo que tú y yo pactamos? Y que, aún, a pesar de que “yo” pacté que puedas recolectar mis datos ¿qué haría un buen padre de familia con los datos que yo te estoy dando?

Si es verdad que puedes usar mis datos para detectar patrones de conducta, verificar gustos, necesidades o incluso desarrollo de nuevos productos de investigación, usar la información que yo tengo para tratar de variar mi conducta que yo normalmente y en libertad pueda tomar, creo que es un primer patrón de abuso de derecho, es decir, tratar de moldear mi conducta para algo que tú quieres y no lo que yo quiero.

En pocas palabras, yo pacté que tú podrías hacer eso, pero cuando ya tú estás cambiando mi forma de pensar, mi forma de conducir mis decisiones, privándome de la libertad de yo saber que tú lo estás haciendo en mi inconsciente, ahí puede haber un abuso de derecho, y hoy en día está pasando, cuando las redes sociales te hacen ofrecimiento de información, ofrecimiento de cuentas que seguir, basado en tu conducta y no en tu verdadera libertad para escoger una cosa o la otra, y tú también tienes la posibilidad de escoger relacionarte en esa red social de una manera más orgánica y menos con inteligencia artificial, o decir, “me encanta la inteligencia artificial, sigue vendiéndome lo que tú me quieras vender”, entonces si no hay consentimiento realmente informado de estas dos, creo que puede haber un abuso.

En segundo lugar, cuando yo no puedo acceder a la información que yo te he entregado con el fin de pedirte “suprime, modifica, cambia, etc.” en este sentido, si yo no puedo pedirte a ti que suprimes, varíes, mejores o modifiques la información que te he dado, allí puede haber un abuso de la información.

Por último, la más clara de todas, ya estás fuera del abuso de derecho, que es dentro de los derechos que yo te di y llevarlo a un extremo donde se vuelve excesivo, es decir, no estás violando el pacto en sí mismo, pero en el caso concreto, puede ser abusivo. Cuando estamos hablando del “Habeas Data”, es cuando yo no puedo pedir “suprime, modifica, etc.”, y el último caso es cuando, por ejemplo, yo no te autoricé para usar mis datos en experimentos con animales, poner mi foto para gorilas y chimpancés entrenados para ver cómo reaccionan ante mi imagen, tono de voz, ademanes y comportamiento, porque es algo que violaría mi identidad como humano y, además, es algo para lo que no pacté y no di mi consentimiento.

5. ¿Cómo se protege la tutela del consumidor en la gestión de los datos de los usuarios de redes sociales en Venezuela?

En Venezuela tenemos un vacío legal muy importante y una deuda legislativa que ha sido brevemente llenada por la Sala Constitucional en un recurso de interpretación sobre el Artículo 28 de la Carta Magna que habla del “Habeas Data”, hay una ausencia total de regulación y lo que no tengo muy claro es si esa deuda legislativa es necesaria ser llenada o no, es mi gran duda, porque para ello yo tengo que verificar datos económicos, que en este momento se está generando una falla del mercado que necesita ser corregida a través de la regulación, eso no lo tengo claro.

Creo que la Constitución como instrumento legal en algunas normas autoaplicativas, como puede ser el Artículo 28 o superado el paradigma de las normas programáticas de la Constitución y entendiendo que esta tiene normas de fuerza o exigibilidad, yo puedo pedir por ejemplo a alguien que esté usando mis datos y que yo quiero que se corrijan esos datos, se supriman, la Constitución tiene el vínculo perfecto para hacerlo si hay alguien que está usando mis datos sin mí autorización o usándolos para alguien que yo no lo autoricé, entonces hay una violación del contrato y si alguien, a pesar de que yo hice la autorización del uso,

abusan de él, yo tengo en la legislación civil el “abuso de derecho” que me permite ir contra estas empresas o estos prestadores de servicios.

Hay dos limitaciones ante esto, la primera, la legislación de protección al consumidor se justificó por las razones que ya hablamos, que era tratar de equilibrar la posición de desigualdad que existía entre un vendedor de bienes o un prestado de servicios y un singular agente económico, y requirió una tutela administrativa forzada que pudiera corregir rápidamente esa falla del mercado, y además, dar rapidez y acceso más eficiente porque el “abuso de derecho” está en el Código Civil, pero usted tendría que intentar una demanda civil o mercantil ante los tribunales ordinarios, entonces si usted no tiene dinero para iniciar ese juicio, es muy difícil que se corrija esa falla del mercado y que usted pueda verse satisfecho en sus pretensiones.

La tutela administrativa lo que hace es acortar tiempo y dinero para corregir la falla del mercado.

6. ¿Cómo se puede mejorar la racionalidad del individuo como consumidor en la gestión de los datos de los usuarios de redes sociales?

Considero que es imposible, hacerlo sin violar la propia humanidad del individuo, la racionalidad es un proceso innato del ser humano, nosotros no podemos evitar que un ser humano se comporte racional o irracionalmente, me parece que no le corresponde ni al Estado eso, y quizás la autorregulación la pueda dar la propia sociedad frente al individuo. En conclusión, la racionalidad del individuo no puede ser moldeada a través de la legislación.

Análisis de la Entrevista realizada al Profesor Juan Esteban Korody Tagliaferro.

Como se desprende de la entrevista realizada a Juan Esteban Korody Tagliaferro, profesor de la Especialización en Derecho de la Economía y especialista en la materia, existe una línea muy “transparente” entre la figura del consumidor y el usuario en las redes sociales, ya que los usuarios son los que consumen el contenido e información, pero en virtud de que le otorgan sus datos personales al prestador de servicio, ese intercambio es delimitado como un intercambio económico en la actualidad, esto en pocas palabras se traduce a que los datos

personales son más valiosos que consumir un “bien”, en virtud de que estos datos le pueden proporcionar más beneficios económicos al prestador de servicios.

Por su parte, el Paradigma de la Tutela del Consumidor se origina de la exigencia de rectificar las deficiencias del mercado, como la ausencia de información completa y perfecta. Esta disparidad en la información provoca una inequidad que facilita a los proveedores de servicios un uso inadecuado de la información personal de los usuarios. Este uso inadecuado puede manifestarse de diversas formas, como la denigración, la calumnia, la venta de datos a terceros sin consentimiento, el uso para fines publicitarios no deseados, entre otros.

Ahora bien, de las declaraciones del experto se puede entender que actualmente la legislación venezolana tiene un vacío, ya que no existe una legislación específica en materia de protección de datos personales de los consumidores, sino que la seguridad jurídica del consumidor solamente se encuentra en la Constitución de la República Bolivariana de Venezuela y en jurisprudencia específica emanada del Tribunal Supremo de Justicia, por ende, parece ser más viable que la sociedad misma a medida que avance en temas tecnológicos se puedan autorregular en los contratos o pactos que acuerden con los prestadores de servicios de las redes sociales.

Por último, se hace énfasis en que es imposible modificar, a través de una legislación específica, la racionalidad humana, ya que se encuentra íntimamente relacionado con el “ser” mismo, por ende, se resalta nuevamente la necesidad de utilizar la autorregulación para fomentar una reflexión extensa en los derechos que pueden ser ejercidos por el consumidor.

Entrevista al Profesor Daniel Betancourt Ramírez.

Realizada el 5 de junio de 2024

1. ¿En las redes sociales hay un consumidor o un usuario?

En efecto, en las redes sociales hay un consumidor, como un usuario, como un producto, la persona que accede a una red social pasa por las tres partes, es decir, es un usuario de un servicio prestado por un tercero dentro de un terminado software, y a su vez también es un consumidor porque está expuesto a un intercambio económico donde es la parte “pasiva”,

pero adicionalmente, también es un producto. Es decir, el acceso gratuito en teoría a las redes sociales no termina siendo así, por lo tanto, el consumidor, unas veces voluntaria, en otras no y en determinadas ocasiones tampoco de forma consciente termina aportándole datos a las redes sociales y a las plataformas, las cuales son procesadas y monetizadas por los desarrolladores de las redes.

2. ¿Qué rige el paradigma de la tutela del consumidor?

La tutela del consumidor es parte de un interés del Estado en que no exista violación de derechos fundamentales o exista la preservación de valores constitucionales o valores superiores del ordenamiento jurídico, los cuales se materializan con el interés público.

Al final, esta protección de derechos de bienes o valores que están en el ordenamiento jurídico y que tienen un tratamiento superior y diferenciado, normalmente se concretiza en razón de la regulación. Esto quiere decir, el establecimiento de límites a derechos subjetivos de partes contractuales a los fines de la preservación del derecho.

3. ¿Qué críticas se pueden hacer a la aplicación de la teoría neoclásica de la economía a la gestión de los datos de los usuarios de redes sociales?

La crítica fundamental es que la Teoría Neoclásica de la Economía busca una maximización de la utilidad en razón de los datos, sin embargo, los datos no son un objeto aislado, sino que están relacionados a personas tuteladas por el ordenamiento jurídico y en nuevo entendimiento del derecho a la confidencialidad y a la privacidad de las personas, estos datos tienen tutela jurídica.

En otras palabras, el tratamiento que se le dan a estos datos no solo tiene que tener ser consentido por el usuario, sino que además tiene que tener estándares mínimos dentro de la concepción del derecho actual, no son simplemente una mercancía económica susceptible de tráfico.

4. ¿Cuándo considera usted que ocurre el abuso y uso de los datos en las redes?

El abuso de los datos comienza desde que se abre la aplicación o se suscribe la persona en la aplicación. Normalmente se aportan o se piden datos que son totalmente irrelevantes para el funcionamiento de la aplicación, pero que se disfrazan como una manera de customizar o de establecer preferencias del usuario, sin embargo, esto evidentemente son bases estadísticas para poder monetizar los datos personales y que estén lo más completos para los fines de su comercialización, bien sea en cualquiera de los usos que se le da en cualquiera de sus proveedores de las redes sociales.

En otras palabras, es muy evidente que hay una recolección de datos personales con fines comerciales y que tiende a su abuso, y que supera la simple necesidad de esos datos para que la aplicación funcione.

5. ¿Cómo se protege la tutela del consumidor en la gestión de los datos de los usuarios de redes sociales en Venezuela?

La tutela solamente existe a partir del Derecho a la Privacidad que está establecido en la Constitución de la República Bolivariana de Venezuela que ha tenido un desarrollo incipiente a través de la jurisprudencia en materia de habeas data, el cual es el medio procesal para conocer la data personal que tiene un tercero en su base de datos y los cuales han establecido unas reglas que terminan siendo rudimentarias. Por ejemplo, el derecho a conocer los propios datos en la base de datos y el derecho al olvido o al derecho que sean borrados, existen específicamente en algunos ordenamientos como el bancario, algunas previsiones especiales como por ejemplo que la base de datos esté físicamente en Venezuela y ciertas obligaciones en ese ámbito que estén bajo la confidencialidad o el secreto bancario.

Fuera de eso, no existe en Venezuela ningún ordenamiento secundario, es decir, no existen leyes orgánicas ni de base que establezcan previsiones respecto a la protección de datos, y mucho menos de consumidores ni en materia de redes sociales.

6. ¿Cómo se puede mejorar la racionalidad del individuo como consumidor en la gestión de los datos de los usuarios de redes sociales?

La primera respuesta es evidente, y es que el individuo tenga la información completa de cuál es el tratamiento de sus datos, sin embargo, esta medida no es suficiente, ya que, en la mayoría de los casos los contratos que se suscriben o que se aceptan con las redes sociales son públicos y nadie los lee, pues vendría un panorama de evitar sesgos para que esto ocurra o también de exposición pública, es decir, una herramienta educativa de qué es lo que sucede con esos datos y quizás a partir de allí se empiecen a tomar decisiones consciente por parte de los usuarios, pero en ningún caso existe garantía por el medio digital, por la rapidez que involucra, un consumidor se tome el tiempo para evitar sesgos y aumentar su racionalidad en razón del aporte de datos constante que hace de manera consciente o no.

Análisis de la Entrevista realizada al Profesor Daniel Betancourt Ramírez.

Daniel Betancourt, profesor de la Especialización en Derecho de la Economía, y especialista en Derecho Financiero y Derecho Administrativo, delimita que en las redes sociales el individuo que accede a estas plataformas, no solamente es consumidor o usuario, sino que posee un tercer papel, y es el del producto, es decir, el individuo es usuario porque efectivamente utiliza el servicio ofrecido por las empresas de redes sociales, es consumidor porque ofrece un intercambio económico al ofrecer sus datos de forma gratuita, con la precisión que la empresa o plataforma de red social monetiza sus datos personales, y, en último lugar es un producto en virtud de que sus datos personales son procesados, analizados para diferentes fines y comercializados en algunos casos.

En cuanto al paradigma de la tutela del consumidor, el experto menciona que forma parte del interés del Estado en preservar esos derechos fundamentales y valores constitucionales. En síntesis, se materializa el paradigma a través de la regulación, debido a que la misma establece límites a los derechos de las partes que forman parte de ese “contrato” para precisamente proteger los derechos del consumidor o usuario, es decir, el fin último de una regulación específica en esta material de protección de datos debe aludir o tener como base evitar la violación de los derechos fundamentales y preservar el interés público

Por su parte, también con lo delimitado por el experto, se concluye que el abuso en el uso de los datos personales del usuario comienza desde el momento de su registro en la

plataforma, ya que la empresa que ofrece el servicio de red social solicita datos irrelevantes para el funcionamiento propio de la aplicación, lo cual expone que los datos personales efectivamente se recolectan para otros fines, excediendo así la necesidad real de la aplicación.

También se delimita que, en Venezuela la protección del consumidor en relación a su gestión de datos de usuarios en redes sociales es sumamente precaria, debido a que solamente se regula o limita a través del derecho a la privacidad contemplado en la Constitución de la República Bolivariana de Venezuela. Sin embargo, esa protección es sumamente blanda, a pesar de que existe un desarrollo jurisprudencial incipiente a través del recurso de *habeas data*, el cual permite conocer los datos personales que terceros puedan tener en sus bases de datos. En suma, en Venezuela no existe una regulación específica como leyes orgánicas o de base que puedan regular previsiones específicas sobre protección de datos y derechos del consumidor en materia de las plataformas de redes sociales.

Finalmente, no existe una fórmula precisa en la que el consumidor o usuario pueda mejorar su racionalidad, ya que para poder hacerlo, el consumidor debería tener información completa sobre el uso o tratamiento que se le dará a sus datos personales. Sin embargo, esta medida no es suficiente, ya que en la práctica, no en todos los casos, el individuo se toma el tiempo necesario para leer y analizar el contrato de "Términos y Condiciones" del uso de la plataforma.

No obstante, se puede “educar” o “capacitar” al individuo en materia de protección de datos y la legislación específica que lo protege, con el fin de evitar los sesgos que lleven a los usuarios a compartir sus datos personales por circunstancias como el factor de tiempo o la rapidez. Asimismo, también es importante aclarar que no hay una garantía de que estas medidas funcionen en virtud que las decisiones racionales provienen de las distintas experiencias y conocimientos que pueda tener el usuario. Por ende, mejorar la racionalidad del usuario o consumidor enfrenta un reto sumamente importante derivado a los sesgos propios de cada individuo y a la dinámica de rapidez del uso de las redes sociales.

CAPÍTULO IV

LA TUTELA DEL CONSUMIDOR

En este capítulo se expone el tema del consumidor en las redes sociales y su participación dentro del comercio electrónico, ya que el consumo es una fuerza que impulsa la economía de mercado y la teoría económica, entre otros temas, se enfoca en el estudio del comportamiento del consumidor.

Además, se analiza la figura del consumidor en la era de la *Big Data*, como un usuario activo dentro de las diversas plataformas de redes sociales. Asimismo, se delimita el concepto de la tutela del consumidor y el paradigma de la tutela del consumidor, destacando su importancia para garantizar la protección de los derechos de los consumidores en el entorno digital.

I. Definición y relevancia de la tutela del consumidor

Con la finalidad de comprender de forma correcta la figura del “usuario” y del “consumidor” en las redes sociales, primero se debe revisar los distintos conceptos que existen sobre estos, en este sentido se encuentran las siguientes definiciones:

El Presidente John Fitzgerald Kennedy el 15 de marzo de 1962 ante el Congreso de los Estados Unidos proclamó uno de las definiciones más famosas sobre la figura del consumidor, él comentó que los consumidores, por definición, incluye a todos. Son el grupo mayoritario de la economía, afectando y siendo afectados por la práctica totalidad de las decisiones económicas públicas y privadas. Dos tercios del gasto total en la economía provienen de los consumidores. Pero son el único grupo importante en la economía que no están organizados eficazmente, cuya opinión es a menudo ignorada. (Vergara, 2022)

Sin embargo, algunos autores como Ghunter Flass (2019) exponen que, la figura del consumidor es bastante problemática, ya que “(...) el consumidor, no es una categoría ontológica como la de trabajador, ciudadano, menor de edad etc., sino una condición circunstancial que de momentos asume la persona”.

No obstante, existen autores como Platero Alejandro y Jiménez Cristina (2017) que hacen una diferencia entre el Consumidor físico y el Consumidor *online*, estos señalan que no

siempre ha sido fácil concretar un concepto de consumidor, ya que no existe unanimidad doctrinal ni legal a la hora de concretar dicho concepto. Siendo más precisos, si se acude al ámbito comunitario, tanto la jurisprudencia como las normas, con carácter general, solo reconocen como consumidores a las personas físicas que adquieren bienes o servicios sin un fin que pueda considerarse comprendido en sus actividades comerciales o profesionales, sino como consumidores finales privados (STJUE, 2015, asunto C-297/14. FJ 25). Pero, la mera circunstancia de que se encuentra ante una persona física, no quiere decir automáticamente que sea un consumidor, es decir, “ser persona física no basta para determinar su condición de consumidor (STJUE, 2013, asunto C-19/11. FJ 38), por lo que es necesario que realice un acto de consumo.

Ahora bien, la Real Academia Española (2024) define al consumidor como la persona que adquiere productos de consumo o utiliza ciertos servicios, pero, por otra parte, el mismo diccionario expone que el usuario es el que “*usa algo*”. Estas dos distinciones se podrían resumir delimitando que, el consumidor es aquel que compra el producto o servicio, y el usuario es el que disfruta habitualmente de ese servicio o producto.

La teoría económica tradicionalmente ha contemplado al consumidor como un agente racional que maximizar su satisfacción (utilidad) dadas sus restricciones presupuestarias. Este modelo, es conocido como el *homo economicus*, asume que los individuos toman decisiones de consumo basadas en cálculos de costo-beneficio, actuando de manera individualista y maximizando su bienestar personal. No obstante, esta visión es controversial por ser un poco “simplista” y por no considerar factores sociales, psicológicos y contextuales que influyen en las decisiones de compra. (Artiles, 2022)

En las últimas décadas, diversos campos de estudio como la economía conductual y la psicología económica han tomado participación en la comprensión del comportamiento del consumidor. Estos enfoques reconocen que los individuos no siempre actúan de manera lineal y racional, sino que sus decisiones pueden ser influenciadas por factores emocionales, normas sociales, hábitos y la información que tengan disponible en este momento. También, el contexto social y cultural en el que se encuentra el consumidor juega un papel medular dentro de sus preferencias y comportamientos.

- **Protección jurídica de los usuarios y consumidores**

Previamente se hizo la distinción entre el usuario y el consumidor, se llegó a delimitar que no todos los usuarios son consumidores y viceversa, en pocas palabras, que los consumidores digitales son individuos con atributos y expectativas particulares que están constantemente conectados a Internet, accediendo a una amplia gama de información sobre productos y servicios en cualquier momento del día o la noche, a través de una variedad de dispositivos tecnológicos (Plaza, 2022, como se citó en Vargas Basilio, Yaulilahua Llancari, & Quincho Zevallos, 2024)

Todo ello conlleva a que el consumidor esté expuesto a ciertas situaciones de desventaja e inclusive injusticias de las que puede no tener conciencia y puede ser “víctima” de prácticas comerciales agresivas que tienen distintos propósitos tales como la influencia en la elección del consumidor respecto a sus preferencias o comportamiento, por ende, varios países de Latinoamérica, Estados Unidos y los que conforman la Unión Europea, han buscado a través de los años, crear formas de proteger a los consumidores por medio de leyes, políticas y acciones que estén enfocadas en resguardar los derechos e intereses de los consumidores en el mercado y en su relación comercial que poseen con las empresas que ofrecen servicios de redes sociales.

No obstante, a pesar de que según esta premisa el consumidor es un individuo que busca maximizar u obtener el mayor provecho o ventaja de algo, puede suceder que esté expuesto a prácticas comerciales abusivas en el mercado, definidas como todo acto, omisión, conducta o manifestación o comunicación comercial incluidas la publicidad y la comercialización procedente de un comerciante y directamente relacionado con la promoción, la venta o el suministro de un producto a los consumidores” (Artículo 2, literal D, de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo de 11 de mayo de 2005 relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, como se citó en López D, 2023)

Así pues, los consumidores representan la parte más vulnerable de la relación comercial, en virtud de que se enfrentan a las conductas previamente descritas, en las que

destacan las asimetrías de la información, cláusulas abusivas y prácticas engañosas por parte del proveedor del servicio, y es así como surge la acción de tutelar o proteger al consumidor. Esta protección, tutela o derecho es definida por primera vez a través de cuatro derechos fundamentales recogidos en la Carta Europea de Protección de los Consumidores en el año 1973 del Consejo de Europa según Resolución 543/73, en la que se puede esclarecer que, la tutela del consumidor busca establecer un equilibrio en las relaciones de poder que existe entre la empresa o proveedor del servicio y el consumidor, a través de regulaciones, protección de derechos y el empoderamiento del consumidor.

Por su parte, la tutela de protección al consumidor también puede delimitarse desde la perspectiva de la “Teoría de los derechos humanos del consumidor” y este se refiere a un sistema legal que incluye normas, principios e instituciones enfocados en la justicia y equidad en el mercado, sin importar si la ley es buena o mala. Este enfoque sistémico busca la validez y eficacia de las normas y se adhiere a la teoría del derecho del consumidor como un derecho social, cumpliendo así con el razonamiento garantista y el discurso dogmático en la disciplina del derecho del consumidor. (Durand, 2019, como se citó en Laurente, 2022)

- **Importancia en la protección de los derechos de los consumidores**

Es así entonces como se puede observar que, el consumidor tiene derecho a que exista equidad e igualdad en sus interacciones comerciales, por lo cual, es necesario un marco legal que tenga como objetivo equilibrar las relaciones entre los consumidores, usuarios y las empresas, evitando posibles abusos por parte de los proveedores debido a su posición dominante. Sin embargo, es importante destacar que, en lugar de asumir que siempre el proveedor tiene una posición dominante, se reconoce que esto puede variar según el mercado específico. En el caso de las redes sociales, por ejemplo, se identifica una posición dominante de los proveedores en ese segmento particular.

Además de ello, la existencia de un marco regulatorio impulsa la transparencia y la puesta a disposición de información a los consumidores, ya que las sanciones y políticas rigurosas obligan a los proveedores a suministrar datos precisos y ciertos sobre sus productos o

servicios, permitiéndole a los consumidores tomar decisiones con fundamento y elegir basándose en toda la información disponible. Por otro lado, esa “sensación” que puede tener un consumidor o usuario al tener la seguridad jurídica necesaria al momento de adquirir un servicio o producto, incentiva a los competidores a entrar en el mercado con estrategias de competencia más justas y asegurando la excelencia del producto que ofrecen, la cual se entiende como un atributo propio de cada oferente.

También, las legislaciones de protección al consumidor proveen medios para reclamar y hacer valer los derechos, otorgándole a los consumidores vías y procedimientos para ejercer sus derechos ante incumplimientos o fallas abusivas por parte de los proveedores. En consecuencia, una parte importante de la protección de los derechos de los consumidores es que exista la eficacia en conjunto de las legislaciones, políticas internas de los proveedores, entes encargados para aplicar las leyes y los consumidores para que se puedan identificar las necesidades más fundamentales de estos últimos.

En resumen, este marco regulatorio promueve la "eficiencia normativa", es decir, un sistema donde las reglas son claras, se aplican de manera efectiva y contribuyen a un mercado más justo y transparente.

Asimismo, *Consumers International (CI)* describe once “necesidades legítimas” de los consumidores, en el cual toman como contexto la creciente complejidad de los mercados y de asimetrías de poder entre empresas y consumidores, dicho enfoque representado por el CI se muestra como una “guía” para poder entender al consumidor, motivar la economía justa y transparente. Dichas necesidades son las siguientes:

1. Acceso: la capacidad de tener acceso a los bienes y servicios esenciales.
2. Inclusión: la protección de los consumidores vulnerables y desfavorecidos.
3. Seguridad: la protección frente a los riesgos para la salud y la seguridad.
4. Protección de los intereses económicos: fomento del valor de inversión y protección frente al riesgo.
5. Información: acceso a información clara y exacta, que permita tomar decisiones informadas.

6. Educación: asistencia para que los consumidores comprendan sus transacciones y las consecuencias medioambientales, sociales y económicas de sus decisiones específicas.
7. Compensación: capacidad de contar con servicios eficaces de resolución de disputas y mecanismos de compensación.
8. Representación: la libertad para que los consumidores se organicen en grupos y que sus opiniones se incluyan en los procesos relevantes de toma de decisiones.
9. Sustentabilidad: la promoción de modelos de consumo sustentable.
10. Derechos relativos al comercio electrónico: se debe proporcionar la misma protección a los consumidores que tratan con organizaciones tanto en línea como fuera de línea.
11. Privacidad: la protección de la privacidad de los consumidores y la circulación libre y global de la información

En conclusión, estas necesidades son una demostración de que las leyes de protección del consumidor desempeñan un papel fundamental en salvaguardar los derechos y el bienestar de los ciudadanos. Estas regulaciones garantizan que los bienes y servicios adquiridos cumplan con los estándares de calidad establecidos, evitando así que los consumidores se vean perjudicados por productos defectuosos o prácticas comerciales desleales. Además, estas leyes alertan a los consumidores sobre posibles fraudes y estafas, ofreciendo mecanismos de compensación en caso de ser víctimas de engaños. En resumen, la existencia y aplicación efectiva de las leyes de protección del consumidor son esenciales para mantener un mercado justo y transparente, donde los derechos y la confianza de los ciudadanos se encuentren debidamente salvaguardados.

II. El Paradigma del Consumidor

- **Teoría Neoclásica del Consumidor**

La economía es la ciencia de la elección y su teoría en relación a la elección de los consumidores se fundamenta en examinar las disyuntivas que enfrentan las personas en sus roles de consumidores.

Cuando un consumidor compra una mayor cantidad de un bien, su capacidad para adquirir otros bienes disminuye. Cuando pasa más tiempo descansando y menos tiempo trabajando, su ingreso es menor y, por consiguiente, su capacidad de consumo también es menor. Cuando gasta más de su ingreso en el consumo presente y ahorra menos, debe aceptar un nivel de consumo más bajo en el futuro. La teoría de la elección del consumidor examina la forma en la cual los consumidores que enfrentan estas disyuntivas toman decisiones y la forma en la cual responden a los cambios en su entorno. (Mankiw, 2012, pp 439-440)

Ahora bien, otro de los ámbitos que aborda la economía es la teoría del consumidor, esta se enfoca en estudiar el comportamiento de un agente económico en su carácter de consumidor de bienes y servicios encaminado a la obtención de la curva de demanda del consumidor, explica la forma en que se comporta el consumidor, y, la mencionada teoría “(...) es observada bajo la microeconomía y actualmente el análisis del consumidor es de vital importancia pues a través de él se puede observar como una persona alcanza su máximo bienestar dado su presupuesto” (Coronado, 2019, p. 7)

En este contexto, el consumidor es conceptualizado como un *Homo Economicus* (Hombre Económico). Este modelo económico representa al individuo como un ser racional que toma decisiones basadas en un análisis lógico y objetivo, siempre buscando maximizar su utilidad. Este enfoque asume que el consumidor es egoísta y prioriza su propio bienestar sobre el de los demás. De eso se desprende que, el individuo cuenta con toda la información relevante sobre los productos o servicios, lo que le permite tomar decisiones consistentes y predecibles, sin considerar factores externos o incertidumbre. (Mosqueda, 2022, p.)

Si bien el modelo del *homo economicus* asume que los consumidores actúan racionalmente en su propio beneficio, la realidad es que las redes sociales exponen a los individuos a la interacción social y la influencia de otros, lo que puede afectar sus decisiones de compra. No obstante, es importante aclarar que esta interacción no es exclusiva de las redes sociales, ya que los individuos también se influyen mutuamente en entornos físicos.

En este sentido, la desinformación en redes sociales no se refiere a una falta de información general, sino más bien a un desconocimiento específico sobre el uso que se da a

los datos personales que los usuarios proporcionan al registrarse e interactuar en estas plataformas. En consecuencia, en las plataformas de redes sociales el usuario se vuelve más pasivo porque puede estar desinformado en cuanto al uso de la data que provee al momento de registrarse e interactuar dentro de la plataforma o red social, y la desinformación en los términos de la *Big Data* representa varias aristas, acorde la Comisión Europea, la desinformación es definida como:

Información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público, dicha delimitación también comprende la figura de las “*fake news*” ya que son hechas para intencionalmente engañar a un usuario o consumidor, por su parte, otra categoría de desinformación es la “*misinformation*” la cual hace referencia a un tipo de información involuntariamente engañosa. (Hernon, 1995, citado por Sánchez, 2022)

Como consecuencia de la desinformación cuando el entorno online se encuentra personalizado y micro-segmentado, los ciudadanos están expuestos a informaciones que refuerzan los sesgos ideológicos y es más difícil encontrar opiniones diferentes, lo que lleva a una mayor polarización política e ideológica. (Melo, 2022, p. 30)

Una de las fallas de mercado que influyen en las decisiones de los consumidores es la asimetría de información. Esta se refiere a la situación en la que una de las partes en una transacción posee más información relevante que la otra, lo que puede llevar a decisiones que no maximizan el beneficio del consumidor. (Nunes, 2019, citado por Laurente, 2022; Mosqueda, 2022)

En el ámbito del consumo digital, esta asimetría se manifiesta en la falta de transparencia sobre el uso de los datos personales y la complejidad de los términos y condiciones. Los consumidores, al priorizar la inmediatez y la comodidad, a menudo aceptan estos términos sin una comprensión completa de sus implicaciones. Esta situación, en contraste con el modelo del *Homo Economicus* que asume una racionalidad perfecta y

omnisciencia, crea un escenario en el que los derechos de los consumidores pueden ser vulnerados.

Es fundamental fortalecer los marcos regulatorios y promover la transparencia en las prácticas de las empresas para proteger a los consumidores en este entorno digital complejo. Se sugiere que para la versión final de este trabajo se utilicen argumentos encontrados en las referencias bibliográficas para respaldar la afirmación sobre la asimetría de información en el consumo digital.

En resumen, en la era actual de la *Big Data*, el usuario quiere y siente la necesidad de que todo lo que quiere, se suscribe, solicita, compra, vende, se debe entregar u obtener de forma inmediata. Es así como, la protección del consumidor en la era de la *Big Data* exige una adaptación constante de las leyes y regulaciones para hacer frente a los desafíos planteados por la asimetría informativa y la complejidad de las tecnologías emergentes, con la finalidad de lograr garantizar que los usuarios como consumidores tomen decisiones informadas y protegidas respecto a sus datos personales.

I. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de fecha 04 de julio de 2023. *Meta Platforms Inc* (anteriormente *Facebook Inc* vs, *Bundeskartellamt*)

Meta Platforms Inc, fue creada en el año 2003 por Mark Zuckerberg, estudiante de Ciencias de Computación en Harvard, sin embargo, tenía otro nombre y propósito, se denominaba “*FaceMash*”, esta era una red social ilegal y básicamente se trataba de un sitio que permitía calificar a las mujeres de acuerdo a su atractivo físico. Básicamente los usuarios podían acceder a esta red social y calificar si una persona era atractiva o no lo era. ¿El riesgo? Las fotografías que ahí aparecían se habían obtenido de manera ilegal desde los anuarios de las universidades en Estados Unidos. (GQ, 2024)

Esta red social ilegal tan infantil y ofensiva fue un éxito después de su creación, de hecho, en tan solo cuatro horas en línea recibió 450 visitantes y generó 22,000 vistas de fotos. De

haber permanecido más tiempo en Internet, seguramente hubiese impuesto algunos récords en la Universidad de Harvard. Sin embargo, posterior a su éxito, las autoridades de la universidad lograron encontrar al responsable y fue acusado de violar la privacidad de los estudiantes en la institución y descargar datos que eran propiedad de la Universidad de Harvard. Su estancia en la universidad fue condicionada. Sin embargo, todo ello importó muy poco a Zuckerberg. Había conseguido abandonar el anonimato asociado a la condición de simple estudiante de psicología, para empezar a ser reconocido en Harvard como un respetado programador. Islas et al. (2021)

Seguidamente, en el año 2004 llegó *Facebook* como una red virtual famosa entre los estudiantes de las mejores universidades de Estados Unidos, su éxito era tan rápido que Zuckerberg se dedicaba tiempo completo para desarrollar dicha red social, sin embargo, continuó con sus estudios y se graduó de Harvard, y ya para el año 2006 con 22 años tenía una oferta multimillonaria de Yahoo! Y de otras redes sociales, no obstante, no las aceptó.

Luego de ese período de ofertas, ya ese mismo año Facebook permitió el acceso a todos los usuarios de internet en el mundo, ya no solamente era para el uso exclusivo de universitarios.

Ahora bien, este fue el comienzo de los patrones de uso y abuso de los datos personales de los usuarios en Meta, y por ende, la *Federal Cartel Office (Bundeskartellamt)* de Alemania en el año 2016 comenzó a investigar las actitudes que tenía la empresa en el mercado, leyendo y analizando con detenimiento los “Términos y Condiciones” de los servicios de red social que ofrecía Meta, y uno de los puntos que más llamó la atención era el tratamiento de datos personales de los usuarios, ya que según las autoridades, dichos “Términos y Condiciones” contenían cláusulas abusivas y el usuario no tenía opinión en ello, ya que si no aceptaban dichos términos, entonces no podía disfrutar o suscribirse a la red social.

Esta afirmación vino precedida de una consulta a la autoridad de protección de datos alemana, con la que colaboró en este asunto, y que entendió que la autoridad de competencia está legitimada para aplicar los principios instituidos por el RGPD en el marco de la evaluación de la conducta de la empresa dominante. (Colangelo, 2019, citado en Díez, 2023).

Asimismo, las autoridades consideraron que el consentimiento que otorgaban los usuarios de Meta dentro de los “Términos y Condiciones” se encontraba poco claro y era abusivo, en virtud, de que en realidad los usuarios no tenían toda la información sobre el proceso de almacenamiento, archivo o tratamiento de sus datos personales, además, también recopilaban información excesiva y no necesaria para la finalidad o los objetivos de la red social.

Por ende, las autoridades alemanas concluyeron que Meta actuaba contrario a los valores estipulados en Reglamento General de Protección de Datos (UE) 2016/679, y con dichas pruebas y argumentos *Bundeskartellamt* en el 2019 concluyó que efectivamente los “Términos y Condiciones” impuestos a los usuarios de Meta eran cláusulas contractuales abusivas, y, que en esa conducta también se manifestaba el poder de mercado que tenía el servicio de red social, lo cual conllevó a las acusaciones de posición de dominio en el mercado de las redes sociales. Ahora bien, a medida que el caso avanzaba, el Tribunal de Düsseldorf cuestionaba que *Bundeskartellamt* estaba analizando y exclusivamente un problema de protección de los datos personales y uno de falta de competencia en los mercados (*Oberlandesgericht Düsseldorf*, 2019, citado en Díez, 2023). Sin embargo, en el año 2020 el Tribunal Regional Superior de Düsseldorf suspende la orden de *Bundeskartellamt* sobre el tratamiento de los datos personales los usuarios, y, permite que Meta Platforms Inc (anteriormente Facebook Inc) proceda con su proceso regular de tratamiento de los datos de los usuarios de la red social.

No obstante, *Bundeskartellamt* no estuvo de acuerdo con dicha decisión y apela a la decisión del Tribunal mencionado anteriormente, esta decisión terminó por elevarse ante el Tribunal de Justicia de la Unión Europea en fecha 22 de abril de 2021, y en fecha 04 de julio de 2023 el Tribunal, previamente identificado, expresó que la conformidad o no conformidad de las actividades de una empresa dominante con las disposiciones del Reglamento General de Protección de Datos puede constituir un indicio relevante para determinar si dichas actividades constituyen medios que rigen una competencia normal y para evaluar las consecuencias de una determinada práctica en el mercado o para los consumidores.

De ello resulta que en el marco de un procedimiento por abuso de posición dominante puede ser necesario que la Autoridad nacional de competencia examine también la

conformidad de las actividades de dicha empresa con las normas en materia de protección de datos personales establecidas en el Reglamento General de Protección de Datos. (Santacruz, 2024)

Es importante destacar que, para el objetivo de este Trabajo Especial de Grado, se ha decidido enfocarse en el tratamiento de los datos dentro del caso expuesto previamente y no en la posición de dominio del que se acusaba a Meta.

Así pues, el cuestionamiento de *Bundeskartellamt* al Tribunal de Justicia de la Unión Europea se enfocaban en el alcance sobre la prohibición del tratamiento de categorías especiales de datos personales o tratamiento de datos sensibles estipulados en los siguientes Artículos del Reglamento General de Protección de Datos (UE):

- Artículo 9, apartado 1. Tratamiento de categorías especiales de datos personales: Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

De seguidas, el como excepción a la aplicación del apartado 1 del Artículo 9 se encuentra en el apartado 2 del mismo Artículo, el que es delimitación a la justificación para el tratamiento de datos personales consistente en la “necesidad para la ejecución de un contrato”:

- Artículo 9, apartado 2. Tratamiento de Categorías especiales de datos personales:

A) El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

- B) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
- C) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
- D) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
- E) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
- F) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
- G) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
- H) h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

- I) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
- J) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.
4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Por su parte, el Artículo 6, en su apartado 1, letra B y F el mencionado Reglamento establece la necesidad para la satisfacción de “intereses legítimos”:

- Artículo 6, apartado 1. Licitud de tratamiento:

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;

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.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Otro Artículo medular en este caso fue el Artículo 4, apartado 11 del mencionado Reglamento, ya que define el “Consentimiento del Interesado”:

- Artículo 4, apartado 11. Definiciones: “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 informativa, el tratamiento de datos personales que le conciernen.

Es así como el Tribunal de Justicia de la Unión Europea respalda la decisión del Tribunal Federal de Justicia de Alemania confirmando que *Bundeskartellamt* sí tenía las facultades necesarias para intervenir en casos de abuso dominante y protección de datos. En resumen, el caso se resolvió a favor de *Bundeskartellamt* de prohibir a Facebook la combinación de datos de usuarios sin su consentimiento explícito. Esto se consideró un abuso de la posición dominante de *Facebook* en el mercado. Actualmente, esta decisión sigue vigente, obligando a *Meta (Facebook)* a respetar la normativa de protección de datos y competencia en Alemania.

En resumen, el resultado del caso anterior sentó un precedente relacionado con la regulación de las principales plataformas digitales como *Facebook*, *Google*, etc. Las autoridades competentes ahora tienen una base legal o jurídica más sólida para hacer frente a los abusos de supremacía en relación con el procesamiento de datos personales. Por el contrario, este caso fortalece los derechos de los consumidores en el entorno digital al limitar la influencia de las grandes plataformas y exigir un control más justo y claro sobre los datos

personales. Finalmente, la sentencia destaca claramente la complejidad de la relación entre competencia y protección de datos y la necesidad de una coordinación efectiva entre las diferentes autoridades reguladoras.

CAPÍTULO V

LOS PRINCIPIOS RECTORES PARA LA PROTECCIÓN DE DATOS DEL USUARIO EN EL ÁMBITO DE LAS REDES SOCIALES EN EL ORDENAMIENTO JURÍDICO VENEZOLANO

En el presente capítulo, se exponen algunos principios para un manejo íntegro y transparente de los datos personales de los usuarios de redes sociales en Venezuela. En vista de que en el país actualmente no existe dentro del ámbito legislativo una regulación clara y efectiva respecto al tratamiento de los datos de los usuarios de redes sociales ni los distintos derechos que pueden ejercer frente a las autoridades competentes

El propósito es presentar una propuesta para solventar la problemática concerniente a la falta de regulación sobre protección de datos y específicamente, el uso y trato de los datos personales de los usuarios de redes sociales, con la finalidad de que se permita dar los primeros “lineamientos” o “bosquejos” para lograr la debida protección jurídica del usuario y consumidor.

Lo cierto es que en Venezuela en materia de protección de datos ha sido un terreno poco explorado o que no ha evolucionado con la tecnología y la globalización, ya que a pesar de que existen concepciones sobre ello y se encuentran establecidos en los Artículos 60 y 28 de la Constitución de la República Bolivariana de Venezuela de 1999, el primero alude al derecho que tienen los individuos de protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación, y, en el segundo se señala el derecho al acceso que tienen los individuos a la información que sobre sí mismos o sobre sus bienes consten en registros públicos o privados, pues la realidad es que no existe un marco legal que regule precisamente la protección de los datos personales en las redes sociales en el país.

A lo largo de la presente investigación se delimitaron varias definiciones, normativas y políticas internacionales, jurisprudencia internacional y aspectos sobre la protección de datos, los usuarios, los consumidores, la tutela de la protección del consumidor. Para interpretar la relación jurídica y económica existente entre el usuario, consumidor y proveedor del servicio, se revisó también lo que desde la teoría económica se refiere a la elección del consumidor, como parte de las herramientas provistas a través del análisis económico del derecho.

Se entiende que el consumidor es considerado como un agente teóricamente débil y, en algunos casos, pasivo dentro de esta relación, y que el producto o resultado económico se centra en el mismo consumidor y usuario al entregar sus datos personales. Sin embargo, este reconocimiento no es la única solución, ya que aún existen muchos aspectos por abordar y vacíos por llenar.

Para considerar que los datos personales de los usuarios de redes sociales estén realmente tutelados o protegidos no basta con el reconocimiento de la legislación vigente, pues como se ha analizado y estudiado anteriormente, se necesita cumplir varias consideraciones sobre el consumidor y el bien tutelado, por ende, falta una regulación clara y precisa que permita acoger principios específicos que sean lo suficientemente actualizados y en vanguardia para que sirvan de guía para llevar el procedimiento de la protección de los datos de los usuarios de redes sociales en Venezuela. Es por ello que, a continuación, se presenta una serie de principios rectores orientados a lograr una solución a ese vacío legal ya identificado anteriormente.

1. Principio Del Consentimiento Informado

En primer lugar, se debe incluir dentro de una futura legislación un apartado específico que recoja la garantía de los usuarios cuando otorguen su consentimiento expreso y específico para el uso de sus datos personales, el proceso de almacenamiento y el entendimiento total por parte del usuario del cómo ese proveedor de servicio utilizará sus datos personales. Pues esto no se encuentra expresamente descrito en la Carta Magna.

Por lo cual, la normativa debe proporcionar información clara, concisa y de fácil comprensión sobre el procedimiento del tratamiento de los datos personales de los cuales se puede destacar:

Que la mera obtención de datos de carácter personal también es considerada tratamiento de los mismos, cuando, obviamente, la recogida de datos personales es previa a la creación del fichero y a las posteriores operaciones de tratamiento en sentido estricto; del mismo modo se incluye en el concepto de tratamiento la cancelación que, como su propio nombre indica, supone la desaparición y destrucción de los datos tratados (Palomino , 2009, p. 7)

Como guía para redactar dicho Principio, se podría tomar como ejemplo lo estipulado por la Comisión Económica para América Latina y el Caribe (CEPAL) en sus Principios Básicos de la Protección de Datos, el cual indica lo siguiente:

Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

Asimismo, en abril del año 2021, el Comité Jurídico Interamericano de la Organización de los Estados Americanos (OEA) aprobó “Los Principios Actualizados sobre privacidad y la protección de datos personales con anotaciones” (Resolución CJI/Res. 266, contenidos en el informe correspondiente, en el cual se delimita el “Principio de Transparencia” de la siguiente manera:

Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para los cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el procesamiento se base en

el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, libre, inequívoco e informado de la persona a que se refieran. (OEA, 2021, p. 13)

Como puede apreciarse previamente en la redacción de los citados principios es que son específicos, pues dichas organizaciones delimitan la naturaleza del estudio de los datos personales y sus categorías, con el fin de darle la interpretación más precisa y el tratamiento adecuado. Lo cierto es que sería recomendable entender que los proveedores de servicios de las redes sociales deben desarrollar y comunicar de forma clara y accesible las Políticas de Privacidad donde expongan los procesos de almacenamiento, utilización y protección de la información de los usuarios, además de ello, una recomendación bastante simple sería implementar dentro de ese Principio, la obligación por parte de los proveedores de servicios de informar a los usuarios sobre cualquier modificación o actualización de sus Políticas de Privacidad, y darles la oportunidad a los usuarios de revisar, rechazar o aceptar dichos cambios atendiendo a la tutela efectiva de protección del consumidor. En pocas palabras, la OEA sostiene que:

El consentimiento debería reflejar la preferencia y la decisión fundamentada de la persona afectada. Evidentemente, el consentimiento obtenido bajo coacción o sobre la base de declaraciones falsas o incluso información incompleta o engañosa no puede cumplir las condiciones para la recopilación o el Tratamiento legítimos. (2022, p. 33).

2. Principio del Empoderamiento del Consumidor y Usuario.

Por otro lado, al comprender que efectivamente el consumidor y el usuario son el verdadero producto, es importante protegerlos de cualquier manipulación de su conducta o que la información utilizada por los proveedores de servicio no se haga sin la previa autorización y consentimiento expreso, para otros fines que no estén contemplados dentro del contrato que hizo el usuario o consumidor al suscribirse a la red social.

Es por ello que, el Principio que se plantea recoger de forma explícita el consentimiento antes de almacenar, usar y compartir los datos personales. Además, los servicios de redes sociales no pueden bajo ningún concepto recopilar información de los usuario o

consumidores de forma excesiva, es decir, se deben solicitar únicamente el consentimiento específico para cada tipo de dato personal y su uso.

3. Principio de Recopilación Necesaria.

Es fundamental tomar en cuenta que, el usuario y el consumidor dentro de su racionalidad pueden tener poca capacidad de decisión, por factores externos a él o por desconocimiento, es por ello que, se deben proteger estas dos figuras ante cualquier daño a la autonomía de sus datos personales, esto conlleva a que las empresas o proveedores de servicios deberían estar obligados a recopilar la mínima cantidad de datos personales para cumplir con fines ya previstos dentro del pacto o contrato, garantizando que ese almacenamiento o recopilación sea proporcional al servicio de red social que le ofrecen y sea limitada para el funcionamiento adecuado de la aplicación o portal web.

La finalidad del mencionado Principio también tendría que fomentarse en garantizar que los servicios de redes sociales no se excedan en el registro de datos de los usuarios, es decir, que incurran en la solicitud de datos excesivos o innecesaria sobre la información personal o sensible del usuario, un ejemplo de ello sucedió con la red social llamada TikTok, dicha aplicación sí se conecta a China y solicita un acceso casi completo al contenido del teléfono mientras la aplicación está en uso. Esos datos incluyen el calendario, las listas de contactos y las fotos. (Barbaschow, , 2022, p.)

Otro ejemplo es el simple seguimiento excesivo por parte de los servicios de redes sociales en cuanto a las interacciones entre el usuario y el servicio, recopilándolas de forma detallada, tales como los comentarios y las cuentas de otros usuarios que siguen, además de ello, y quizás el caso más notorio es el uso de los datos personales de los usuarios para fines publicitarios sin su consentimiento expreso, incluso también solicitan información de contenido sensible sin ningún tipo de justificación, tales como la orientación sexual o creencias políticas.

Los ejemplos descritos en el anterior párrafo denotan las formas o prácticas de recopilación excesiva de datos personales, que traspasan de lo estrictamente necesario, por lo cual, se recomienda establecer que, una vez el servicio de red social haya cumplido con su

propósito, la empresa debe eliminar de manera segura y permanente los datos personales, con la excepción de que exista otro motivo legal o regulatorio que exija mantenerlos por un período determinado de tiempo. Adicionalmente, este Principio fomenta la confianza entre los usuarios y los proveedores de servicios de redes sociales, ya que permite la transparencia en la contratación o pacto, al mismo tiempo que garantiza la protección a los derechos del consumidor y la protección de los datos de los usuarios.

4. Principio de Autorregulación.

El autor Barriuso (2009) en su obra “Las redes sociales y la protección de datos hoy” explica que el usuario de estas redes sociales es a la vez consumidor y productor (Prosumer). *“Pero debe saber que su identidad digital y sus relaciones sociales en línea repercuten en la vida real, que a su vez retroalimenta su identidad digital”*(p. 303).

Dicha explicación alude a que los usuarios tienen otro papel protagónico que es el del consumidor, como ya se mencionó previamente, por ende, es recomendable que exista un Principio que le permita al usuario gestionar de manera conjunta con los servicios de redes sociales, las normas y condiciones que regirán sobre el tratamiento de sus datos personales y la protección de su privacidad e intimidad, con la finalidad de que los usuarios tengan la oportunidad de negociar y acordar términos y condiciones de uso de las redes sociales, especialmente en las áreas sobre el uso y recopilación de la información.

Este principio se debería basar en el poder que tiene el usuario sobre sus datos, por lo cual permitiría a los usuarios ejercer un control total y efectivo sobre la gestión de los mismos, incluyendo la posibilidad de acceder, modificar, limitar el uso o solicitar la eliminación completa de su información. En pocas palabras, el usuario debe tener la capacidad de supervisar por sí mismo la gestión de sus propios datos dentro de las redes sociales y exigir la rendición de cuentas por parte de las empresas, todo ello en el marco del pacto o contrato que hicieron al principio de la relación.

Asimismo, este principio se concentra básicamente en lo siguiente:

La idea esencial de esta propuesta es que haya contratos entre proveedores y usuarios que ayuden a poner en salvaguarda los derechos de los participantes y que, con ello, se logre evitar conductas ilícitas. La segunda tendencia es la que defiende que la Red sea un espacio de plena libertad en donde se eliminen las regulaciones de todo tipo y que los usuarios que participan diariamente sean los que elijan cómo deben conducirse. Esta postura tan radical respalda una total anarquía de Internet, que reivindica el caos (Díaz, 2013, p. 138)

5. Principio de Educación.

Explica la Real Academia Española que el conocimiento es definido como la “acción y efecto de conocer” (Real Academia Española, s.f., definición 1) dicho concepto se relaciona con el principio que se propone, ya que para tener un manejo responsable y transparente de la información de los usuarios de redes sociales la normativa específica debe contemplar que, dentro de las obligaciones y deberes de los proveedores que ofrecen servicios de redes sociales se exige proveerle a sus usuarios una educación integral y continua sobre el uso seguro y responsable de dichas plataformas digitales.

Además de ello, este Principio tendría como objetivo otorgarle a los usuarios las herramientas necesarias para que no existan fallas de mercado tales como la asimetría de la información, es decir, permitirle a los usuarios que no poseen un conocimiento profundo sobre los riesgos asociados a la protección de sus datos personales en las redes sociales, tener las herramientas precisas para exigir sus derechos, rechazar “*Términos y Condiciones*” con los que no estén de acuerdo, eliminar o rectificar sus datos, ejercer el derecho al olvido de sus datos personales, en pocas palabras, el usuario tomaría decisiones de consumo mucho más informadas o fundamentadas y salvaguardaría su privacidad.

Por último, algunos elementos claves que podrían tomar en consideración los proveedores de servicios de redes sociales serían otorgar servicios gratis de asistencia a los usuarios para que estos reciban orientación y apoyo en cuando al uso seguro y responsable de las redes sociales, también podrían realizar programas de capacitación dirigidos a sus

usuarios, con el objetivo de informarles los temas más actuales sobre la privacidad, seguridad digital, políticas de la empresa sobre el almacenamiento y uso de los datos personales, por su parte, otra manera de que quizás la información se mantenga con el usuario sea que los proveedores de servicios de redes sociales pongan a disposición de los usuarios materiales cortos y dinámicos sobre las prácticas de gestión de su información en las redes sociales.

6. Principio de Auditabilidad.

Este Principio se encuentra sumamente conectado con la transparencia y el consentimiento, ya que le permitirá al usuario tener la seguridad jurídica de que las empresas que ofrecen servicios de redes sociales son susceptibles de ser auditadas sobre los procesos de recopilación, almacenamiento, uso y gestión de los datos personales de los usuarios, además de ello, se revisarían y verificarían regularmente los algoritmos, entendidos de la siguiente forma:

Cada red social posee su propio algoritmo matemático, encargado de determinar qué es visible para cada usuario en su feed. Para ello, es necesario considerar que criterios que revelen las preferencias de los usuarios, como el último contenido visitado, el tiempo de visualización de la publicación o el tipo de interacción con ellos (me gusta, comentarios, compartidos, etc.). (Rodríguez, 2021, como se citó en Jiménez y Gómez, 2019).

Es decir, estos algoritmos son utilizados de una forma que podría afectar la toma de decisiones de los usuarios, un ejemplo de ello es el caso de Facebook que es :

Uno de los gigantes dentro del mundo social network y en este caso nuestro objeto de estudio, reúne cotidianamente grandes cantidades de datos o big data de sus usuarios. Esto le permite crear perfiles que le facilita ubicar las publicaciones de una manera selectiva. Sin embargo, no sólo recaba la información que los usuarios colocan en sus páginas, sino también la de otros sitios en los que sus usuarios también interactúan. (Rodríguez, 2021, como se citó en Magnani, 2017).

Por ende, es necesario que las autoridades competentes encargadas de hacer cumplir la normativa de la protección de datos de los usuarios en las redes sociales tengan la capacidad

de auditar los algoritmos de estas plataformas, y quizás crear comités o consejos de auditores independientes que estén conformados por expertos en informática, ética, derechos de los usuarios y consumidores, tecnología, permitiendo la prevención de sesgos consciente o inconscientemente, y que pueden resultar en situaciones perjudiciales para ciertos grupos.

En pocas palabras, la auditoría permitiría identificar y corregir estos sesgos, de hecho, la revisión y evaluación constante de los algoritmos por parte de expertos podría llevar a mejoras y actualizaciones que beneficien a los usuarios, consumidores y a los mismos proveedores de servicios de redes sociales.

7. Principio de Colaboración.

A pesar de que dentro de la presente propuesta se está recomendado que Venezuela tenga normativas específicas sobre la protección de datos de los usuarios en redes sociales, también sería ideal que el país fuese miembro de un Trato Internacional que regule el tema y tomar como guía el Principio Trece estipulado por la OEA en los “Principios Actualizados sobre privacidad y la protección de datos personales con anotaciones” (Resolución CJI/Res. 266) sobre las “*Autoridades de Protección de Datos*” en el cual indica lo siguiente:

Los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios. Los Estados Miembros deberían promover la cooperación entre tales órganos. (OEA, 2021, p. 16)

Es fundamental que exista una cooperación efectiva entre las empresas que ofrecen servicios de redes sociales y los organismos estatales encargados de la protección de datos personales y el entorno digital en el país. Entre estos organismos se encuentran la Comisión Nacional de Telecomunicaciones (CONATEL) y la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), los cuales deben cooperar en el marco de sus competencias establecidas por la ley que los rige. Es crucial que estos organismos cuenten con talento humano capacitado para llevar a cabo sus funciones de manera eficiente.

Las empresas de redes sociales deben facilitar el acceso de las autoridades competentes a su información, algoritmos y sistemas utilizados en la gestión de datos personales de los usuarios, permitiendo inspecciones y auditorías. Además, se considera necesario, desde el punto de vista de la eficiencia regulatoria, la creación o fortalecimiento de un organismo de defensa del consumidor y usuario robusto, con las capacidades técnicas necesarias para atender las nuevas dinámicas en las que interactúan los consumidores en el entorno digital.

El objetivo principal de esta cooperación es generar un entorno de confianza entre usuarios, consumidores, el Estado y las empresas de redes sociales. Se deben implementar mecanismos efectivos para que los usuarios puedan reportar incidencias, solicitar información o ejercer sus derechos sobre la gestión de sus datos personales.

CONCLUSIONES

A través del análisis económico del derecho, se realizó una revisión documental y análisis de la información recopilada, así como entrevistas, para entender tanto aspectos normativos como la perspectiva del consumidor, elementos claves para la propuesta de los principios rectores.

Como se ha planteado previamente y según los expertos entrevistados, el individuo es el producto, el valor fundamental de la operación entre la red social y sus datos. Son los datos de los usuarios lo que realmente interesa a las empresas que ofrecen servicios de redes sociales, pues a partir de ellos pueden obtener ganancias y desarrollar más proyectos.

A pesar de que existen regulaciones específicas para el tratamiento de datos personales a nivel internacional, el abuso por parte de las empresas privadas es evidente. Estas estudian al individuo y el mercado de usuarios de forma detallada, aprovechándose de que las "Políticas" o "Términos y Condiciones" que los usuarios deben aceptar son documentos exageradamente extensos, engorrosos y técnicos, que pocos leen completamente. Esto genera un desequilibrio de información que permite a las empresas recolectar datos sensibles, como fecha de nacimiento, ubicación, preferencias o inclinaciones

personales, sin que los usuarios sean plenamente conscientes de quién tiene sus datos, qué hacen con ellos y cómo los utilizan.

En Latinoamérica, si bien las autoridades han observado la importancia de la tecnología y de los datos personales, y la necesidad de digitalizar procesos, no se le ha dado la suficiente importancia a la protección de los datos personales. Esto se refleja en la falta de regulaciones específicas y en la falta de mecanismos efectivos para hacer cumplir las regulaciones existentes.

Es importante señalar que este no es un problema exclusivo de Latinoamérica. En todo el mundo, las empresas de redes sociales han sido acusadas de abusar de los datos personales de los usuarios. En algunos casos, estas empresas han sido sancionadas por las autoridades, pero en muchos otros casos, han quedado impunes.

La situación es preocupante, ya que los datos personales son un activo muy valioso para las empresas. Con ellos, pueden elaborar perfiles detallados de los usuarios, conocer sus gustos y preferencias, y ofrecerles publicidad personalizada. Esta información también puede ser utilizada para manipular a los usuarios, por ejemplo, para influir en sus decisiones de compra o en sus votos en elecciones.

Es fundamental que los usuarios sean conscientes de la importancia de proteger sus datos personales. Para ello, es necesario que lean detenidamente las "Políticas" o "Términos y Condiciones" de las redes sociales que utilizan, y que se informen sobre cómo pueden ejercer sus derechos en relación con sus datos personales.

También es importante que las autoridades tomen medidas para proteger los datos personales de los usuarios. Para ello, es necesario que se establezcan regulaciones claras y específicas, y que se creen mecanismos efectivos para hacer cumplir estas regulaciones. Solo de esta forma se podrá garantizar que los datos personales de los usuarios sean utilizados de forma responsable y transparente.

Como se ha planteado previamente y según los expertos entrevistados, el individuo es el producto, el valor fundamental de la operación entre la red social y sus datos. Son los

datos de los usuarios lo que realmente interesa a las empresas que ofrecen servicios de redes sociales, pues a partir de ellos pueden obtener ganancias y desarrollar más proyectos.

A pesar de que existen regulaciones específicas para el tratamiento de datos personales a nivel internacional, el abuso por parte de las empresas privadas es inminente. Estas estudian al individuo y el mercado de usuarios de forma detallada, aprovechándose de que las "Políticas" o "Términos y Condiciones" que los usuarios deben aceptar son documentos exageradamente extensos, engorrosos y técnicos, que pocos leen completamente. Esto genera un desequilibrio de información que permite a las empresas recolectar datos sensibles, como fecha de nacimiento, ubicación, preferencias o inclinaciones personales, sin que los usuarios sean plenamente conscientes de quién tiene sus datos, qué hacen con ellos y cómo los utilizan.

Esta situación se ha evidenciado hasta la fecha, y con la dinámica de estos mercados, surgen nuevos espacios en los que las plataformas pueden tener conductas abusivas con respecto a distintos temas de cara al consumidor.

En Latinoamérica, si bien las autoridades han observado la importancia de la tecnología que se nutre de los datos personales, y la necesidad de digitalizar procesos administrativos, en el caso de Venezuela la normativa es insuficiente. No se delimita claramente quién recolecta los datos, para qué fines, cómo se obtiene el consentimiento de los usuarios, ni las condiciones de seguridad en el almacenamiento de esos datos.

Las futuras legislaciones sobre protección de datos personales y su gestión en redes sociales deben tener una visión menos individualista, considerando el impacto colectivo de la recolección de datos. Debe haber transparencia para el usuario sobre quién posee sus datos y cómo se utilizan, pero también se debe analizar cómo esos datos, que son el combustible económico de empresas y gobiernos, facilitan u obstaculizan el ejercicio de los derechos económicos, digitales y culturales de los usuarios. Además, las normativas deben prever que los agentes económicos, públicos o privados, gestionen los datos de forma arbitraria, afectando a sectores enteros mediante estrategias de negocios o políticas públicas. Es necesario que el gobierno venezolano implemente una regulación visionaria, alineada a

estándares internacionales, que permita la creación de autoridades especializadas capaces de fiscalizar el cumplimiento de los derechos digitales de los usuarios

REFERENCIAS

- Álvarez P, T. (2008). El Hábeas Corpus y la Tutela de la Libertad Personal. Corte Interamericana de Derechos Humanos, Pág. 23. Disponible en: <https://www.corteidh.or.cr/tablas/r23321.pdf>
- Arpio Santacruz, J. (2024). Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 4 de julio de 2023. Asunto C-252/21 Meta Platforms Inc., Meta Platforms Ireland Ltd y Facebook Deutschland GmbH c. Bundeskartellamt [ECLI:EU:C:2023:537]: Defensa de la competencia por las autoridades nacionales y derecho de protección de las personas físicas en lo que respecta al tratamiento de los datos personales. AIS: *Ars Iuris Salmanticensis*, 12(1), 244–249. <https://revistas.usal.es/cuatro/index.php/ais/article/view/32053>
- Arteaga, H. (2024). La procedencia del habeas data cuando existen elementos inherentes a la justicia ordinaria. Universidad San Gregorio de Portoviejo, Departamento de Posgrado. <http://repositorio.sangregorio.edu.ec/handle/123456789/3428>
- Baño Carvajal, Ángela E. ., & Reyes Estrada, J. L. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. *Revista Jurídica Crítica Y Derecho*, 1(1), 49–60. <https://doi.org/10.29166/criticayderecho.v1i1.2447>
- Barbaschow, Asha. (2022). *Turns Out Tiktok Does Does Have an Alarming Level of Access to Your Phone*. Gizmodo Au. <https://gizmodo.com.au/2022/07/tiktok-app-phone-access/>
- Barriuso, Carlos (2009). “Las redes sociales y la protección de datos hoy”. Universidad de Alcalá II, *Anuario Facultad de Derecho* 301-338, p. 303. Disponible en: https://core.ac.uk/outputs/58906859/?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1
- Benavides, S. L., et al. (2021). La manifestación del consentimiento en los contratos click-wrap: análisis del poder vinculante de un click. <http://hdl.handle.net/10554/62296>

- Bundeskartellamt. (2019). Bundeskartellamt prohibits Facebook from combining user data from different sources. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html
- Burgos Chumpitazi, M. R., & Saldivar Vidaurre, U. G. Propuesta de protección de datos personales y confidenciales de los clientes para la prevención de riesgos en la empresa Support Brigades Fire & Safety SAC. <http://hdl.handle.net/10757/670307>
- Caloca Osorio, O. R., & Leriche Guzmán, C. E. (2011). **Una revisión de la teoría del consumidor: la versión de la teoría del error**. Análisis Económico, XXVI(61),21-51. <https://www.redalyc.org/articulo.oa?id=41318401003>
- Cañas O., S. (2023).Abusos explotativos de posición dominante en precios en plataformas digitales y su aplicación a la explotación de datos. <https://repositorio.uchile.cl/handle/2250/194971>
- Cedeño, C. (2021). La protección de datos en Venezuela. Revista de Derecho Penal Económico, No. 2-XXI. <https://www.rdpe.info/la-proteccion-de-datos-en-venezuela/>
- Chavez Vilcahuaman, R. D., Aldaba Murrieta, M. N. ., & Corrales Baldoceda, C. E. . (2020). Una revisión teórica sobre la adopción del comercio electrónico. Revista De Investigación Valor Agregado, 7(1), 61–66. <https://doi.org/10.17162/riva.v7i1.1418>
- Children’s Online Privacy Protection Act (COPPA). (1998). <https://www.congress.gov/105/bills/s2326/BILLS-105s2326is.pdf>
- Comisión Económica para América Latina y el Caribe (2024). “*Gestión de datos de investigación: Privacidad de los datos y confidencialidad*”. Biblioteca CEPA, Biblioguías. Versión web: <https://biblioguias.cepal.org/c.php?g=495473&p=4398114>
- Comisión Económica para América Latina y el Caribe. (2002). *Principios Básicos de la protección de datos*. <https://biblioguias.cepal.org/c.php?g=495473&p=4398118>

- Comisión Económica para América Latina y el Caribe. (2024). Gestión de datos de investigación: Privacidad de los datos y confidencialidad. Biblioteca CEPA, Biblioguías. V<https://biblioguias.cepal.org/c.php?g=495473&p=4398114>
- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: “Una estrategia europea para los datos” (Bruselas, 19 de febrero de 2020) p., 4. Consultado en <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3a52020DC0066>
- Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones. (2018) “La lucha contra la desinformación en línea: un enfoque europeo” COM(2018) 236. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=EN>
- Consejo de Europa (1950). Convenio Europeo de Derechos Humanos (CEDH). [https://elearning.icrc.org/detention/es/story_content/external_files/Convenci%C3%B3n%20Europea%20de%20Derechos%20Humanos%20\(1950\).pdf](https://elearning.icrc.org/detention/es/story_content/external_files/Convenci%C3%B3n%20Europea%20de%20Derechos%20Humanos%20(1950).pdf)
- Consumers Internacional (CI). (2016). Guía practica sobre las directrices de Naciones Unidas de Protección al Consumidor. Consumers International, 24 Highbury Crescent, Pág. 11. Londres, Inglaterra. https://unctad.org/system/files/official-document/ditccplpmisc2016d1_es.pdf
- Corona Lisboa, J. L. (2018). Investigación cualitativa: fundamentos epistemológicos, teóricos y metodológicos. *Vivat Academia*, (144), 69–76. <https://doi.org/10.15178/va.2018.144.69-76>
- Coronado A, L. (2019). Teoría de Comportamiento del Consumidor. https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/6965/Linda_Exam.Suf.Prof_Titulo_2019.pdf?sequence=1&isAllowed=y
- De La Cruz Rodríguez, G., Méndez Fernández, R. A., & Méndez Fernández, A. C. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Innovación y Software*, 4(1), 219-236. <https://www.redalyc.org/articulo.oa?id=673874721015>
- Díaz B, Anid (2013). “La autorregulación en redes sociales como forma de garantizar los derechos de intimidad, privacidad y protección de datos personales”. *Revista Internacional*

de Derecho de la Comunicación y de las Nuevas Tecnologías, p. 138. Disponible en:
<https://dialnet.unirioja.es/descarga/articulo/4330473.pdf>

- Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, del Grupo de Protección de datos del Artículo 29, adoptadas el 04 de mayo de 2020.
https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf
- Estella, F. D. (2023). ¿Se puede cometer un abuso de domino ex artículo 102 TFUE en relación los datos personales y por infracción del RGPD?. Revista de Derecho de la Competencia y la Distribución. <https://fernandodiezestella.com/>
- Flass, G. (2019). El concepto de consumidor. Anuario De Derecho Civil, 12, 1-63. [https://doi.org/10.22529/adc.2017\(12\)01](https://doi.org/10.22529/adc.2017(12)01)
- Flores de Valgas Cedeño, S. B. (2024). El comercio electrónico y su incidencia en el derecho a la protección de datos personales.
<https://repositorio.sangregorio.edu.ec/handle/123456789/3638>
- Gárate Amoroso, J. ., Reina Cunín, J., Samaniego Nugra, E. ., & Loyola Moreano, K. . (2021). Habeas Data: origen y evolución. *Revista Lex*, 4(13), 197–210.
<https://doi.org/10.33996/revistalex.v4i13.82>
- García Pérez, R. M. (2020). Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales. *Cuadernos De Derecho Transnacional*, 12 (1), 875-907. <https://doi.org/10.20318/cdt.2020.5228>
- Gavilanes, C. (2024). Los riesgos contractuales de las plataformas digitales: Caso Meta-Facebook. Universidad Regional Autónoma de Los Andes (UNIANDES).
<https://dspace.uniandes.edu.ec/handle/123456789/17730>
- Gomez-Barrera, J. (2021). Estudiar las redes sociales: perspectivas teóricas para un análisis, Mediaciones, 26 (17) Pp. 190-203.
<https://dialnet.unirioja.es/descarga/articulo/7996370.pdf>
- GQ. (28 de febrero de 2021). Facemash: la red social ilegal que Zuckerberg inventó antes de Facebook. GQ.
<https://www.gq.com.mx/entretenimiento/articulo/facemash-historia-red-social-antes-de-facebook>

- Gutiérrez Cruz, F., & Moreno Brid, J. C. (2024). Teoría de juegos y elección racional: selección de candidatos en México en 2021. *Revista Mexicana De Ciencias Políticas Y Sociales*, 69(252). <https://doi.org/10.22201/fcpys.2448492xe.2024.252.86741>
- Hurtado de Barrera, J. (2024). Investigación proyectiva: más allá de la investigación tecnológica. *Impacto Científico*, 19(1), 13-26. <https://produccioncientificaluz.org/index.php/impacto/article/view/42213>
- Islas, O., Arribas, A., & Garcés, M. E. (2022). Luces y sombras en la breve historia de Facebook, hoy Meta. *Razón y Palabra*, 25 (112), p. 473. <https://doi.org/10.26807/rp.v25i112.1897>
- La Declaración Universal de Los Derechos Humanos. (1948). <https://www.un.org/es/about-us/universal-declaration-of-human-rights>
- Laurente M, J. (2022). La asimetría informativa y el derecho de protección al consumidor en productos, servicios de telefonía, distrito de Los Olivos. Universidad César Vallejo, p. 6. <https://hdl.handle.net/20.500.12692/132403>
- Ley francesa N° 78-17. (1978). Relativa a la informática, los archivos y las libertades (modificada hasta el 1 de junio de 2019). <https://www.wipo.int/wipolex/es/legislation/details/18965>
- López D, P. (2023). *Aggressive Practices and Consumer Protection: An Approach from Chilean Law*. *Latin American Legal Studies*, Vol. 11 N° 2, pp. 115-181. [HTTPS://DOI.ORG/10.15691/0719-9112VOL11N2A4](https://doi.org/10.15691/0719-9112VOL11N2A4)
- López M, S. (2020). Cómo la economía emocional puede ayudar a resolver las fallas de la economía neoclásica para entender la conducta del consumidor. Universidad de Guanajuato. <http://repositorio.ugto.mx/handle/20.500.12059/7499>
- López M, Selene (2020). “Cómo la economía emocional puede ayudar a resolver las fallas de la economía neoclásica para entender la conducta del consumidor”. Universidad de Guanajuato, p. . Recuperado de: <http://repositorio.ugto.mx/handle/20.500.12059/7499>
- Machuca Vivar, S. A., Vinuesa Ochoa, N. V., Sampedro Guamán, C. R., & Santillán Molina, A. L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244-251.

http://scielo.sld.cu/scielo.php?pid=S2218-36202022000200244&script=sci_arttext&tlng=pt

- Mankiw. Gregory N. (2012). “Principios de Economía” Pág. 472.
<https://clea.edu.mx/biblioteca/files/original/bd2711c3969d92b67fcf71d844bcbaed.pdf>
- Martín Artiles, A. (2022). Manuel Santana Turégano. ¿Homo economicus u homo sociologicus? Madrid: Editorial Aula Magna, 2022. McGraw-Hill Interamericana de España S.L. Revista Española De Sociología, 32(1), a155.
<https://doi.org/10.22325/fes/res.2023.155>
- Melo, Verónica (2022). “Inteligencia artificial, desinformación y protección de datos personales”. Revista Digital de Estudios Humanísticos de la Universidad FASTA, ISSN 1853-5585, p. 30. Disponible en:
<https://repositorio.uca.edu.ar/bitstream/123456789/16405/1/inteligencia-artificial-desinformaci%C3%B3n.pdf>
- Mosqueda, S. (2022). Cómo la economía emocional puede ayudar a resolver las fallas de la economía neoclásica para entender la conducta del consumidor. (Tesis de licenciatura). Repositorio Institucional de la Universidad de Guanajuato:
<http://repositorio.ugto.mx/handle/20.500.12059/7499>
- Nieves-Lahaba, Y., y Ponjuan-Dante, G. (2021). Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia. Universitas-XXI, 35, pp. 167-185. <https://doi.org/10.17163/uni.n35.2021.08>
- Oberto de Grube, L., & Govea de Guerrero, M. (2008). Algunas Consideraciones Sobre El Habeas Data En Venezuela. Télématique, 7(3),100-109.
<https://www.redalyc.org/articulo.oa?id=78411657006>
- Organización de los Estados Americanos (OEA). (2021). Protección de datos personales: Principios actualizados.
[https://www.oas.org/es/sla/cji/docs/Publicacion Protección Datos Personales Principios Actualizados 2021.pdf](https://www.oas.org/es/sla/cji/docs/Publicacion%20Proteccion%20Datos%20Personales%20Principios%20Actualizados%202021.pdf)
- Osorio Morales, Hugo. (2021). Análisis económico en el derecho: defensa de una metodología. Revista de derecho (Coquimbo), 28, 10.
<https://dx.doi.org/10.22199/issn.0718-9753-2021-0010>

- Otero Laborda, V. J. (2021). Impacto económico y financiero del uso de redes sociales en empresas dedicadas a la comercialización de prendas de vestir en Guayaquil (Bachelor's thesis). <http://dspace.ups.edu.ec/handle/123456789/21394>
- Villacís, Carlos. (2021). La preferencia revelada frente al enfoque utilitarista: discusión sobre los fundamentos de la teoría del consumidor. *Cinta de moebio*, (72), 164-182. <https://dx.doi.org/10.4067/s0717-554x2021000300164>
- Palomino Diez, Isabel (2009). La Protección de Datos de Carácter Personal. Universidad Europea Miguel de Cervantes. <https://uvadoc.uva.es/bitstream/handle/10324/66277/Cap%C3%ADtulo%20de%20ibro.%20La%20protecci%C3%B3n%20de%20datos%20de%20car%C3%A1cter%20personal.pdf?sequence=1>
- Peña P, P.(2021). El derecho a la muerte digital y la protección post mortem de los datos personales: nuevas prerrogativas aplicables al ecosistema digital. Revista de la Facultad de Derecho de México, p. 737. https://www.researchgate.net/publication/347057809_La_proteccion_de_los_datos_personales_como_derecho_fundamental_su_autonomia_y_vigencia_propia_en_el_ordenamiento_juridico_estatal
- Peruzzotti, M. (2024). Actualidad en materia de protección de datos personales en Argentina. Cuadernos del Centro de Estudios en Diseño y Comunicación. Ensayos, (217), 191-203. <https://dialnet.unirioja.es/servlet/articulo?codigo=9567040>
- Platero Alcón, A., & Jiménez Asensio, C. (2017). El consumidor online en el ordenamiento jurídico español. Nuevo Derecho. 13(21),57-80. ISSN: 2011-4540. <https://www.redalyc.org/articulo.oa?id=669770733003>
- Polo R, A. (2022). Privacidad, Intimidad y Protección de Datos: Una mirada estadounidense y europea. Revista De Filosofía Del Derecho Y Derechos Humanos. <https://doi.org/10.20318/dyl.2022.6884>
- Polo Roca, A. (2020). El Derecho A La Protección De Datos Personales Y Su Reflejo En El Consentimiento Del Interesado. Revista de derecho político, (108). <https://scholar.googleusercontent.com/scholar?q=cache:Ze38qmbgFSEJ:scholar.google.com/+EL+DERECHO+A+LA+PROTECCI%C3%93N+DE+DATOS+PERSO>

[NALES+Y+SU+REFLEJO+EN+EL+CONSENTIMIENTO+DEL+INTERESADO
&hl=es&as_sdt=0,5&as_ylo=2020](#)

- Porven Hondares, Y., Morejón Almora, R., & Pérez Véliz, A. (2021). La protección de datos personales. Presupuestos constitucionales para su protección en los procesos judiciales en Cuba. *Revista Científica Ecociencia*, 8, 126–161. <https://doi.org/10.21855/ecociencia.80.644>
- Real Academia Española (RAE), sección de Diccionario panhispánico del español jurídico. “Red Social”. Versión web: <https://dpej.rae.es/lema/red-social>
- Rico C, M. (2012). El impacto de Internet y las redes sociales en el derecho a la libertad de expresión. *Revista de Filosofía Jurídica, Social y Política*; Instituto de Filosofía del Derecho Dr. J.M. Delgado. Vol. 19, No. 3, 2012: 331 – 349; Universidad Católica del Tachira, Venezuela. Versión web: <https://www.corteidh.or.cr/tablas/r32923.pdf>
- Rico Carrillo, Mariliana. (2012). “*El impacto de Internet y las redes sociales en el derecho a la libertad de expresión*”. *Revista de Filosofía Jurídica, Social y Política*; Instituto de Filosofía del Derecho Dr. J.M. Delgado Ocando. Vol. 19, No. 3, 2012: 331 – 349; Universidad Católica del Tachira, Venezuela. <https://www.corteidh.or.cr/tablas/r32923.pdf>
- Rodríguez A, Alba. (2021). “***La personalización de contenidos en redes sociales: Algoritmos y segmentación en Facebook***”. Universidad de Valladolid, Facultad de Filosofía y Letras, p. 22). Disponible en: https://uvadoc.uva.es/bitstream/handle/10324/52437/TFM_F_2021_135.pdf?sequence=1
- Sala Constitucional del Tribunal Supremo de Justicia. (2011). Expediente Nro. AA50-T-2004-23-95. Caracas. <http://historico.tsj.gob.ve/decisiones/scon/agosto/1318-4811-2011-04-2395.HTML>
- Sánchez D, J. M. y Magallón-Rosa, R. (2023). Desinformación. *Eunomía. Revista en Cultura de la Legalidad*, 24, pp. 236-249. <https://doi.org/10.20318/eunomia.2023.7663>
- Sánchez Duarte, J. M. y Magallón-Rosa, R. (2023). “Desinformación”. *Eunomía. Revista en Cultura de la Legalidad*, 24, pp. 236-249. <https://doi.org/10.20318/eunomia.2023.7663>

- Santi, M. (2016). Ethical controversies involving privacy, confidentiality and anonymity in social research. *Revista de Bioética y Derecho*, (37), 5-21. <https://dx.doi.org/10.1344/rbd2016.37.16147>
- Santiago Campión, R., & Navaridas Nalda, F. (2012). La Web 2.0 en escena. *Pixel-Bit. Revista de Medios y Educación*, (41),19-30. ISSN: 1133-8482.: <https://www.redalyc.org/articulo.oa?id=36828247002>
- Silva Álvarez, G. A. (2024). La naturaleza jurídica del habeas data y el derecho a la protección de datos personales (Bachelor's thesis). <https://dspace.uniandes.edu.ec/handle/123456789/17993>
- Silva Álvarez, G. A. (2024). La naturaleza jurídica del habeas data y el derecho a la protección de datos personales (Bachelor's thesis). <https://dspace.uniandes.edu.ec/handle/123456789/17993>
- Statista (2024). Previsión del número de usuarios activos mensuales (MAU) de Facebook a nivel mundial desde 2021 hasta 2026 (en millones). <https://es.statista.com/estadisticas/635414/numero-de-usuarios-mensuales-activos-de-facebook-en-el-mundo/>
- Tejero G, Jesús. (2021). Técnicas de Investigación cualitativa en los ámbitos sanitario y sociosanitario. Ediciones de la Universidad de Castilla-La Mancha, p. 76. <https://hdl.handle.net/10578/28525>
- Turégano M, I. (2020). Los valores detrás de la privacidad. Universidad de Alicante, Departamento de Filosofía de Derecho, pág. 258. <https://rua.ua.es/dspace/handle/10045/106968>
- Universidad Católica San Pablo (UCSP), postgrado. *Artículo: Big Data: definición, tipos, características y beneficios*. <https://postgrado.ucsp.edu.pe/articulos/que-es-big-data/>
- Vare M, Víctor (2023). La asimetría informativa y su incidencia en los derechos del consumidor en el comercio electrónico peruano. Universidad Privada del Norte, p. 18. <https://hdl.handle.net/11537/35240>
- Vargas Basilio, M., Yaulilahua Llancari, S. M., & Quincho Zevallos, H. (2024). Gestión de redes sociales y el nuevo consumidor digital millennial en una ciudad del

Perú. Revista de Investigación en Comunicación y Desarrollo, 15(1), 44-55.
<https://doi.org/10.33595/2226-1478.15.1.1000>

- Vergara, E. (05 de septiembre de 2022). Discurso de Kennedy por los Derechos de los Consumidores - President Kennedy Message to the Congress.
https://www.youtube.com/watch?v=kVU_aMkBFxw
- Zubillaga, M. (2022). Recorrido por la normativa sobre protección de datos en la Unión Europea y la situación en Venezuela. Revista de derecho público, (171), 226-241. <https://dialnet.unirioja.es/servlet/articulo?codigo=9132393>