

Impacto de las Redes Sociales en la Privacidad de la sociedad en los Medios Digitales

Mg. Madeleine Karin Bartra-Bautista¹  Mg. Janet Natalia Mendoza-Rejas²  Mg. Kelly Fara Vargas-Prado³ , Dra. Elizabeth Lizbel Jurado-Enriquez⁴ , Mg. Ursula Rosalia Aniceto-Norabuena⁵ , Mg. Cinthya Paucarhuanca-Tenorio⁶ , and Mg. Ignacia Tinco-Melchor⁷ 

¹Universidad Tecnológica del Perú, Perú, c20592@utp.edu.pe

²Universidad Tecnológica del Perú, Perú, c20618@utp.edu.pe, ³Universidad Autónoma de Ica, Perú, kelly.vargas@autonomadeica.edu.pe, ⁴Universidad Tecnológica del Perú, Perú, c20422@utp.edu.pe

⁵Universidad Nacional Santiago Antúnez de Mayolo, Perú, uaniceton@unasam.edu.pe

⁶Universidad Tecnológica del Perú, Perú, Perú, c22986@utp.edu.pe

⁷Universidad Tecnológica del Perú, Perú, Perú, c20428@utp.edu.pe

Abstract– Social networks in the privacy of society in the digital sphere is important today, being a complex issue that requires a multidisciplinary approach, implementation of legal and technological measures. The objective was to examine social networks, which have changed the way we share personal information and interact online, identifying the violation of the privacy of people who access them. The PRISMA methodology was essential to rigorously collect and evaluate the relevant information, allowing an accurate and understandable synthesis of the results. There is a need to ensure accuracy and objectivity in data collection and analysis using Scopus and Scielo databases. Data protection results in India are lagging behind other countries, it is important to establish a solid legal framework in this area. Mention is made of the concept of "right to be forgotten" implemented in the European Union as a commendable measure that gives individuals a second chance and protects their reputation. Finally, in Latin America, countries such as Chile, Peru, Colombia, Brazil and Uruguay have established laws that ensure the protection of consumers' personal data, emphasizing the importance of consent for data processing. The social landscape of social networks is based on shared emotions and generates virtual communities through the distribution of memes and humorous content. The need to balance freedom of expression with the protection of brands is debated.

Keywords– Social networks, Digital privacy, Personal data, Online security, Digital footprint

Resumen–Las redes sociales en la privacidad de la sociedad en el ámbito digital es importante en la actualidad siendo un tema complejo que requiere un enfoque multidisciplinario, implementación de medidas legales y tecnológicas. El objetivo examinar las redes sociales, las cuales han modificado la forma en que compartimos información personal y nos relacionamos en línea identificando la vulneración de la privacidad de las personas que acceden a ellas. La metodología PRISMA fue esencial para recopilar y evaluar de manera rigurosa la información pertinente permitió una síntesis precisa y comprensible de los resultados. Hay necesidad de asegurar la precisión y objetividad en la recopilación y análisis de datos haciendo uso de base de datos Scopus y Scielo. Los resultados de protección de datos en la India están rezagados en comparación con otros países, tiene importancia de establecer un marco legal sólido en este ámbito. Se hace mención del concepto de "derecho al olvido" implementado en la Unión Europea como una medida elogiable que brinda a los individuos una segunda oportunidad y protege su reputación. Finalmente, en América Latina, países como Chile, Perú, Colombia, Brasil y Uruguay han establecido leyes que aseguran la protección de los datos personales de los

consumidores, enfatizando la importancia del consentimiento para el procesamiento de datos. El panorama social de las redes sociales se basa en emociones compartidas y generan comunidades virtuales mediante la distribución de memes y contenidos humorísticos. Se debate la necesidad de equilibrar la libertad de expresión con la protección de las marcas.

Palabras clave– Redes sociales, medios digitales, privacidad, libertad de expresión, protección

I. INTRODUCCIÓN

En los últimos años, se ha producido cambios con los avances de las nuevas tecnologías de la información, de dispositivos electrónicos conectados a internet y el procesamiento masivo de datos personales [1]. Estos cambios principales amenazan a la privacidad ya no vengán de los medios de comunicación convencionales, sino que son moldeadas con tecnologías y en especial las redes sociales, sean la fuente principal de conflictos [2].

Las prácticas comunicativas y relacionales cotidianas están cada vez más influenciadas por lo digital, ya que el Internet se ha vuelto parte en la vida cotidiana de los jóvenes [3] [4]. Según Ciolan (2014) [5], la apertura de nuevos canales de información ha revolución en las formas de comunicación y en las experiencias asociadas a su uso

Desde el ámbito jurídico, el Reglamento General de Protección de Datos (RGPD), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo representa el marco normativo en Europa para la protección de datos personales. En vigencia desde el 25 de mayo de 2018, busca garantizar que los ciudadanos de la Unión Europea ejerzan un control efectivo sobre su información personal. Se basa en principios como la legalidad, equidad, transparencia, minimización de datos, seguridad y responsabilidad. Además, exige a las empresas pedir el consentimiento claro del usuario, informar si hay alguna filtración de datos y, en algunos casos, nombrar a un delegado de Protección de Datos (DPO). Las multas pueden llegar hasta los 20 millones de euros o el 4 % de los

ingresos anuales de una empresa, lo que demuestra Protección de Datos (DPO). [6]

Este modelo europeo ha influenciado a nivel internacional, sirviendo de referencia para normativas similares en otras regiones. En América Latina, países como Brasil, Colombia y Perú han desarrollado marcos legales para garantizar la protección de datos como un derecho fundamental. [7] [8] [9] La Ley General de Protección de Datos Personales de Brasil (Ley N.º 13.709/2018) reconoce como esencial el ejercicio de la ciudadanía. En Colombia, la Ley Estatutaria 1581/2012 promueve la autodeterminación informativa y establece controles ciudadanos sobre el uso de datos. En Perú cuenta con la Ley N.º 29733, Ley de Protección de Datos Personales, promulgada en 2011, garantiza principios como el consentimiento informado, la finalidad específica, la calidad y la seguridad de los datos.

Desde lo conceptual, D. M. Boyd y N. B. Ellison definen las redes sociales como “servicios web que permiten construir un perfil público o semipúblico dentro de un sistema delimitado, articular una lista de otros usuarios con los que comparten una conexión, y ver y recorrer sus listas de conexiones dentro del sistema” [10]. En este entorno, la privacidad se vuelve compleja. Como señala D. J. Solove, implica un conjunto de problemas vinculados con la recopilación, procesamiento, difusión e invasión de datos personales [11].

Reflexionar sobre la privacidad y su impacto social también considera el concepto de sociedad. Según A. Giddens, la sociedad es “un sistema de interrelaciones que conecta a los individuos que la componen” [12], lo cual implica que cualquier cambio en la manera en que las personas se relacionan digitalmente afecta la estructura social. En este sentido, H. Jenkins señala que los medios digitales han generado una cultura participativa, en la que los usuarios no solo consumen contenido, sino que también lo producen, transformando los modelos tradicionales de comunicación [13]

G. González-Fuster resalta que la protección de los datos personales ha emergido como un derecho fundamental en la Unión Europea, esencial para salvaguardar la dignidad humana en la era digital [14]. Así, la privacidad debe ser entendida como un derecho estructural dentro de la sociedad digital, cuyo respeto y garantía son indispensables para el desarrollo de una ciudadanía activa, informada y segura en el ciberespacio.

La situación descrita anteriormente se vuelve más complicada debido a la forma en que funcionan y están estructuradas las redes sociales. Estas plataformas fomentan que las personas compartan una gran cantidad de información personal sin considerar las posibles consecuencias de esta difusión. A pesar de esto, las personas aún mantienen la esperanza de que la información compartida en línea permanecerá como privada.

Se ha argumentado que, dentro del contexto de las redes sociales, las personas actúan bajo una falsa sensación de seguridad, ya que confían en que la información que comparten allí será privada, a pesar de que los tribunales han rechazado repetidamente esta idea [15].

Dentro del contexto de la sociedad de la información, surge la disciplina de la protección de datos personales con la finalidad de resguardar la integridad del individuo ante los potenciales riesgos asociados con el manejo de información personal. Su principal propósito no es proteger exclusivamente los datos, sino más bien garantizar la seguridad y bienestar de la persona a la que pertenecen dichos datos [16].

Según Villegas (2012) [17], las principales discrepancias entre los modelos europeos y estadounidense radican en el hecho de que, en el último, la noción de libertad surge como contraposición a la injerencia del Estado en la vida de los ciudadanos, lo que conduce hacia la autorregulación y las regulaciones específicas por sectores. Por el contrario, el enfoque europeo se caracteriza por una protección más amplia y homogénea, partiendo del reconocimiento del derecho fundamental a la privacidad, lo que implica una intervención activa por parte del Estado en la protección de los individuos.

El derecho fundamental a la protección de datos se define específicamente en el artículo 18.4 de la Constitución Española, dentro del derecho a la intimidad del artículo 18.1 de la misma [18].

En Brasil, se reconoce que los derechos a la protección de datos personales e información son considerados como fundamentales y subjetivos para la población.

Estos derechos se consideran los pilares de un estado de derecho y democrático, y requieren la participación de la ciudadanía a través de diversas instituciones sociales [19].

Formular leyes y políticas de protección de datos personales se presenta como un desafío, ya que se consideran un bien de interés público [20]. En Paraguay, se observa una inquietud debido a la ausencia de protocolos para la eliminación de datos sensibles de la población [4].

En Colombia, se plantea la importancia de reforzar la protección de los datos personales y establecer una entidad independiente para regular este ámbito, especialmente en el sector salud. Para lograr este objetivo, es necesario desarrollar herramientas tecnológicas y nuevas estrategias de gestión de la información, en las cuales participen diversos profesionales para asegurar el derecho a la protección de los datos personales [21] [22]. Según diversos estudios, es esencial garantizar el derecho de acceso, modificación y seguridad en los sistemas mientras se previenen posibles amenazas de seguridad en las redes [23].

Sin embargo, las consecuencias de las prácticas de aprendizaje, los comportamientos y las interacciones sociales resultantes del uso de Internet aún están en debate. Este

capítulo investiga la relación entre los jóvenes y el uso de los medios digitales explorando sus riesgos y efectos potenciales en la socialización, sociabilidad y formación de identidad de los jóvenes.

Finalmente, en el contexto digital actual, es importante analizar las políticas de privacidad de las redes sociales y los riesgos inherentes para promover un entorno en línea más seguro en beneficio de la sociedad.

Redes sociales

Las redes sociales son plataformas digitales que permiten la interacción, elaboración y propagación de contenido entre individuos, comunidades e instituciones. Estas herramientas han transformado los medios de comunicación tradicional, facilitando nuevas formas de participación ciudadana y transparencia pública. Según Pertegal, Delgado y Rodríguez (2019), las redes sociales son un fenómeno que abarca dimensiones tecnológicas, culturales y sociales, cuyo uso varía según la experiencia del usuario y el contexto socio tecnológico [24]. Esta complejidad también implica riesgos, como el ciberacoso y la exposición no consentida, especialmente entre jóvenes (Marín-Cortés y Linne, 2021) [25].

Privacidad

La privacidad, se refiere al derecho de los individuos a controlar el acceso, uso y difusión de su información personal en entornos digitales. En las redes sociales, esta noción se vuelve frágil debido a la constante exposición de datos y la vigilancia algorítmica. Abbas et al. (2023) señalan que muchos gobiernos utilizan mecanismos digitales no solo para censurar contenidos, sino también para vigilar a los ciudadanos, socavando así los derechos a la privacidad y a la libre expresión [1]. Asimismo, advierten que la vigilancia masiva en los entornos digitales contribuye a una "normalización del control", debilitando la concepción de privacidad como derecho fundamental [16].

Sociedad

La sociedad contemporánea se encuentra profundamente atravesada por el proceso de digitalización, configurando una “sociedad hipervisualizada” en la que la exposición mediática y la construcción de identidades digitales como prácticas cotidianas (Rocha y Filpo, 2018) [26]. Esta realidad conlleva una redefinición de los vínculos sociales y de los espacios públicos y privados. En este contexto Guzzetti y Lesley (2015), señalan que los medios digitales modifican la estructura tradicional del poder comunicacional, desplazando la influencia de los medios masivos hacia una participación más horizontal, pero también más fragmentadas [27].

Medios digitales

Los medios digitales conforman un entorno donde confluyen tecnologías de la información, la comunicación y la interacción social. Se caracterizan por estar presente en todo

momento, por su rapidez y amplia capacidad de almacenamiento y compartir información. Garavaglia et al. (2020) indica que los jóvenes, son los principales usuarios de estas plataformas, acceden a diversas oportunidades para empoderarse digitalmente, aunque también son expuestos a riesgos frecuentes como la desinformación o la exposición involuntaria [22]. Por su parte, Kemp (2024) sostiene que el crecimiento del uso de medios digitales a nivel mundial plantea nuevos desafíos, entre ellos mayor responsabilidad en el cuidado de los datos personales y la alfabetización digital [28].

II. MÉTODOS

La metodología PRISMA facilita la organización y análisis de todos los artículos pertinentes al tema, lo que permite sintetizar la información y proporcionar una respuesta más precisa y comprensible [29]. El propósito de la revisión sistemática fue indagar acerca de las siguientes interrogantes:

QR1: ¿Qué regulaciones jurídicas se han implementado en vulneración al derecho a la privacidad en relación con el acceso a redes sociales? La revisión sistemática implica realizar una evaluación minuciosa e interpretación exhaustiva de la investigación, siendo esencial para fundamentar una pregunta de investigación específica o un área de interés particular [29]. Además, el uso de la metodología PRISMA simplifica la comparación de los resultados obtenidos con otras revisiones sistemáticas y metaanálisis en el mismo campo, lo que permite integrar los descubrimientos de diferentes investigaciones [30].

QR2: ¿Qué métodos jurídicos se han implementado para determinar el nivel de vulneración al derecho a la privacidad personal con relación al acceso a redes sociales?

P	Sociedad civil
I	Método e implementación de la regulación jurídica del derecho a la privacidad personal
C	Clima e imagen institucional
O	Nivel de vulneración del derecho a la privacidad
C	espacios de trabajo: plataformas más populares al acceso de las redes sociales

2.1. Estrategias de búsqueda

La búsqueda se realizó en la base de datos Scopus y Scielo el día 24 de febrero del 2024. Para la pregunta de investigación establecida, era necesario revisar bases de datos de revistas o artículos seleccionados con la ayuda de una serie de palabras clave que permitieran recopilar suficiente información, manteniendo la investigación dentro del mismo ámbito (social, económico, político, seguridad, etc.) [31].

También se tuvo en cuenta que la información debía ser relevante para un análisis posterior. En esta investigación, se incluyó una serie de palabras clave utilizadas para filtrar los resultados de búsqueda en diferentes revistas [32]. Basándose en lo mencionado anteriormente, se creó una lista de palabras clave que sirvieron de base para desarrollar las cadenas de búsqueda requeridas.

Las palabras clave seleccionadas para orientar la estrategia de búsqueda fueron: “Society”, “Civil Society”, “Community”, “Social Network”, “Social Media”, “Right to Privacy”, “Private Rights Legislation” y “Invasion of Privacy” [20].

Las bases de datos utilizadas para la búsqueda fueron Scopus y Scielo, con un rango de búsqueda del año 2010 al 2023. En la Tabla 1 se presenta cómo se emplearon estas palabras clave en la estrategia específica para cada una de las bases de datos utilizadas, así como el total de artículos identificados a partir de dicha búsqueda [33].

TABLA 1.
 RELACIÓN DE ARTÍCULOS IDENTIFICADOS EN LA BASE DE DATOS.

Base de datos	Estrategia de Búsqueda	Identificación
SCOPUS	(“Society” OR “Civil Society” OR “community” AND “Social Network” OR “Social media” AND “right to privacy” OR “privacy rights legislation” OR “Invasion of privacy”)	37
SCIELO	“(right to personal privacy and right to digital information or invasion of privacy)”	15

De acuerdo con los criterios de búsqueda, se obtuvo en total 52 artículos, de los cuáles, la mayoría pertenecen a Scopus y finalmente a Scielo, por lo que se eliminaron de esta última para tener artículos únicos por cada base de datos.

2. 2. Criterios de inclusión y exclusión

Con el objetivo de alcanzar los objetivos establecidos, se realizó un exhaustivo análisis de la literatura siguiendo las pautas y recomendaciones de la Guía PRISMA, elaborada en 2020 por Page et al [29]. Para este estudio, se limitó la inclusión a publicaciones a partir del año 2010, considerando la constante evolución tecnológica y la importancia de la actualización de las investigaciones.

Se incluyeron publicaciones en inglés o español, ya que ambos idiomas son ampliamente reconocidos en el ámbito de la tecnología y la ciencia. Los temas abordados en los artículos se relacionaron con el impacto de las redes sociales en la privacidad de la sociedad en los medios digitales [3].

Con el fin de garantizar la selección de los estudios más pertinentes y fiables, se decidió excluir investigaciones presentadas en formato de diapositivas y ejemplares, ya que estos formatos pueden no proporcionar la certeza necesaria en cuanto a la información empleada [28]. También se consideró desechar publicaciones clasificadas como "lecturas grises", es decir, escritos que no se han divulgado adecuadamente. La aplicación de estos criterios aseguró la calidad y fiabilidad de los artículos seleccionados para esta revisión sistemática [34].

En el contexto de la privacidad en el entorno digital y la promoción de un uso seguro y responsable de las redes sociales, la protección de la privacidad en línea es un esfuerzo conjunto que requiere la colaboración de diversos actores, desde los responsables de formular políticas hasta los usuarios individuales [16]. Trabajar en conjunto para desarrollar estrategias de protección de datos, promover la concienciación sobre la seguridad cibernética y fomentar prácticas responsables en línea es fundamental para garantizar un entorno digital seguro y respetuoso de la privacidad de los usuarios [21].

TABLA 2.
 CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios de Inclusión y exclusión	
Inclusión	Exclusión
Periodo 2010 - 2023	Se excluyen documentos de áreas temáticas que no tengan relación con el título de la revisión.
Artículos	No se consideran todos los documentos
Artículos en Idioma Ingles, portugués y español	Exclusión de palabras claves que no estén en relación con el tema como a continuación detallo: derechos de los niños, menores de edad, artes, censura, derechos de autor, grandes datos, derecho parlamentario, reforma penal, piratería, censura, cyberbullig.
Palabras claves: Social networks, social media, law, privacy, legislation.	Exclusión por falta de credibilidad de la fuente; Se descartan los documentos cuya fuente o autor que no estén respaldados por instituciones o investigadores reconocidos en el campo o los registros que no abren.
Inclusión de artículos científicos con revisión de pares	Se ha excluido el tipo de documento: libro.
Inclusión de documentos en áreas temáticas pertinentes	Exclusión del área temática: Negocios y gestión y contabilidad, artes y humanidades, matemáticas, humanidades, ciencias medioambiente, medicamento, Ingeniería, enfermería, Bioquímica, genética y biología, ciencias de la decisión, física y astronomía, ciencias de los materiales, ingeniería química, ciencias agrícolas y biológicas.

Finalmente, se realizó una exhaustiva evaluación de los artículos completos identificados, no se encontró documentos duplicados. En total se revisaron 15 registros en Scopus, excluyendo 22 y 8 registros en Scielo excluyéndose 7 registros, haciendo un total de 23 registros revisados. De estos tras aplicar los criterios de elegibilidad se seleccionó 11 artículos Scopus y 6 de Scielo, luego aplicando criterios, como año de publicación, artículos relacionados, palabras claves e idiomas, quedando un total de 5 artículos de Scopus y 4 Scielo.

En los siguientes apartados, se presentan los hallazgos de la revisión sistemática, centrándose en las regulaciones legales sobre la privacidad personal en las redes sociales. Estos resultados ofrecerán una visión de las prácticas más efectivas y proponer recomendaciones claras y bien fundamentadas para los profesionales involucrados en este ámbito.

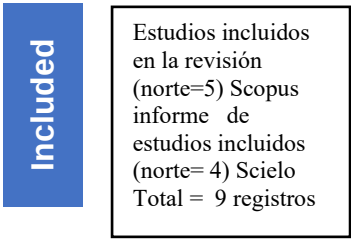
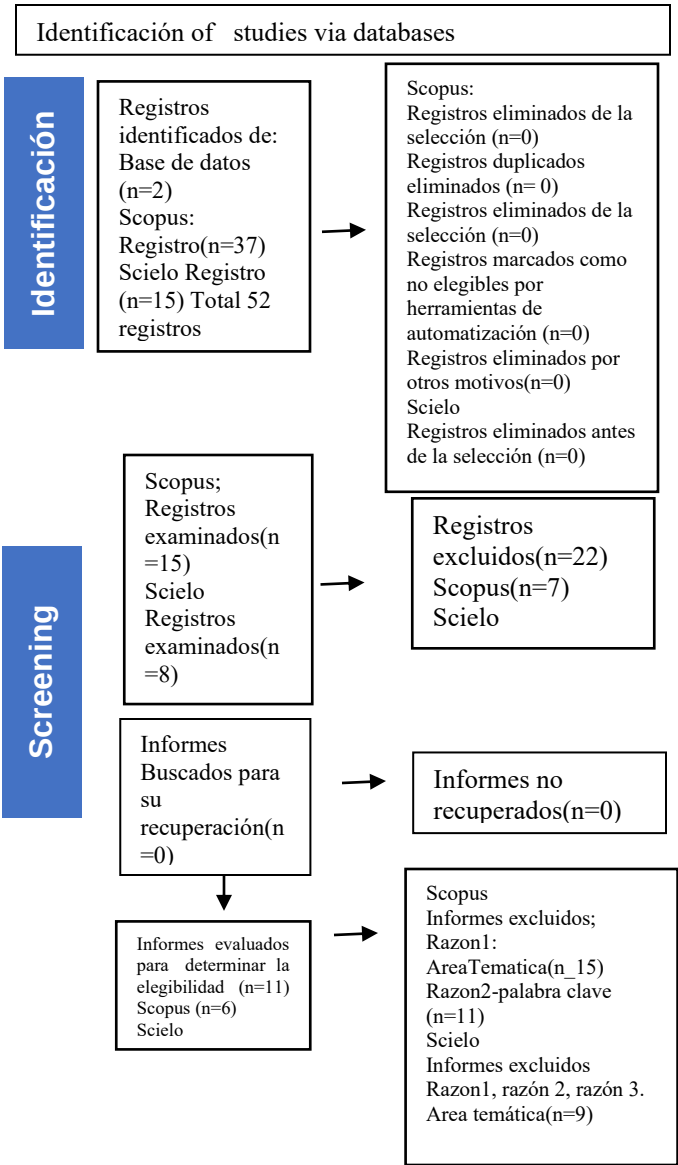


Tabla 3. Diagrama del flujo de selección (adaptación prisma)

III. RESULTADOS

AUTOR	AÑO	TITULO	DESCRIPCION
Patterson S.; McGoldrick K	2023	'Look at us ... we're walking': parental advocacy vs a child's privacy in the age of internet sharing	El contexto utilizado en este estudio es la investigación social y psicológica, se centra en crear apoyo dinámico y conexiones entre padres de niños con discapacidad a través de redes sociales y plataformas en línea así cómo afecta la autonomía y la privacidad de los niños.
Pichardo Flores L	2023	Use of social media by public education institutions: problems and legal solutions; [empleo de las redes sociodigitales por las instituciones de educación pública: problemas y soluciones jurídicas	La investigación se centra en las áreas de protección de datos personales, libertad de expresión y derechos de propiedad intelectual. Se analizan cuatro casos de diferentes instituciones educativas públicas para identificar cuestiones jurídicas comunes, tipos de conflictos de derechos que surgen en los medios digitales y delitos.
Rocha L.A.C.B.D.L .M.D.; Filpo K.P.L.	2018	Protection of right to privacy in the hyperexposition society: Paradoxes and empirical limits; [Proteção do direito à vida privada na sociedade da hiperexposição: Paradoxos e limitações empíricas]	El derecho actual a la privacidad tiene muchos matices, cada uno de los cuales ha sido desarrollado gracias a arduos esfuerzos del poder judicial para garantizar que este derecho sea ejercido por todas las personas en el mundo.
Martorell L.B.; do Nascimento W.F.; Garrafa V	2016	Social networks, privacy, confidentiality and ethics: Exhibition of pictures of patients on Facebook; [Redes sociais, privacidade, confidencialidade e ética: A exposição de imagens de pacientes no facebook]; [Redes	Este trabajo implicó examinar la exposición de los pacientes a la publicidad de Facebook por parte de médicos y dentistas. Estas imágenes pueden contener violaciones de confidencialidad y/o privacidad.



		sociales, privacidad, confidencialidad y ética: La exposición de imágenes de pacientes en el facebook]	
Garavaglia A.; Merico M.; Pandolfini V.; Pattaro C.; Setiffi F	2020	Youth and digital media: Risks and opportunities	El contexto de este estudio es investigar la relación entre la juventud y el uso de los medios digitales, estudiando sus riesgos y posibles efectos en la socialización, sociabilidad y formación de identidad de los jóvenes.
Putter, Dries, Henrico, Susan	2022	Social media intelligence: The national security-privacy nexus	Este artículo presenta SOCMINT a quienes aún no están expuestos al fenómeno y destaca el impacto que los datos, la información y el conocimiento ("contenido") de las redes sociales pueden tener en las comunidades de inteligencia y privacidad.
Moreira, Arnaldo Luis Darg, Razzolini Filho, Edelvino, Adrião, Milton Cesar	2023	Vigilância e privacidade no ambiente digital	Cuando se analiza desde un contexto social, hace un aporte significativo ya que resalta la importancia del monitoreo de la información y su aplicabilidad en la protección de datos. Los resultados iniciales incluyen 39 estudios, 18 artículos BDTD (6 resúmenes y 12 artículos), 15 artículos de Scopus y 6 artículos de Web of Science.
Mangope, Karabo, Alberts, Wim	2022	"Something old, something new" – aspects of personality rights in the united states and south africa.	Los antecedentes naturales, sociales y experimentales del estudio y aplicación del derecho personal en los Estados Unidos y Sudáfrica cubren varios aspectos importantes: El uso de plataformas de redes sociales como Twitter, Instagram y Snapchat crea oportunidades para violar los derechos de privacidad y, por lo tanto, crea desafíos legales para proteger la identidad y la privacidad en el entorno digital.
Phungula, Simphiwe P	2020	The clash between the employee's right to privacy and freedom of expression and social media misconduct: ¿what justifies employee's dismissal to be a fair dismissal?	El contenido se centra en los desafíos legales que surgen en la era de las redes sociales e Internet en cuanto a la protección de los derechos de publicidad y personalidad.

3.1. ¿Cómo define el derecho a la privacidad personal?

El derecho a la intimidad se define como la libertad y los derechos que tiene cada persona de acuerdo con sus patrones de comportamiento, hábitos o costumbres en su entorno social,

familiar o personal. Este derecho significa que nadie puede interferir en la vida privada de otros sin permiso. Además, el derecho a la privacidad incluye la capacidad de determinar en qué medida comparte pensamientos, sentimientos y hechos sobre su vida personal con otros, incluidos ciertos aspectos de su identidad personal, como su voz, imagen, edad, nacionalidad, salud, hábitos sexuales, religión, política, ideas filosóficas, situación patrimonial y financiera y otros datos estrictamente personales [1].

La privacidad se define como actividades no regulares de otros seres humanos como resultado del uso excesivo de Internet. El Estado debe ser capaz de "hacer responsables a las asociaciones de sus acciones", combinando el derecho a la privacidad y el mandato de garantizar la seguridad en la legislación (siempre basada en principios éticos, moral, cuestiones de derechos y libertades) [35].

La privacidad se entiende como un derecho legal, constitucional o fundamental, que varía en los tribunales [16].

El derecho a la privacidad es la dignidad y ética de la publicación de imágenes en relación con la bioética profesional [36].

3.2. ¿Cuáles son los dispositivos que más acceden a las redes sociales?

Los teléfonos Android de gama alta más nuevos tienen habilitado el cifrado, la mayoría de los teléfonos básicos más antiguos aún no lo tienen, lo que efectivamente amplía la brecha de cifrado entre plataformas. En este sentido, la privacidad en las plataformas muchas veces asume las características de una mercancía, la cantidad de privacidad que una persona puede obtener está relacionada con la riqueza y el estatus general, el estatus social: nunca se distribuye uniformemente entre la población [36].

Según la revisión sistemática de los siguientes autores, el acceso a los dispositivos más accesibles es el siguiente: [37], [36], [16], [29], [38]. Cinco autores mencionan el acceso a los dispositivos, mientras que cuatro no lo especifican, observando que los dispositivos con mayor mecanismo de cifrado de datos, que protege el derecho a la privacidad, son los más costosos (teléfonos inteligentes), y los dispositivos con menor cifrado de datos incluyen teléfonos móviles como Android y smartphones, marcando una brecha entre las clases sociales que dependen de los ingresos económicos. Según la visión de las empresas que fabrican estos dispositivos, esto debería ser regulado por la normativa de los estados, buscando la igualdad de las personas en el derecho a la privacidad, sin que dependa del ingreso económico para acceder a equipos con mejor protección de datos.

3.3. ¿Cuál es el tratamiento de las empresas frente al derecho a la privacidad?

El enfoque de la empresa en materia de privacidad incluye la implementación de políticas y medidas de seguridad adecuadas para proteger la información personal de los usuarios en las redes sociales y plataformas en línea. Las empresas deben cumplir con la normativa y leyes de protección de datos vigentes en cada país, asegurar la transparencia en el uso de los datos personales y obtener el consentimiento inequívoco para su tratamiento [1] [2]. Las empresas de comunicación y otras organizaciones a menudo regulan y limitan el control de los usuarios sobre su información personal en las redes sociales [22].

Algunas plataformas pueden utilizar la información personal de los usuarios y permitir que terceros accedan a esa información sin el consentimiento previo del usuario, lo que genera preocupaciones sobre la privacidad en línea [35]. Según se informa, la empresa puede utilizar la información proporcionada en el perfil de un usuario para adaptar los anuncios a los intereses del usuario. Sin embargo, esta práctica conlleva riesgos para la privacidad y el potencial de uso indebido de la información y las opiniones, lo que puede afectar tanto a celebridades como a personas comunes y corrientes [38] [37].

Facebook tiene su propia política donde contiene formularios, solicita más información, etc., manteniendo a los usuarios informados de las modificaciones de las políticas, pero no es suficiente porque estas empresas han sido declaradas responsables de violaciones de la privacidad y, por lo tanto, publicar imágenes médicas es, en cierta medida, una violación de los derechos humanos básicos [16]. Las empresas sudafricanas parecen centrarse más en proteger su reputación corporativa que en los derechos de los trabajadores, lo que puede afectar a una sociedad democrática como Sudáfrica; el uso de las redes sociales en el lugar de trabajo crea un conflicto entre el derecho a la libertad de expresión y la privacidad de los empleados [29].

Según la figura 2, se observa que el tratamiento o control de las empresas frente al derecho a la privacidad de los usuarios en las redes sociales está regulado por la protección de datos establecida por cada país, mientras que la menor regulación se encuentra en los protocolos de seguridad y confidencialidad en el acceso a las redes sociales. Aunque algunas plataformas han implementado protocolos de seguridad, ¿son realmente eficaces y eficientes las regulaciones de las propias empresas? Se ha evidenciado que estas han sido vulnerables a actos ilícitos, por lo que se debe considerar un trabajo conjunto entre empresas y el Estado a fin de establecer lineamientos que permitan garantizar la igualdad, la justicia y la lucha contra la violación del derecho a la privacidad, siendo este un tema aún sensible que afecta la dignidad de la persona [1].

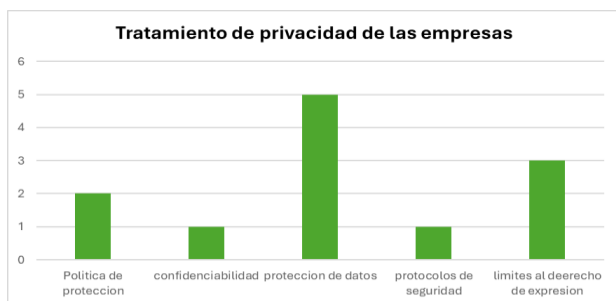


Fig. 2 Tratamiento de privacidad de las empresas

3.4. ¿Se propusieron o desarrollaron soluciones / se llegó a conclusiones?

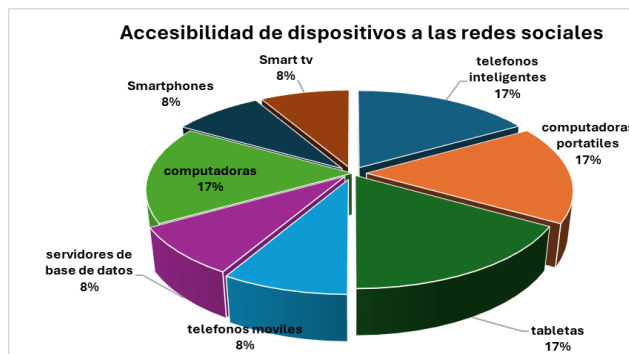


Fig. 3 Accesibilidad de dispositivos a las redes sociales

Se prioriza la protección de la información personal y la necesidad de actuar con agilidad a través de departamentos especializados en delitos informáticos para prevenir y abordar violaciones a la privacidad en línea [37], [24], [38], [35]. Uno de los mayores logros en la UE es la implementación de la Ley de Protección de Datos Directiva de 1995. Su principal objetivo es armonizar la legislación sobre privacidad en los países de la UE y garantizar leyes uniformes y unificadas al desarrollar procedimientos administrativos. El caso S. & Marper es uno de los casos de protección de datos más importantes en la UE. Este caso se refiere a la conservación legal de datos personales pertenecientes a personas físicas, como muestras de ADN y huellas dactilares [36] [39]. Una de las mejores soluciones revisadas en los documentos en la UE es la implementación de la Ley de Protección de Datos Directiva de 1995, teniendo una mejor legislación desarrollada y actualizada en los protocolos de seguridad y almacenamiento de bases de datos en protección al derecho a la privacidad personal de los usuarios en las redes sociales [1].

IV. DISCUSIÓN

El uso creciente de redes sociales ha transformado el ecosistema de la comunicación global, pero también ha incrementado la vulnerabilidad de los usuarios frente al tratamiento inadecuado de sus datos personales. A través de una revisión sistemática, se identificaron vacíos en las normativas y deficiencias en su implementación, lo que ha resultado en mayores riesgos para la privacidad digital [40] [41].

A nivel internacional, diversos instrumentos legales han servido como referencia para regular la protección de datos personales:

- Reglamento General de Protección de Datos (RGPD) de la Unión Europea (Reglamento [UE] 2016/679), que

reconoce derechos como el consentimiento informado, el derecho al olvido, la portabilidad de los datos y la limitación del tratamiento. Este reglamento ha influido en legislaciones de países de América Latina y Asia [14].

- Convenio 108 del Consejo de Europa sobre la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal, ratificado por más de 50 países, constituye el único instrumento internacional vinculante en esta materia [42].
- Directrices de la OCDE sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales, revisadas en 2013, promueven la cooperación internacional y la responsabilidad empresarial [43].
- Pacto Internacional de Derechos Civiles y Políticos (artículo 17) establece que “nadie será objeto de injerencias arbitrarias en su vida privada”, norma que ha sido interpretada como aplicable al entorno digital [44].

Se destaca la necesidad de fortalecer la protección de la privacidad en línea y de implementar medidas más efectivas para garantizar este derecho fundamental en el entorno digital [1] [45]. Se puede evidenciar en un análisis de caso que examina la eficacia de las órdenes judiciales para resguardar la privacidad de los individuos ante la divulgación de información confidencial en los medios de comunicación [26]. La sugerencia de aplicar un procedimiento uniforme en ambas cámaras del Parlamento del Reino Unido para determinar si la conducta denunciada constituye un abuso del privilegio parlamentario fue vista como una medida eficaz para prevenir el mal uso de dicho privilegio [26]. Se resaltó la importancia de evaluar el impacto de la difusión de información privada en plataformas en línea, como las redes sociales, y la necesidad de reforzar las medidas de protección de datos y privacidad en este contexto, teniendo en cuenta que las figuras públicas también tienen derecho a cautelar su privacidad, por lo que observamos que, en algunos casos, quedan desprotegidos ante las regulaciones de algunos países [26].

En el plano regional, América Latina ha mostrado avances dispares. Países como Chile con la Ley N.º 19628, Brasil con la Ley General de Protección de Datos (LGPD, Ley N.º 13.709/2018), Colombia con la Ley 1581 de 2012, Uruguay con la Ley 18.331, y Perú con la Ley N.º 29733 (Ley de Protección de Datos Personales), han adoptado marcos normativos relativamente sólidos. Sin embargo, la falta de armonización e implementación efectiva limita su impacto [46] [47].

En contraposición, países como Ecuador recién han promulgado la Ley Orgánica de Protección de Datos Personales en 2021, cuya implementación es aún incipiente [48], mientras que, en países como India, la Digital

Personal Data Protection avanza en la protección jurídica de datos, pero presenta lagunas al permitir excepciones discrecionales al Estado [49].

Otro punto crítico es la jurisdicción extraterritorial de las plataformas tecnológicas globales. Empresas como Meta (Facebook, Instagram), TikTok y Google operan bajo normativas corporativas que no siempre se alinean con las leyes nacionales, generando vacíos legales y dificultades en la exigibilidad de derechos [11]. La falta de transparencia en el uso de algoritmos y la comercialización de los datos con fines publicitarios o políticos incrementan los riesgos para la privacidad de los usuarios [50] [40].

Desde la doctrina, se ha señalado que los adolescentes y niños son el grupo más vulnerable ante la exposición no consentida de sus datos, especialmente en plataformas como TikTok, WhatsApp o YouTube [51]. En este contexto, el Reglamento Europeo exige consentimiento verificable de los padres para menores de 16 años, aunque esto no se aplica uniformemente a nivel mundial. El marco legal también requiere considerar la figura del derecho a ser olvidado, reconocido por el Tribunal de Justicia de la Unión Europea (TJUE) en el caso *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos* [52], que sienta jurisprudencia sobre la eliminación de resultados perjudiciales de motores de búsqueda, lo cual es vital para figuras públicas y usuarios comunes [14].

Se ha advertido que la autorregulación empresarial no es suficiente, por lo que es necesaria una acción conjunta entre legisladores, órganos de control, empresas tecnológicas y ciudadanos para lograr una gobernanza digital responsable [50] [11]. Las entidades regulatorias deben contar con recursos para fiscalizar, aplicar sanciones y emitir directrices técnicas claras.

La normativa de protección de datos es fundamental para garantizar la privacidad de los datos de cualquier persona física o jurídica, pública o privada. En un mundo cada vez más digital, donde se generan y comparten grandes volúmenes de información, se necesitan estándares para garantizar la seguridad de los datos y su uso adecuado [31] [35]. De hecho, estas plataformas motivan a las personas a compartir una amplia variedad de información y datos personales sin considerar las posibles repercusiones legales y sociales que esta acción de difusión podría acarrear [53], [24], [54].

La identificación de tendencias, riesgos y áreas de mejora en la protección de datos personales en línea se ha llegado a determinar que los dispositivos más usados son los androides por los bajos costos, teniendo una diferencia abismal con respecto a las clases sociales y económicas de acceso, ya que, a mayor costo del dispositivo, mayor será el cifrado de datos, perjudicando a la clase más popular [31]. Asimismo, podemos encontrar que el tratamiento de

protección de datos de la Unión Europea ha servido de ayuda e implementación para los demás países; esto va a diferenciarse por cada uno de los sistemas jurídicos de los estados [19].

En cuanto a la privacidad de los datos, la India está muy por detrás del mundo sin un marco regulatorio en esta área, lo que representa una situación preocupante que requiere el establecimiento de una estructura jurídica sólida lo antes posible. En este sentido, ciertas características de las leyes de protección de datos de otros países pueden ser emuladas. Por ejemplo, el concepto del "derecho a ser olvidado" implementado en la Unión Europea [26], lo cual brinda una segunda oportunidad de vida a los individuos. Sin embargo, esto debe complementarse con regulaciones legales y mejores políticas de las empresas en sus plataformas, considerando que el acceso se da en todas las edades. Actualmente, el tratamiento de datos es vulnerado por actos ilícitos, por lo que los estados y las empresas deberían mejorar las regulaciones para ser más seguras y hacer que las plataformas asuman mayores responsabilidades [45].

El marco legal incorporado en algunos países como Chile, Perú, Colombia, Brasil y Uruguay ha establecido leyes que garantizan la protección de los datos personales de los consumidores [2] [55]. Estas leyes hacen hincapié en la importancia del consentimiento otorgado por los titulares de los datos para su procesamiento. Por otro lado, Ecuador se encuentra entre los pocos países de América Latina que carecen de una legislación específica que regule este tema [46], lo que destaca la necesidad de implementar medidas para proteger la privacidad y seguridad de los datos personales en el país.

Hemos encontrado que Sudáfrica también tiene una escasa legislación en este ámbito [25], donde es necesario implementar regulaciones en diferentes partes del mundo, pero también fomentar la conciencia y los valores en los ciudadanos respecto a su uso. Es crucial regular el uso de datos, así como la responsabilidad de las empresas y el Estado. Una mejor coordinación permitiría una regulación más eficaz. Aún queda camino por recorrer en esta investigación para que los Estados trabajen en la sensibilización sobre el uso de datos, así como en la implementación de sanciones y penas que regulen eficazmente a empresas y usuarios.

El uso de la informática y las telecomunicaciones otorga un poder que puede comprometer la privacidad de las personas cuyos datos son procesados o transmitidos [1]. La responsabilidad primordial de mitigar los riesgos asociados recae en aquellos que generan y manejan dichos datos [2]. La autorregulación se presenta como la estrategia principal que los Estados emplean para proteger la dignidad de las personas en una sociedad donde la ciencia y la tecnología juegan un papel dominante, y donde los principales desafíos provienen de los avances en estos ámbitos [3].

Los derechos fundamentales de los ciudadanos en línea, como la privacidad, la libertad de expresión y la protección de datos personales, deben ser salvaguardados a través de marcos legales sólidos y mecanismos de cumplimiento efectivos [4]: Es fundamental que existan leyes y regulaciones claras que protejan los derechos fundamentales de los usuarios en línea, incluyendo la privacidad y la protección de datos personales [5]. Asimismo, es necesario contar con mecanismos de cumplimiento y sanciones efectivas para garantizar el respeto de estos derechos por parte de las empresas y los individuos [56].

Se pueden plantear diversas líneas de investigación que abren un abanico de exploración, como las consecuencias del exceso del uso de las redes sociales por parte de los adolescentes [35], las repercusiones de la divulgación irresponsable de información sobre la intimidad personal [22], el aislamiento en los jóvenes debido a la poca comunicación con el entorno familiar [39], o la actividad de ciberdelincuentes [40].

Se plantea una situación conflictiva entre la necesidad de intercambiar información para propósitos de investigación y la preservación de la privacidad de cada individuo [15]. En este contexto, es esencial alcanzar un punto de equilibrio que facilite la cooperación en el ámbito científico sin poner en peligro la confidencialidad de los datos personales de las personas [16], lo que conlleva a una colaboración entre diferentes actores, incluyendo gobiernos, empresas de tecnología, organizaciones de la sociedad civil y la propia comunidad [57].

Finalmente, resulta imperativo que las universidades, medios de comunicación y la sociedad civil promuevan una cultura digital de privacidad, fomentando el conocimiento sobre derechos digitales, la ciberseguridad y el uso ético de las tecnologías [58] [59].

Es esencial abordar los desafíos relacionados con la privacidad en el entorno digital y promover un uso seguro y responsable de las redes sociales [26]: La protección de la privacidad en línea es un esfuerzo conjunto que requiere la colaboración de diversos actores, desde los responsables de formular políticas hasta los usuarios individuales [21]. Trabajar en conjunto para desarrollar estrategias de protección de datos, promover la concienciación sobre la seguridad cibernética y fomentar prácticas responsables en línea es fundamental para garantizar un entorno digital seguro y respetuoso de la privacidad de los usuarios [27].

REFERENCIAS

- [1] Z. Abbas, R. Khan, M. Z. Khan, and M. Imran, "Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail Freedom of Expression and Right to Privacy," *J. Creat. Commun.*, Dec. 2023, doi:

- 10.1177/09732586231206913.
- [2] D. Álvarez, "Privacidad en línea en la jurisprudencia constitucional chilena," *Rev. Derecho Público*, vol. 89, no. 89, p. 11, Dec. 2018, doi: 10.5354/0719-5249.2018.52027.
- [3] M. Ato, J. López-García, and A. Benavente, "Un sistema de clasificación de los diseños de investigación en psicología," *An. Psicol.*, vol. 29, no. 3, pp. 1038–1059, Oct. 2013, doi: 10.6018/analesps.29.3.178511.
- [4] E. Carrillo and M. Sequera, "Personal data in the social security institute: exploratory analysis on some personal data protection practices in the social security system of the Paraguayan state," *Rev. Derecho, Estado y Telecomunicaciones*, vol. 12, no. 2, p. 14, 2020, doi: 10.26512/lstr.v12i2.34689.
- [5] I. M. Ciolan, "Defining Cybersecurity As The Security Issue of The Twenty First Century: A Constructivist Approach," *Rev. Adm. Publica si Polit. Soc.*, vol. 12, no. 1, pp. 120–136, 2014.
- [6] Parlamento Europeo y Consejo de la Unión Europea, "Reglamento (UE) 2016/679 General de Protección de Datos (RGPD)," 2016.
- [7] Gobierno de Brasil, "Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018)," 2018, *Presidência da República Federativa do Brasil*, 2018.
- [8] Congreso de Colombia, "Ley Estatutaria 1581 de 2012," 2012, *Diario Oficial, República de Colombia*.
- [9] Congreso de la República del Perú, "Ley N.º 29733, Ley de Protección de Datos Personales," 2011, *El Peruano*.
- [10] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *J. Comput. Commun.*, vol. 13, no. 1, pp. 210–230, 2007, doi: 10.1111/j.1083-6101.2007.00393.x.
- [11] D. J. Solove, *Understanding Privacy*. Harvard University Press, 2008.
- [12] A. Giddens, *Sociology*, 6th ed. Polity Press, 2009.
- [13] H. Jenkins, *Convergence Culture: Where Old and New Media Collide*. New York University Press, 2006.
- [14] G. González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, 2020.
- [15] I. Cunha, J. Cavalcante, and A. Patel, "A proposal for curriculum development of educating and training Brazilian police officers in digital forensics investigation and cybercrime prosecution," *Int. J. Electron. Secur. Digit. Forensics*, vol. 9, no. 3, pp. 209–238, 2017, doi: 10.1504/IJESDF.2017.085195.
- [16] A. Moreira, E. Razzolini, and M. Adrião, "Vigilância do fluxo informacional e privacidade no ambiente digital," *RDBCI Rev. Digit. Bibliotecon. e Ciência da Informação*, vol. 21, Aug. 2023, doi: 10.20396/rdbci.v21i00.8671505.
- [17] I. Villegas, "Comparative analysis of data protection regulations in the EU and US," 2012.
- [18] Constitución Española, "Artículo 18.1 y 18.4, 1978," 1978.
- [19] J. Delva and I. Gonzalez, "Venta sexual digital: las redes sociales y su regulación internacional," *JURÍDICAS CUC*, vol. 18, no. 1, pp. 241–278, Mar. 2022, doi: 10.17981/juridcuc.18.1.2022.11.
- [20] P. Dries and S. Henrico, "Social media intelligence: The national security-privacy nexus," *Sci. Mil. South African J. Mil. Stud.*, 2022, doi: 10.5787/50-1-1345.
- [21] G. P. Hernández-Sotomayor, R. K. Moscoso-Parra, and J. A. Álvarez-Carrión, "Protección de datos personales y derechos humanos en Ecuador: Desafíos en la era de la inteligencia artificial y la digitalización," *MQRInvestigar*, vol. 9, no. 2, p. e489, Apr. 2025, doi: 10.56048/MQR20225.9.2.2025.e489.
- [22] A. Garavaglia, M. Merico, V. Pandolfini, C. Pattaro, and F. Setiffi, "Youth and digital media: Risks and opportunities," *Rev. Technol. Digit.*, 2020.
- [23] J. Martínez, "Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento," *Rev. Española Derecho Const.*, no. 106, pp. 119–148, Apr. 2016, doi: 10.18042/cepc/redc.106.03.
- [24] M.-Á. Pertegal-Vega, A. Oliva-Delgado, and A. Rodríguez-Meirinhos, "Systematic review of the current state of research on Online Social Networks: Taxonomy on experience of use," *Comunicar*, vol. 27, no. 60, pp. 81–91, Jul. 2019, doi: 10.3916/C60-2019-08.
- [25] A. Marín-Cortés and J. Linne, "Una tipología del ciberacoso en jóvenes," *Rev. Mex. Sociol.*, vol. 83, no. 2, pp. 331–356, Mar. 2021, doi: 10.22201/iis.01882503p.2021.2.60087.
- [26] L. Rocha and K. Filpo, "Protection of right to privacy in the hyperexposition society: Paradoxes and empirical limits," 2018.
- [27] B. Guzzetti and M. Lesley, *Handbook of research on the societal impact of digital media*. IGI Global, 2015, doi: 10.4018/978-1-4666-8310-5.
- [28] S. Kemp, "Global Overview Report," 2024.
- [29] M. J. Page et al., "Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas," *Rev. Española Cardiol.*, vol. 74, no. 9, pp. 790–799, Sep. 2021, doi: 10.1016/j.recesp.2021.06.016.
- [30] C. Maguiña, R. Gastelo, and A. Tequen, "El nuevo Coronavirus y la pandemia del Covid-19," *Rev. Médica Hered.*, vol. 31, no. 2, pp. 125–131, Jul. 2020, doi: 10.20453/rmh.v31i2.3776.
- [31] G. Mascheroni and K. Ólafsson, "The mobile Internet: Access, use, opportunities and divides among European children," *New Media Soc.*, vol. 18, no. 8, pp. 1657–1679, Sep. 2016, doi: 10.1177/1461444814567986.
- [32] K. Mangope and W. Alberts, "Something el,

- something new aspects of personality rights in the United States and South Africa,” *Obiter*, vol. 43, no. 3, pp. 416–435, 2022.
- [33] C. Manterola, P. Astudillo, E. Arias, and N. Claros, “Revisones sistemáticas de la literatura. Qué se debe saber acerca de ellas,” *Cirugía Española*, vol. 91, no. 3, pp. 149–155, Mar. 2013, doi: 10.1016/j.ciresp.2011.07.009.
- [34] L. Martorell and V. Nascimento, Wanderson Garrafa, “Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no facebook,” *Interface - Comun. Saúde, Educ.*, vol. 20, no. 56, pp. 13–23, Nov. 2015, doi: 10.1590/1807-57622014.0902.
- [35] V. Monsalve, “La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos,” *Prolegómenos*, vol. 20, no. 39, pp. 163–195, Jan. 2017, doi: 10.18359/prole.2729.
- [36] G. Mushwana and H. Bezuidenhout, “Social media policy in South Africa,” *South. African J. Account. Audit. Res.*, vol. 16, no. 1, pp. 63–74, 2014.
- [37] C. Paine, D. Reips, S. Stieger, A. Joinson, and T. Buchanan, “Internet users’ perceptions of ‘privacy concerns’ and ‘privacy actions,’” *Int. J. Hum. Comput. Stud.*, vol. 65, no. 6, pp. 526–536, 2007, doi: 10.1016/j.ijhcs.2006.12.001.
- [38] S. Patterson and K. McGoldrick, “‘LOOK AT US ... WE’RE WALKING’: Parental Advocacy vs a Child’s Privacy in the age of Internet Sharing,” in *Handbook of Research on Digital Media*, 2023. doi: 10.4324/9781003056737-34.
- [39] L. Pichardo, “Empleo de las redes sociodigitales por las instituciones de educación pública: problemas y soluciones jurídicas,” *Estud. en Derecho a la Inf.*, pp. 115–149, Nov. 2022, doi: 10.22201/ijj.25940082e.2023.15.17473.
- [40] S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs, 2019.
- [41] A. Acquisti, C. R. Taylor, and L. Wagman, “The economics of privacy,” *J. Econ. Lit.*, vol. 54, no. 2, pp. 442–492, 2015, doi: 10.1257/jel.54.2.442.
- [42] Consejo de Europa, “Convenio 108+ para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales,” 2018.
- [43] OCDE, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” 2013.
- [44] Organización de las Naciones Unidas (ONU), “Pacto Internacional de Derechos Civiles y Políticos,” 1966.
- [45] S. Phungula, “The clash between the employee’s right to privacy and freedom of expression and social media misconduct: What justifies employee’s dismissal to be a fair dismissal?,” *Rev. Univ. KwaZulu Natal*, 2020.
- [46] F. Velasco and A. Miranda, “Protección de datos personales en América Latina: avances y desafíos,” *Rev. Iberoam. Derecho Digit.*, vol. 5, no. 2, pp. 45–67, 2022.
- [47] Red Iberoamericana de Protección de Datos, “Panorama legislativo de la privacidad en América Latina,” 2023.
- [48] A. Villacrés, “Implementación inicial de la Ley Orgánica de Protección de Datos Personales en Ecuador,” *Rev. Ecuatoriana Derecho y Tecnol.*, vol. 3, no. 1, pp. 22–39, 2022.
- [49] R. Sharma, “India’s Digital Personal Data Protection Act: Progress and pitfalls,” *Asian J. Law Technol.*, vol. 15, no. 1, pp. 105–124, 2023.
- [50] L. Floridi, *Ethics, governance, and policies for the digital age*. Oxford University Press, 2022.
- [51] S. Livingstone and M. Stoilova, “Children’s privacy online: Experimenting with boundaries within digital platforms,” *New Media & Soc.*, vol. 23, no. 4, pp. 789–805, 2021, doi: 10.1177/1461444820912530.
- [52] Tribunal de Justicia de la Unión Europea (TJUE), “Sentencia del caso Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos y Mario Costeja González,” 2014.
- [53] M. Soto, “El crimen on-line. Una mirada a la responsabilidad del proveedor de servicio de Internet,” *Rev. Justicia Juris*, vol. 8, no. 1, pp. 75–83, 2012, doi: 10.15665/rj.v8i1.253.
- [54] A. Roos and M. Slabbert, “Defamation on Facebook: Isparta v Richter 2013 6 SA 529 (GP),” *Potchefstroom Electron. Law J.*, vol. 17, no. 6, 2015, doi: 10.4314/pej.v17i6.18.
- [55] J. Kaye, “The Tension Between Data Sharing and the Protection of Privacy in Genomics Research,” *Annu. Rev. Genomics Hum. Genet.*, vol. 13, no. 1, pp. 415–431, Sep. 2012, doi: 10.1146/annurev-genom-082410-101454.
- [56] A. Tapajós, M. Prado, and V. Garrafa, “Tradução brasileira da Declaração Universal sobre Bioética e Direitos Humanos da Unesco,” 2005.
- [57] L. Rainie, J. Anderson, J. Albright, and H. Herzog, “The Future of Free Speech, Trolls, Anonymity and Fake News Online,” 2017.
- [58] M. Ventura and C. Coeli, “Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança,” *Cad. Saude Publica*, vol. 34, no. 7, Jul. 2018, doi: 10.1590/0102-311x00106818.
- [59] M. Ventura and C. M. Coeli, “Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança,” *Cad. Saude Publica*, vol. 34, no. 7, pp. 83–98, Jul. 2018, doi: 10.1590/0102-311x00106818.