Universidad del Azuay

Facultad de Ciencias Jurídicas

Escuela de Estudios Internacionales

LA INJERENCIA DE LA INTELIGENCIA ARTIFICIAL EN LA VIOLACIÓN A LA PRIVACIDAD EN LAS REDES SOCIALES.

Autora:

Renata Nicole Lozano Figueroa

Directora:

Dra. Ana Isabel Malo Martínez

Cuenca-Ecuador

2024

DEDICATORIA

Empiezo dedicando esto a mi familia, cuyo amor incondicional y constante apoyo han sido mi mayor inspiración y fortaleza a lo largo de mi camino. A mi madre, quien me ha inculcado los valores de dedicación, fe inquebrantable, amor genuino y valentía. Su presencia constante a mi lado y enseñanzas me han moldeado en la mujer que soy hoy en día. Y a mi padre, cuya perseverancia y arduo trabajo han sido una luz guía en el logro de mis metas. El esfuerzo de mis padres ha sido una inspiración para mí, y agradezco profundamente el apoyo incondicional y el sacrificio que han hecho para hacer posible mis estudios. A mis hermanos, cuya compañía ha enriquecido mi vida con alegría y recuerdos hermosos, estoy agradecida por la bendición de haber crecido con ellos. A mis abuelos, quienes han iluminado mi camino con su sabiduría. Especialmente a mi Papito Julio quien ahora descansa en paz, pero siempre presente en mi corazón, espero haberlo hecho sentir orgulloso. A mis mejores amigos, ya sea cerca o lejos, ofreciendo su cariño y aliento en las buenas y malas, convirtiendo las amistades en familia. A todos aquellos que de una forma u otra han contribuido a mi formación académica y personal, les dedico este logro con profunda gratitud y afecto.

AGRADECIMIENTOS

Quisiera expresar mi más sincero agradecimiento a todas las personas que han hecho posible la culminación de este proyecto académico.

En primer lugar, agradezco profundamente el apoyo brindado por mis padres y mis hermanos, quienes han sido mi mayor fuente de fortaleza y aliento a lo largo de mi vida. Gracias a su amor incondicional y su sacrificio, he encontrado la determinación y la perseverancia necesarias para alcanzar mis metas.

Deseo expresar mi profundo agradecimiento a una persona que ha desempeñado un papel crucial en este proceso. A mi directora de tesis, la Dra. Ana Isabel Malo, por su guía y constante apoyo durante todo el proceso de investigación. Sus conocimientos compartidos han sido fundamentales para la orientación de este trabajo y para mi crecimiento como estudiante. La Dra. ha sido una de las mayores influencias que han fortalecido mi aprecio por esta carrera, especialmente en el ámbito de los derechos humanos. Le tengo un aprecio y respeto realmente grande.

Agradezco a mi profesora, Melita Vega, quien ha dejado una marca indeleble en mi trayectoria académica. No solo proporcionó una orientación clara y valiosos insights sobre el proceso de investigación, sino que también posee cualidades que admiro profundamente como mujer — bien preparada y respetada por sus firmes convicciones. Bajo su mentoría, he aprendido lecciones invaluables sobre la preparación y comunicación efectiva en el ámbito académico.

Quiero extender mi reconocimiento al cuerpo docente de la Escuela de Estudios Internacionales de la Universidad del Azuay, cuyo compromiso con la excelencia académica ha sido importante en formar estudiantes dedicados y exitosos.

Finalmente, quiero expresar mi gratitud a todos aquellos que, de una u otra manera, han contribuido a la realización de este trabajo. Su colaboración y su apoyo han dejado una huella imborrable en mi camino hacia la consecución de mis metas académicas y profesionales.

INDICE DE CONTENIDO

INDICE DE TABLAS Y ANEXOS

Índice de tablas

Índice de anexos

LA INJERENCIA DE LA INTELIGENCIA ARTIFICIAL EN LA VIOLACIÓN A LA PRIVACIDAD EN LAS REDES SOCIALES

Resumen

La presente investigación aborda la creciente preocupación sobre la injerencia de la inteligencia artificial (IA) en la violación de la privacidad en las redes sociales. Se examina cómo la IA impacta los derechos individuales desde una perspectiva de derechos humanos, ética informática y lineamientos por las regulaciones de las redes sociales. Se analizan los desafíos éticos, legales y sociales, así como las medidas regulatorias existentes, incluido el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. La metodología empleada es una revisión sistemática de la literatura. Se observa que la utilización de la IA plantea nuevos desafíos para la privacidad individual y puede afectar directamente a los derechos humanos.

Palabras clave: Derechos Humanos, Ética Informática, Inteligencia Artificial, Privacidad, Redes Sociales

THE INTERFERENCE OF ARTIFICIAL INTELLIGENCE IN THE VIOLATION OF PRIVACY IN SOCIAL NETWORKS

Abstract

This research addresses the growing concern about the interference of artificial intelligence (AI) in privacy violation on social media platforms. It examines how AI impacts individual rights from the perspective of human rights, computer ethics, and social media guidelines. The ethical, legal, and social challenges are analyzed, along with existing regulatory measures, including the General Data Protection Regulation (GDPR) of the European Union. The methodology employed is a systematic literature review. It is observed that the application of AI poses new challenges to individual privacy and directly impact human rights.

Keywords: Artificial Intelligence, Computer Ethics, Human Rights, Privacy, Social Networks

LA INJERENCIA DE LA INTELIGENCIA ARTIFICIAL EN LA VIOLACIÓN A LA PRIVACIDAD EN LAS REDES SOCIALES.

1. Introducción

El presente trabajo se adentra en este campo de estudio crucial, donde convergen la innovación tecnológica y las preocupaciones éticas. La privacidad, entendida como un derecho fundamental consagrado en documentos internacionales como la Declaración Universal de Derechos Humanos de 1948, se ve amenazada por el creciente poder que tiene la Inteligencia Artificial (IA) en el ámbito de las redes sociales. Esta investigación se propone a explorar las interacciones entre la IA y la privacidad, con un enfoque centrado en los derechos humanos y la ética informática.

En este contexto, es fundamental comprender cómo la IA, a través de algoritmos sofisticados y el análisis masivo de datos, impacta la forma en que las personas interactúan en las redes sociales y cómo se ven comprometidos sus derechos fundamentales. Según Bernal (2023), la capacidad de la IA para recopilar, analizar y utilizar datos personales para reproducir patrones, el cual, para este autor plantea serias preocupaciones sobre la autonomía individual, la discriminación algorítmica y la vigilancia masiva, entre otros aspectos.

Además, es importante considerar el marco regulatorio actual y su capacidad para abordar los desafíos emergentes relacionados con la IA y la privacidad en las redes sociales. Normativas como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea representan un intento significativo de proteger la privacidad en la era digital, pero aún enfrentan retos en su implementación y aplicación efectiva.

En última instancia, esta investigación busca explorar las implicaciones éticas y sociales de la interacción entre la IA, las redes sociales y la privacidad individual. El objetivo es compartir hallazgos relevantes a partir de la revisión bibliográfica, para informar y orientar la toma de decisiones en los ámbitos legislativo, empresarial y académico. Se espera que este análisis promueva un uso ético y responsable de la tecnología en beneficio de la sociedad en su conjunto.

1.1.Objetivos

Objetivo General

Analizar la influencia de la inteligencia artificial en las redes sociales y su afección a los derechos individuales, desde una perspectiva de derechos humanos, bajo los aspectos éticos, sociales y legales, a través de base de datos.

Objetivos Específicos

1. Analizar las consecuencias de utilización de las redes sociales y la IA en la privacidad de personas.
2. Delimitar las características de los datos usados por la IA y su relación con las redes sociales.
3. Identificar algunos aspectos sociales, legales y éticos de la relación entre inteligencia artificial y redes sociales.

Propósito del estudio

El propósito del estudio es llevar a cabo una revisión sistemática de literatura con el objetivo de analizar la influencia de la IA. Para ello, se utilizaron las bases de datos y fuentes de Web of Science y Scopus. Este análisis se enfocará en responder a la siguiente pregunta de investigación: ¿Cómo la inteligencia artificial viola el derecho a la privacidad en las redes sociales? Junto con tres sub-preguntas:

¿Qué técnicas emplea la inteligencia artificial para recolectar y analizar datos personales en las redes sociales?

¿Cómo contribuyen estas técnicas a violaciones de privacidad como la creación de identidades falsas y hackeos?

¿Cuáles son las medidas regulatorias vigentes destinadas a proteger la privacidad de los usuarios frente a estas tecnologías?

1.2.Marco teórico

El marco teórico de esta investigación proporciona un contexto conceptual para abordar la interacción entre la inteligencia artificial (IA), la privacidad del individuo y las redes sociales. Para comprender plenamente los desafíos y las implicaciones que plantea la intersección de estos campos, es crucial establecer un conjunto de definiciones y conceptos fundamentales. En este contexto, se exploran conceptos fundamentales que incluyen la IA, la privacidad del individuo, las redes sociales, los derechos humanos, la ética informática y el big data. Estos elementos son esenciales para comprender los desafíos éticos, sociales y legales que surgen de la creciente influencia de la IA en la violación de la privacidad en las redes sociales. Este marco teórico establece las bases conceptuales necesarias para analizar de manera integral las implicaciones de la IA en la privacidad del individuo en el entorno digital contemporáneo.

Propósito del estudio

La primera mención a la Inteligencia Artificial (IA) fue dada por John McCarthy et al. (1956), quien expresó la necesidad de generar máquinas que sean capaces de pensar como seres humanos. Es así que Vincent C. Müller (2020), sostiene que el avance de la inteligencia artificial es inevitable y tendrá un impacto transformador en la sociedad, aunque enfrentará numerosos desafíos éticos y sociales en su implementación. Por otra parte, la IA se enfrenta a desafíos significativos, como señala Leach (2022), quien destaca que uno de los mayores retos radica en la necesidad de comprender y responder a las emociones humanas. Esto implica que la IA no debería depender exclusivamente de aspectos matemáticos y racionales en su funcionamiento. Es por este motivo que Bossmann (2016), establece la amoralidad de la IA como la incapacidad de distinguir entre el bien y el mal, dejando esta visión a la naturaleza del usuario de la IA. Además, el aprendizaje automático de la IA, como lo describen autores como Samuel (1959), permite que las máquinas mejoren progresivamente a través de instrucciones proporcionadas por los usuarios o de sus propias actividades. Esta capacidad de aprendizaje automático genera preocupaciones en cuanto a las implicaciones éticas de la IA y la privacidad de los individuos, destacadas por Floridi (2023), quien establece como principal preocupación la sustitución progresiva de la mano de obra humana por IA.

Un aspecto que debe ser analizado al hablar del aprendizaje son las redes neuronales artificiales (ANN siglas en inglés de Artificial Neural Networks) constituyen una pieza fundamental en el aprendizaje de la inteligencia artificial (IA). Según lo descrito por Salas (2000), estas redes poseen la capacidad de aprender de acuerdo a patrones de entrenamiento, lo que implica la habilidad de encontrar modelos que se ajusten a los datos proporcionados. En esencia, las ANN funcionan de manera análoga al proceso de aprendizaje humano, absorbiendo información a través de datos de entrada para mejorar su desempeño y tomar decisiones más precisas en el futuro. Sin embargo, es crucial reconocer que las ANN son herramientas cuyo aprendizaje se basa en las instrucciones y los datos proporcionados por sus creadores y usuarios, lo que plantea importantes implicaciones éticas y sociales en cuanto a responsabilidad, privacidad y equidad en su implementación y uso.

Privacidad del individuo

Para comprender el concepto de privacidad del individuo, es fundamental tener claro qué se entiende por individuo en diferentes contextos filosóficos y jurídicos. Según Nietzsche, como se cita en Wright et al. (1984), el individuo es aquel que persigue su realización a través de su propia voluntad, siendo un ser fuerte e independiente que vive su vida auténtica. Por otro lado, Bizberg (1989), lo describe como un ser moderno que establece ciertas reglas de comportamiento para convivir en sociedad. Desde una perspectiva aristotélica, el individuo es un "zoon politikon", es decir, un ser social cuyo fin se encuentra en la comunidad política, como sugiere (Gintis et al., 2015).

La privacidad del individuo, en el contexto del marco legal ecuatoriano, se erige como un derecho fundamental que abarca diversos aspectos de la vida personal y familiar. Si bien el Código Civil (2005), no ofrece una definición explícita de la privacidad, el Artículo 66 de dicho código constituye una piedra angular en la protección de este derecho. Este artículo establece el derecho a la integridad personal, que trasciende más allá de la mera protección física del individuo, extendiéndose a la salvaguarda de su esfera privada contra intrusiones no deseadas. En este sentido, la privacidad del individuo, según el Código Civil ecuatoriano, se encuentra intrínsecamente ligada al resguardo de su integridad personal y reputación. Esta protección no solo defiende al individuo de intrusiones indebidas, sino que también promueve su pleno desarrollo y dignidad dentro de la sociedad (Código Civil, 2005).

En el ámbito jurídico, las concepciones sobre la naturaleza del individuo han evolucionado a lo largo del tiempo, reflejando tanto los contextos históricos como las preocupaciones contemporáneas. Locke (1690), en su obra clásica "Segundo tratado sobre el gobierno civil", delineó una visión fundamental que ha resonado en el pensamiento político y jurídico hasta nuestros días. Locke argumentaba que el individuo, por el simple hecho de ser humano, posee derechos inalienables, como la vida, la libertad y la propiedad, los cuales deben ser protegidos por el gobierno. Esta concepción estableció las bases para el concepto moderno de derechos humanos, enfatizando la autonomía y la dignidad de cada individuo.

Por otro lado, en un contexto más contemporáneo, Catalini (1944), ofrece una perspectiva innovadora sobre la naturaleza del individuo desde el punto de vista jurídico. Catalini argumenta que el individuo no puede entenderse de manera aislada, sino que su identidad y sus derechos se configuran en relación con el ordenamiento jurídico y la comunidad en la que se encuentra inmerso. Desde esta óptica, la interpretación del derecho se convierte en un proceso dialéctico, donde las normas jurídicas y la realidad social se entrelazan en un constante diálogo, reflejando así la complejidad y la dinámica de la vida jurídica.

Además, la teoría del derecho como integridad, propuesta por Dworkin (1986), ofrece otra perspectiva relevante sobre la naturaleza del individuo en el ámbito jurídico. Según Dworkin, en su obra "Justicia para erizos", argumenta que el derecho debe basarse en principios morales que respeten la dignidad y la autonomía de cada individuo. Desde esta visión, el sistema jurídico no solo busca resolver conflictos, sino también promover la justicia y el respeto por los derechos fundamentales de las personas, reconociendo así la importancia de la integridad y la coherencia en la interpretación y aplicación del derecho.

A pesar de las diferencias en los enfoques y contextos históricos de Locke, Cossio y Dworkin, todos convergen en una idea fundamental, el individuo es el centro del derecho y posee derechos inherentes que deben ser respetados y protegidos por el sistema jurídico para garantizar una sociedad justa y equitativa. Esta convergencia refleja la relevancia continua de las reflexiones sobre la naturaleza del individuo en el ámbito jurídico y subraya la importancia de abordar estas cuestiones de manera integral y reflexiva en la teoría y la práctica del derecho.

Redes Sociales

Aunque las redes sociales tienen sus raíces en la década de 1950, fue en 1968 cuando Licklider y Taylor vislumbraron un futuro en el que las computadoras se convertirían en entornos sociales para los seres humanos, facilitando la comunicación entre ellos (Licklider & Taylor, R.W, 1968). Sin embargo, esta promesa de conexión y comunicación también ha traído consigo preocupaciones significativas sobre la privacidad (Roig, 2009).

Boyd & Ellison (2007), definen las redes sociales como espacios donde los individuos pueden crear perfiles públicos en un entorno de interacción digital. En este contexto, los usuarios tienen la capacidad de controlar la cantidad de información que comparten y regular quiénes tienen acceso a ella. Es decir, las redes sociales según Flores et al. (2007), no solo son plataformas de comunicación, sino que también constituyen una estructura social en la que los individuos interactúan y construyen relaciones.

Sin embargo, esta interacción en las redes sociales no está exenta de implicaciones éticas y prácticas. La exposición pública en línea puede llevar a vulnerabilidades y riesgos para la privacidad personal, como el robo de identidad, el acoso en línea y la manipulación de datos por parte de empresas y gobiernos (Álvarez Caro & Piñar Mañas, 2015). Por lo tanto, es fundamental abordar estas preocupaciones y establecer políticas y prácticas que protejan adecuadamente la privacidad de los individuos en el entorno digital de las redes sociales.

Derechos humanos

Los derechos humanos, según la filosofía de Immanuel Kant como menciona Gruyter (2022), representan imperativos categóricos que deben ser respetados universalmente debido a la dignidad inherente de cada individuo. Bobbio (1951), por otro lado, argumenta que los derechos humanos son derechos subjetivos, es decir, prerrogativas que tienen las personas frente a los poderes públicos y que deben ser garantizadas por el Estado. Estas perspectivas filosóficas destacan la importancia de los derechos humanos como fundamentos para la justicia y la igualdad en la sociedad

A nivel internacional, la Organización de las Naciones Unidas (ONU) es la institución clave en la protección y promoción de los derechos humanos. La ONU a través de la Declaración Universal de Derechos Humanos, estableció un marco normativo global que reconoce los derechos de todos los seres humanos, independientemente de su origen o situación (United Nations, 1948). Por su parte, el Consejo de Europa (2024), mediante la Convención Europea de Derechos Humanos de 1950, busca proteger los derechos humanos en el contexto europeo, estableciendo un sistema de protección jurídica a nivel regional.

En el ámbito regional americano, es relevante mencionar la Declaración de los Derechos y Deberes del Hombre aprobada en Bogotá en 1948, la cual precede a la Convención Europea y establece un marco normativo para la protección de los derechos humanos en América. Adoptada por la novena Conferencia Internacional Americana, esta declaración enfatiza la importancia de salvaguardar los derechos fundamentales de todas las personas en el continente americano, reconociendo su dignidad inherente y su derecho a la libertad, la igualdad y la justicia. Al destacar esta declaración, se resalta la relevancia histórica y la influencia de los principios de los derechos humanos en América, complementando así el marco internacional establecido por la Declaración Universal de Derechos Humanos de las Naciones Unidas.

La conexión entre los derechos humanos y la privacidad del individuo es evidente en el reconocimiento de la privacidad como un derecho humano fundamental. La Declaración Universal de Derechos Humanos establece que "nadie será objeto de injerencias arbitrarias en su vida privada" (United Nations, 1948). Este reconocimiento refleja la importancia de proteger la privacidad personal como parte integral de la dignidad humana y la libertad individual, subrayando así la interrelación entre los derechos humanos y la protección de la esfera íntima del individuo.

1.2.1. Ética informática y consentimiento informado

Para García Carrasco (1994), la ética informática es un conjunto de normas y principios que deben ser respetados por los profesionales de esta área. Esta nueva ética, que pretende rescatar los valores en el uso de la tecnología y sus efectos en los individuos, también representa un proceso evolutivo en el desarrollo de la ética informática, que ha pasado desde una ética tradicional hasta una ética adaptada a la realidad digital en la que vivimos hoy en día (Silva & Espina, 2011). Rodríguez et al. (2000), también alude a la necesidad de desarrollar una ética específica en el ámbito de la privacidad para prevenir delitos que comprometan la privacidad de las personas. Por otra parte, se puede entender a la ética de la informática como argumenta Guibert Ucín (1998), es el análisis de impacto social que tiene la tecnología y la justificación del uso de la información que puede ser obtenida por esta.

Junto a la ética informática tenemos al consentimiento informado, que se convierte en un pilar ético para proteger la autonomía y la integridad del individuo. Beauchamp & Childress (2009), destacan que el consentimiento informado implica que los individuos deben tener una comprensión completa y clara de cómo se utilizará su información en las redes sociales, así como los riesgos asociados, antes de otorgar su consentimiento. Esto se alinea con los principios de la Declaración de Helsinki de la Asociación Médica Mundial, que establece la prioridad del interés individual sobre el interés de la sociedad o la ciencia en cualquier investigación o práctica médica (Montori et al., 2013). Por ejemplo, el Dr. Ezekiel Emanuel (2014), un reconocido bioeticista a nivel internacional y autor del libro "Reinventing American Health Care", enfatiza la importancia de respetar el consentimiento informado de los pacientes en todas las intervenciones médicas. Trabajando en el Hospital General de la Ciudad de Filadelfia, Emanuel aborda temas relacionados con la ética médica y la política de salud, promoviendo la comprensión y el respeto de los derechos de los pacientes en consonancia con los principios de la Declaración de Helsinki (Emanuel, 2014). En el contexto de las redes sociales, donde la privacidad del individuo puede verse comprometida por la recopilación y el uso de datos personales, el consentimiento informado emerge como una salvaguarda esencial para proteger los derechos y la dignidad de los usuarios.

1.2.2. Big Data

Originalmente usado para referirse a las ciencias como la astronomía o genética, en el 2000 se acuñó el término big data como el conjunto masivo de datos, que hoy en día se ha trasladado a todas las áreas humanas (Cukier, 2017). Al hablar de big data, es importante comprender también el concepto de open data, definido por la Open Knowledge Foundation (OKF, 2016) también conocida como Fundación para el Conocimiento Abierto, que define todos los datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona. Estos dos términos van de la mano, pues tener una big data que a su vez sea open, permite a cualquier persona acceder a grandes cantidades de información (Ferrer Sapena & Sánchez Pérez, 2013). Para Gil (2016), big data se refiere a cantidades gigantescas de información que es controlada y filtrada por el uso de algoritmos, generalmente usada por compañías y gobiernos. Otro factor es la cantidad de información digitalizada en la actualidad, pues tan solo hace dos décadas atrás menos del 25% de la información se encontraba digitalizada, hoy en día más del 98% de la información es digital (Mayor-Schonberger & Cukier, 1981).

1.3. Estado del Arte

1.3.1 Inteligencia Artificial y Redes Sociales: Transformación del Entorno Digital

Según Bowser et al. (2017), la IA ha dado un paso agigantado para el análisis de datos y la sociedad. Sin embargo, también se enfrenta a desafíos como la discriminación algorítmica o el atentado contra la privacidad de las personas. La discriminación algorítmica como señala Castillo Parrilla (2023), se refiere al fenómeno en el que los algoritmos de inteligencia artificial perpetúan sesgos existentes en los datos de entrenamiento o en el proceso de toma de decisiones, lo que puede resultar en decisiones injustas o discriminatorias hacia ciertos grupos. Este problema plantea desafíos éticos y sociales significativos, ya que puede tener impactos negativos en áreas como el empleo, la justicia y la atención médica (Carlos et al., 2023). En el análisis de Obermeyer et al. (2019), se requiere una atención cuidadosa en el diseño y regulación de los sistemas de inteligencia artificial para abordar este problema y garantizar la equidad y la justicia. El uso de algoritmos avanzados en estos sistemas ha llevado a una recopilación masiva de datos de usuarios, desencadenando preocupaciones significativas en torno a la privacidad en línea, tales como la filtración de información o el mal uso de la misma (Obermeyer et al., 2019).

El acceso de la IA a los datos de las redes sociales no está sujeto a limitaciones significativas. Esta omnipresencia plantea desafíos adicionales para la protección de la privacidad de los usuarios, es por ello que organizaciones como la Unión Europea (UE) han presentado propuesta de regulación, sin embargo, como destaca Suárez Xavier (2022), no existe un marco jurídico especifico En consecuencia, se produce una limitación de los derechos de privacidad de los individuos, en lo que a redes sociales e IA se refiere.

En relación con las redes sociales, es importante mantener una perspectiva equilibrada debido a los riesgos potenciales que representan para la privacidad individual. Según Morozov (2011), las redes sociales pueden interpretarse como espacios donde se recopila información de individuos que, de alguna manera, han decidido compartir públicamente parte de su vida privada.

Como señalan Van Dijck & Poell (2013), el entorno digital de las redes sociales está moldeado por algoritmos invisibles para el usuario común, los cuales determinan qué contenido se muestra y cómo se distribuye. Sin embargo, la aplicación de estos algoritmos puede ser percibida como intrusiva, ya que influyen en la experiencia del usuario de manera significativa, a menudo sin su pleno conocimiento y pasando por alto el consentimiento informado. Como resultado, la privacidad en las redes sociales se ha convertido en un aspecto regulado no solo por las preferencias individuales, sino también por las decisiones algorítmicas de las plataformas.

Esta interacción entre la IA y las redes sociales no solo tiene implicaciones para la privacidad de los usuarios, sino que también plantea cuestiones sobre la equidad, la transparencia y la responsabilidad en el diseño, la implementación de algoritmos y el manejo de derechos de privacidad. Por lo tanto, Kubler (2016), argumenta que es imperativo abordar estos desafíos de manera integral para garantizar que la evolución de la IA en las redes sociales beneficie a todos los usuarios y respete sus derechos fundamentales en el entorno digital en constante cambia. Además, Chander (2017), señala que los algoritmos pueden ser discriminatorios y sesgados de manera no intencional, debido a la información obtenida de internet. Este aspecto plantea un nuevo desafío en relación con la regulación y la ética de la IA.

Con el crecimiento y la popularidad de las redes sociales, McNamee (2019), destaca la creciente preocupación por el acceso a información personal que estas plataformas poseen, así como por la propagación de información falsa y el acceso a datos privados. De acuerdo a Magaret Hu (2020), la información pública en redes sociales puede ser utilizada para alimentar algoritmos que invaden nuestra privacidad. Como, por ejemplo, la empresa Cambridge Analytica utilizó una aplicación de Facebook llamada "This Is Your Digital Life" para recopilar información personal de millones de usuarios sin su consentimiento (Amnesty International, 2019). Tal como señala Keltner et al. (2014), estos datos se utilizaron posteriormente para desarrollar perfiles psicológicos de los usuarios y para dirigirles anuncios políticos personalizados. Este escándalo alcanzó su punto culminante cuando se reveló que estos datos fueron empleados para influir en votantes indecisos durante las elecciones presidenciales en Estados Unidos, potencialmente afectando los resultados electorales.

1.3.2 Un punto de inflexión en la Privacidad Digital: El Escándalo de Cambridge Analityca

El escándalo de Cambridge Analytica, ocurrido en 2018, marcó un punto de inflexión significativo en la percepción pública global sobre la privacidad digital, resaltando las complejas interacciones entre la inteligencia artificial y la protección de datos personales en las plataformas de redes sociales. Este incidente expuso cómo se pueden manipular grandes volúmenes de información personal sin el consentimiento

explícito de los usuarios, desencadenando un debate crítico sobre la privacidad digital y los principios éticos que deben regir la inteligencia artificial (Vera, 2019).

Antes de este escándalo, la privacidad era frecuentemente percibida como un simple intercambio comercial: los usuarios proporcionaban su información personal a cambio de acceder a servicios digitales personalizados sin costo. Sin embargo, la revelación de las prácticas de vigilancia económica por parte de entidades como Cambridge Analytica y Facebook alteró esta percepción. De acuerdo con Afriat et al. (2020), después del escándalo, se notó un cambio en la actitud de los usuarios, quienes empezaron a cuestionar la idea de la privacidad como un derecho condicional y comenzaron a aceptar la vigilancia económica como un aspecto inevitable del mundo digital. Este cambio subraya la manera en que los escándalos de privacidad pueden modificar la percepción pública y promover un diálogo crítico sobre las normas y prácticas en el manejo de datos personales.

El análisis de la relación entre Facebook y Cambridge Analytica reveló cómo la transferencia de información personal se ha convertido en un modelo de negocio estructurado, implicando un extenso ecosistema de proveedores y consumidores de datos. Cruz & Dias (2022), destacan que este modelo de negocio requiere una reconsideración urgente de las estrategias de protección de datos y propone la implementación de un conjunto integral de recomendaciones sobre la protección de datos para mitigar futuros riesgos.

Además, Wagner (2021), examina cómo la brecha de datos de Cambridge Analytica no solo evidenció la capacidad de influencia política global mediante el uso indebido de la información personal, sino que también planteó interrogantes fundamentales sobre los principios éticos y la responsabilidad en la gestión de datos personales. Este caso enfatiza la necesidad de regulaciones más estrictas y transparentes en el uso de inteligencia artificial y la gestión de datos personales, demostrando cómo la tecnología puede transformar radicalmente el entorno digital y afectar profundamente tanto la privacidad individual como colectiva. Este análisis destaca la importancia de una regulación más rigurosa y transparente en el uso de la IA y la gestión de datos personales en las redes sociales, mostrando cómo la tecnología puede transformar el entorno digital y afectar profundamente a la privacidad individual y colectiva.

1.3.3. Planteamiento de las reglas y condiciones de aceptación de términos de las plataformas más usadas

Los términos y condiciones son documentos legales fundamentales que establecen la relación entre las compañías de redes sociales y sus usuarios. Estos documentos, que surgieron en respuesta a las necesidades legislativas de protección de datos, detallan los derechos y obligaciones de ambas partes. La implementación formal de los términos y condiciones en las plataformas digitales empezó a tomar forma con la evolución de Internet y las primeras regulaciones de privacidad digital en las últimas décadas del siglo XX.

La Directiva de Protección de Datos de la UE en 1995 (European Union, 1995) y la Ley de Protección de la Privacidad Online de los Niños (COPPA) en 1998 en los Estados Unidos (Unied States, 1998) fueron pioneras en exigir a las plataformas obtener consentimiento explícito de los usuarios para el procesamiento de sus datos. Estos desarrollos normativos impulsaron la creación de los primeros términos y condiciones en plataformas emergentes en ese entonces.

Con la llegada de plataformas como Facebook (2004), Twitter (2006), Instagram (2010) y TikTok (2016), se establecieron términos y condiciones adaptados no solo a las leyes de protección de datos sino también a las necesidades comerciales y tecnológicas de cada plataforma. Estos términos y condiciones fueron diseñados para facilitar el uso extensivo de datos en estrategias de marketing y personalización de contenido, impulsado significativamente por avances en inteligencia artificial (IA). La IA ha permitido a estas plataformas optimizar la experiencia del usuario y dirigir con precisión el contenido y la publicidad, aumentando así su rentabilidad y funcionalidad.

Sin embargo, la complejidad y longitud de estos documentos han planteado cuestionamientos éticos y legales, especialmente en cuanto a su comprensibilidad y la verdadera voluntariedad del consentimiento. Según Schneble et al. (2021), los procesos de consentimiento en muchas plataformas no se toman con la seriedad que requieren, con términos y condiciones que a menudo son extensos y difíciles de entender, lo que plantea un desafío significativo en términos de ética y transparencia.

Además, la evolución continua de las políticas de privacidad y los términos de servicio refleja la necesidad de adaptarse a un entorno digital en constante cambio, donde la IA juega un papel cada vez más central. La transparencia y equidad en el uso de la IA son cruciales para mantener la confianza de los usuarios y asegurar el cumplimiento de los estándares éticos y legales en la gestión de datos personales.

1.3.4 Cambios de los términos de aceptación y cómo afectan la privacidad del usuario

Los términos y condiciones son esenciales para el funcionamiento de plataformas como Facebook, Instagram, Twitter y TikTok, desempeñando un papel crucial en el control de la privacidad del usuario. Originalmente claros y directos, estos términos han evolucionado significativamente, adaptándose a las nuevas tecnologías y prácticas, en particular con la introducción de la inteligencia artificial. Aceptar estos términos significa dar permiso a las plataformas para acceder y manejar una variedad de datos personales. A continuación, se detallan los permisos y accesos específicos que se otorgan al aceptar los términos y condiciones de cada una de estas plataformas:

Fundada en 2004, Facebook ha ajustado sus términos de servicio en respuesta a su expansión y a la integración de nuevas tecnologías. Facebook recopila información que se proporciona directamente, como nombre, dirección de correo electrónico, y contenido que se publica, así como información sobre las interacciones, ubicaciones y dispositivos utilizados. Además, la plataforma utiliza IA para personalizar anuncios y contenido, basándose los intereses y actividades. Facebook puede compartir los datos con terceros, incluyendo empresas que forman parte del grupo Meta, anunciantes y otros socios comerciales (Platforms, 2023). También utiliza cookies y tecnologías similares para rastrear el comportamiento dentro y fuera de la plataforma (Facebook, 2023). Un claro ejemplo es el escándalo de Cambridge Analytica que se mencionó como el punto de inflexión. Este caso reveló cómo Facebook permitió a esta consultora acceder a datos personales de millones de usuarios sin su consentimiento explícito. Estos datos fueron utilizados para influir en las elecciones presidenciales de Estados Unidos de 2016 mediante la creación de perfiles psicológicos y la orientación de anuncios políticos específicos (Amnesty International, 2019).

Instagram, adquirida por Facebook en 2012, inicialmente no poseía la complejidad de análisis de datos de su empresa matriz. Sin embargo, después de la adquisición, los términos de servicio de Instagram se expandieron para permitir un análisis más profundo de imágenes y videos. Instagram recopila y analiza las fotos y videos que se suben, así como los datos de las interacciones (me gusta, comentarios). Puede acceder a la ubicación, tanto precisa como imprecisa, para personalizar el contenido. Además, comparte datos con empresas del grupo Meta y otros terceros para mejorar la publicidad y servicios. Recopila datos de los dispositivos, como direcciones IP, tipo de navegador y sistema operativo (Instagram, 2023). Instagram ha sido criticado por su algoritmo de exploración, que promueve contenido basado en los intereses percibidos de los usuarios. Esto ha llevado a problemas como la promoción de contenido que puede afectar negativamente la salud mental de los adolescentes, exponiéndolos a estándares de belleza poco realistas y contenido que fomenta la comparación social (Pew Research Center, 2021).

Twitter, ahora conocida como (X), fue lanzado en 2006. Esta red social ha visto cambios significativos en sus términos de servicio, especialmente en cómo gestiona y utiliza datos en tiempo real para personalizar y moderar contenido. Twitter recopila datos en tiempo real sobre los tweets, retweets, me gusta y otros tipos de interacción. Utiliza los datos para personalizar anuncios y sugerencias de contenido. Recopila información sobre el dispositivo que se usa y la ubicación geográfica. También puede compartir los datos con socios comerciales y anunciantes (Twitter, 2023). Durante las elecciones presidenciales de 2020 en Estados Unidos, Twitter fue criticado por su manejo de la desinformación. La plataforma utilizó algoritmos para identificar y marcar contenido potencialmente engañoso, pero también enfrentó desafíos en cuanto a la aplicación consistente de estas políticas, lo que generó debates sobre la libertad de expresión y la censura (Frenkel & Alba, 2020).

TikTok, emergió en 2016 y rápidamente integró tecnologías de IA para analizar videos y comportamientos de usuarios. Su propiedad por ByteDance (2023), ha planteado preocupaciones internacionales sobre privacidad, especialmente relacionadas con la transferencia y el almacenamiento de datos. TikTok analiza los videos que se suben y el comportamiento en la plataforma (visualizaciones, interacciones) utilizando IA. Recopila datos personales como nombre, edad, información de contacto y datos biométricos. Los datos pueden ser transferidos y almacenados en servidores fuera del país de residencia, incluyendo China. Utiliza los datos para mostrar anuncios y contenido personalizado (TikTok, 2023). En 2020, se reveló que TikTok recopilaba datos biométricos y de ubicación de los usuarios, lo que generó preocupaciones sobre la seguridad nacional en varios países. Además, el algoritmo de TikTok ha sido criticado por promover contenido específico que puede influir en las decisiones de compra y comportamientos de los usuarios, especialmente entre los jóvenes (Fowler, 2020).

1.3.5 Algunos riesgos actuales relacionados con la IA en redes sociales, (como identidades falsas y hackeos)

La inteligencia artificial (IA) ha revolucionado la manera en que interactuamos en las redes sociales, ofreciendo numerosas ventajas en términos de personalización y eficiencia. Sin embargo, también ha

introducido riesgos significativos que afectan la privacidad y seguridad de los usuarios. Este análisis explora algunos de estos riesgos actuales, subrayando la necesidad de medidas de protección adecuadas.

Uno de los riesgos más destacados es la creación y proliferación de identidades falsas. Van der Walt et al. (2018), destacan cómo la IA puede ser utilizada para generar perfiles falsos que son indistinguibles de los reales. Estos perfiles pueden ser usados para realizar actividades maliciosas como estafas y manipulación de opiniones. La detección de estas identidades falsas es un desafío constante debido a la sofisticación de las técnicas empleadas.

Otro riesgo importante es el hackeo de cuentas, donde los atacantes utilizan técnicas de IA para descifrar contraseñas y burlar medidas de seguridad. Según Khan (2017), la vulnerabilidad de las plataformas sociales ante estos ataques ha crecido, y los métodos tradicionales de protección ya no son suficientemente efectivos frente a los programas avanzados de IA que aprenden y evolucionan.

La privacidad de los datos es una preocupación constante en redes sociales. Taddicken (2014), discute cómo la recopilación y análisis de datos por IA pueden llevar a violaciones significativas de la privacidad, donde información personal sensible se ve comprometida sin el conocimiento del usuario. La falta de transparencia en cuanto a qué datos se recopilan y cómo se utilizan es una problemática central en la era de la IA.

Los usuarios de redes sociales a menudo se convierten en stalker cibernéticos, utilizando la información disponible públicamente para seguir y recolectar datos sobre otros sin su consentimiento (Gil, 2016). Otro autor, Castillo Parrilla (2023), señala que la IA puede facilitar este comportamiento al automatizar y optimizar la recopilación de datos, lo que intensifica las preocupaciones sobre la privacidad y el consentimiento.

Un aspecto preocupante es la violación del derecho a la privacidad, un principio fundamental de los derechos humanos. Vásquez & José Alberto (2021), argumentan que la IA, al permitir la vigilancia y el monitoreo intensivo, puede infringir este derecho sin que el usuario tenga opciones claras para optar por no participar o controlar el uso de sus datos.

El papel de la IA en la manipulación de comportamientos también es significativo. A través del análisis de grandes volúmenes de datos, las plataformas pueden influir sutilmente en las decisiones y opiniones de los usuarios, un riesgo que, se identifican como una de las principales amenazas éticas de la IA en plataformas sociales (Carlos et al., 2023).

Finalmente, es crucial reconocer la necesidad de implementar marcos legales robustos para regular el uso de la IA en redes sociales. La introducción del Reglamento General de Protección de Datos (RGPD) en Europa y otras legislaciones similares son pasos hacia la protección de los usuarios contra los abusos potenciales de la IA, como sugiere Bosque & Villan (2018),quienes abogan por un enfoque multidisciplinario para abordar estos desafíos.

1.3.6 Marco Regulatorio: Reglamento General de Protección de Datos (RGPD) y el marco normativo ecuatoriano

En el ámbito regulatorio, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea ha establecido un marco legal integral para la protección de datos personales en la era digital (Unión Europa, 2016). El mismo RGPD destaca y subraya la importancia de la transparencia en el manejo de datos y el consentimiento informado de los usuarios. Esta normativa representa un esfuerzo regulatorio significativo para salvaguardar la privacidad en el contexto de la IA y las redes sociales. Si bien el RGPD representa un paso importante en la protección de la privacidad en línea, también plantea desafíos adicionales en el contexto de la IA y las redes sociales. Alston & Gillespie (2012), argumentan que la IA puede desempeñar un papel crucial en la reducción de la dispersión de la información en línea, lo que podría mejorar la precisión y la relevancia de los resultados de búsqueda.

Aunque Ecuador no implementa directamente el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, Espinosa (2022), señala que este ha servido como referencia y base para el desarrollo de la legislación nacional en materia de protección de datos. La Ley Orgánica de Protección de Datos Personales (LOPD) es la principal regulación en Ecuador para garantizar la privacidad y la integridad de los datos personales de los ciudadanos. Entró en vigor el 27 de mayo de 2021 y establece los principios fundamentales para el tratamiento transparente, justo y seguro de los datos personales, así como los derechos de los individuos sobre sus propios datos. Además, la LOPD introduce la figura del Delegado de Protección de Datos (DPO), quien actúa como defensor de la privacidad y vela por el cumplimiento legal y ético en el manejo de datos personales (Rodríguez Ayuso, 2020).

Un ejemplo concreto del uso de la Ley Orgánica de Protección de Datos Personales (LOPD) en Ecuador se evidencia en el sector de la salud, donde los profesionales y las instituciones médicas deben asegurar la confidencialidad y seguridad de la información médica de los pacientes. El cumplimiento riguroso de estas disposiciones es fundamental para proteger los derechos fundamentales de privacidad y confidencialidad de los pacientes. Cualquier violación de estas normativas puede acarrear no solo sanciones legales, sino también consecuencias graves para la integridad y la confianza en el sistema de salud.

Dentro del contexto ecuatoriano se debe partir de la Constitución del Ecuador del 2008, donde se establece el derecho fundamental a la privacidad y la protección de los datos personales, se evidencia un marco normativo sólido que busca salvaguardar estos derechos en el contexto nacional (Asamblea Nacional del Ecuador, 2008). Aunque la legislación ecuatoriana no aborda específicamente el tema de la Inteligencia Artificial (IA), se puede inferir por analogía que el Estado tiene la obligación de proteger la integridad y confidencialidad de los datos de sus ciudadanos, ya que este es un derecho fundamental. El Codigo Orgánico Integral Penal Del Ecuador (2021), (COIP) establece en sus artículos 179 y 180 sanciones para aquellos individuos que violen la privacidad de terceros al recopilar, almacenar o transmitir información sin autorización expresa.

En donde señalar que, según el Artículo 66 de la Constitución del Ecuador del 2008, se reconocen y garantizan a las personas diversos derechos fundamentales relacionados con la privacidad y la protección de datos personales, entre otros, el derecho a la intimidad (Numeral 7), la inviolabilidad de la correspondencia y las comunicaciones (Numeral 11), el derecho a la protección de datos personales (Numeral 18), la autodeterminación informativa (Numeral 19), la reserva de la vida privada (Numeral 20) y el secreto bancario y financiero (Numeral 21). Estos derechos son parte integral del marco legal ecuatoriano y refuerzan la protección de la privacidad y la confidencialidad de los datos en el contexto nacional.

El análisis del Artículo 92 de la Constitución del Ecuador del 2008, que establece el principio de habeas data, es fundamental para comprender la protección de datos personales en el país. Este artículo garantiza a las personas el derecho a acceder, conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos públicas o privadas y en archivos de entidades públicas o privadas que realicen tratamiento de datos. En otras palabras, el habeas data asegura que los individuos tengan control sobre la información que se almacena sobre ellos y les permite corregir cualquier inexactitud o incompletitud en sus datos personales. Esta disposición constitucional refuerza aún más el compromiso del Estado ecuatoriano con la protección de la privacidad y la integridad de los datos personales de sus ciudadanos, estableciendo mecanismos legales para garantizar el ejercicio efectivo de estos derechos.

Por lo tanto, se puede inferir que cualquier violación de datos en el contexto ecuatoriano no solo constituye una infracción legal, sino también una violación a los derechos humanos fundamentales. La protección de la privacidad y la integridad de los datos personales es un pilar central en la legislación y la jurisprudencia del Ecuador, y su violación conlleva consecuencias legales y éticas significativas. Es necesario reforzar y hacer cumplir estas disposiciones legales para garantizar la protección efectiva de los derechos individuales en la era digital.

1.3.7 El derecho a la protección de datos como un derecho humano fundamental

Los derechos fundamentales, a diferencia de los DDHH son protegidos obligatoriamente por cada estado desde su positivización en la constitución, por ello, la protección de datos personales no es una simple cuestión técnica o administrativa, sino un derecho fundamental que debe ser reconocido y garantizado como tal (Martínez Martínez, 2007). En este sentido, Cannataci et al. (2010), destacados académicos malteses especializados en derechos humanos y la privacidad en la era digital, argumenta que el derecho a la protección de datos es crucial en un mundo cada vez más interconectado y tecnológico.

Basado en la obra "Global Privacy Protection: The First Generation", Rule & Greenleaf (2010), sostienen que el derecho a la protección de datos es esencial para preservar la dignidad humana, la autonomía y la libertad individual en la sociedad contemporánea. Además, advierten sobre los desafíos que surgen en cuanto a la protección de datos en el contexto de la inteligencia artificial (IA). Reconocen que la IA puede conducir a una mayor recopilación y análisis de datos personales, lo que aumenta el riesgo de violación de la privacidad de los individuos.

Sin embargo, Rule y Greenleaf también destacan la necesidad de encontrar un equilibrio entre la innovación tecnológica y la protección de la privacidad. Argumentan que las regulaciones sólidas son fundamentales para salvaguardar el derecho a la protección de datos en el contexto de la IA. Aunque reconocen el potencial beneficio de la IA en diversos ámbitos, advierten sobre los peligros de un uso

irresponsable o malintencionado de esta tecnología que pueda socavar los derechos fundamentales de las personas (Rule & Greenleaf, 2010).

El actual acceso a datos y la libre circulación de la información es el mayor desafío que enfrentan las políticas de protección de datos, es así que el mismo RGPD afirma la necesidad de unificar los valores fundamentales del respeto a la información privada y la libre circulación de la información, tal como afirma Castillo Parrilla (2023). Para Gil (2016), el valor de los datos aumenta de acuerdo a la interconexión entre ellos. La protección de datos se ha estudiado tradicionalmente desde el conjunto de derechos humanos de primera generación, pero de acuerdo con Castillo Parrilla (2023), con la llegada de la IA y big data, se ha añadido una arista más a su análisis y encasillamiento en la cuarta ola de los DDHH, ya que esta tiene su enfoque en un entorno digital. Considerando las declaraciones de Gil, la protección de datos como un derecho humano debe ser abordada desde una perspectiva renovada. Esto implica comenzar con la identificación y el análisis de lo que él denomina "acciones contaminantes", tales como la recopilación excesiva de datos, y luego avanzar hacia la comprensión de un entorno digital saludable que garantice que los individuos puedan desenvolverse con un mínimo de expectativas de anonimato (Castillo Parrilla, 2023). En la actualidad ha dado una tendencia a añadir a la protección de los datos como un derecho fundamental, en el contexto europeo, ya que la protección de datos es mencionada en la Carta Europea de Derechos Fundamentales y también fue mencionado en la fallida constitución europea con una definición de derecho fundamental (Martínez Martínez, 2007).

Por otra parte, en Chile se ha logrado una positivización en protección de datos, ya que, destacado por Contreras (2020), con la última reforma de la constitución chilena, la protección de datos ha encontrado su lugar como un derecho fundamental. Los datos personales son información que puede ser utilizada como herramienta de ventaja competitiva al poder predecir comportamientos y generar una línea de tendencia, esto ha llevado a muchas empresas a rozar con los límites de la privacidad individual ya que han usado estos datos a favor de sus intereses, es esta preocupación lo que nos lleva a establecer a la protección de datos como un derecho fundamental (Frigerio, 2018).

Adicionalmente, para Medina Guerrero (2022), más allá de la protección de datos, los individuos deben tener conocimiento de los algoritmos que usan sus datos y los fines de estos, en los casos en los cuales se utilice su información para la toma de decisiones que les afecten y en procesos automatizados que vayan tener un impacto en la vida de las personas. Es así que la protección de datos debe regularse y tratarse como un derecho fundamental, en una era de digitalización que permite exponer excesivamente información, por lo cual debe también garantizar la protección de esta. Si bien es en Europa en donde se ha desarrollado más la protección de datos. En la Tabla 1 se puede observar que en Sudamérica existen leyes similares.

Tabla 1
Leyes de protección de datos

País	Ley	Año
Chile	Ley N 19628 sobre protección de Vida Privada	1999
Argentina	Ley de protección de datos personales	2000
Paraguay	Ley N 1682 de Protección de Datos Personales	2001
Uruguay	Ley N 18.331 de Protección de Datos Personales y Habeas Data	2008
Venezuela	Ley Orgánica sobre el Derecho a la Protección de los Datos Personales	2008
Bolivia	Ley N 1640 de protección de datos personales	2011
Perú	Ley N 29733 de Protección de Datos Personales	2011
Colombia	Ley Estatutaria N 1581 de 2012 de Protección de Datos Personales	2012
Brasil	Ley general de Protección de Datos Personales	2018
Ecuador	Ley Orgánica de Protección de Datos Personales	2019

Nota: Todas estas leyes se han generado en un contexto no digitalizado pero su aplicación puede darse en este contexto.

1.3.8 Evolución de las normas en casos de violaciones a la intimidad en Ecuador y Latinoamérica

En Ecuador, la Constitución no vela únicamente sobre la protección a la vida, sino también sobre todo tipo de invasión al individuo. “El derecho a la protección de datos reconoce al individuo la facultad de controlar sus datos personales y a su vez la capacidad de disponer y decidir sobre los mismos” (Villalba, 2017). Este principio constitucional se alinea con el hábeas data, reconocido como un mecanismo de garantía del derecho a la protección de datos personales en Ecuador. Este derecho no podrá ser invocado como medio para requerir la entrega física del soporte material o electrónico de los documentos que contengan información personal, sino para conocer su existencia, tener acceso a él y ejercer los actos previstos en el artículo 92 de la Constitución de la República, que establece el marco legal del hábeas data.

El tratadista Puccinelli (1999), analiza la sentencia 001-14-PJO-CC de la Corte Constitucional del Ecuador en referencia a este derecho. En su análisis, señala que el derecho a la protección de datos, conocido como la "autodeterminación informativa", tiene un carácter instrumental. Según Puccinelli, este derecho está supeditado a la protección de otros derechos constitucionales que podrían verse afectados cuando se utilizan datos personales, como la intimidad y otros derechos fundamentales.

Se puede decir entonces que el derecho a la protección de datos ha evolucionado en el actual contexto digital que vivimos. Además del marco normativo establecido en la Constitución y en el Código Orgánico Integral Penal (COIP), la jurisprudencia ecuatoriana ha jugado un papel crucial en el abordaje de violaciones a la intimidad y protección de datos personales. Según estudios realizados por Durán Ramírez & Zamora Vázquez (2023), la Corte Constitucional del Ecuador ha emitido fallos que han sentado precedentes importantes en casos relacionados con la privacidad en línea y el uso indebido de datos personales.

Ejemplos tales como, el caso de la sentencia: No. 2064-14-EP/21 que determinó que la negación de una acción de hábeas data vulneró los derechos de la demandante cuyas fotos íntimas fueron divulgadas sin consentimiento. Reconoció la violación de derechos como la protección de datos personales, intimidad y buen nombre. Se ordenó eliminar las imágenes, prohibir su tratamiento y capacitar a jueces sobre hábeas data para resguardar la privacidad.

Y la sentencia No. 032-17-EP/21 que hace referencia a un caso en el que se determinó que la divulgación no autorizada de información personal en redes sociales constituyó una violación al derecho a la privacidad de un individuo. La Corte ordenó medidas para eliminar la información difundida y proteger los datos personales del demandante en plataformas digitales, reafirmando así la importancia de salvaguardar la privacidad en el entorno digital.

En Argentina, el gobierno ha expresado su intención de presentar un proyecto de ley de inteligencia artificial que incluya disposiciones sobre ética y derechos humanos (Vercelli, 2023). Esto es resultado de la preocupación creciente del uso de datos y la necesidad de generar un marco normativo que regule a la IA, en un contexto de una cuarta ola de DDHH, caracterizada por su enfoque en el entorno digital y tecnológico.

Por su parte, Brasil ha promulgado la Ley General de Datos Personales (LGPD por sus siglas), particularmente enfocándose en la ley No 13.709/2018. Esta ley fue elaborada con el fin de garantizar la libertad y la privacidad de los ciudadanos brasileños (Torres et al., 2018). La misma otorga seguridad jurídica para todos los ciudadanos en una economía cada vez más digitalizada; la LGPD define como dato personal a “cualquier información relacionada a la persona natural identificada o identificable” y establece que el tratamiento de datos es toda operación realizada con los datos de cada individuo (LGPD, 2018).

En su reciente reforma constitucional, Chile ha dado un paso significativo al establecer un marco normativo sólido para la protección de datos personales, tomando como referencia principal al RGPD. Como señala Contreras (2020), la adopción de principios y estándares inspirados en el RGPD refleja el reconocimiento por parte de las autoridades chilenas de la necesidad de alinearse con las mejores prácticas internacionales en materia de protección de datos. Estos esfuerzos legislativos reflejan la creciente preocupación en la región por garantizar la protección de los derechos individuales en un entorno digital en constante evolución. Estos ejemplos representan la influencia del RGPD en Latinoamérica y cómo este marco legal europeo ha llevado a evolucionar a las normas legales actuales.

1.3.9 El uso e influencia del RGPD en algunos países andinos

Como indica el libro “La Visión de América Latina Sobre El Reglamento General de Protección de Datos” Enríquez Álvarez (2020), indica que desde la entrada en vigor del RGPD, la mayoría de países latinoamericanos, especialmente los andinos, iniciaron un proceso de reformas en la protección de datos para adaptarse al marco legal mencionado. Este fenómeno refleja una clara tendencia hacia la nueva era digital y la imperiosa necesidad de contar con un marco regulatorio adecuado. A pesar de los notables avances en la protección de datos impulsados por el RGPD, los profesionales de seguridad en países andinos, se enfrentan a un desafío significativo, ya que su formación se basa principalmente en metodologías estadounidenses.

Bolivia ha establecido una legislación de protección de datos, Reglamento a la Ley 163 de Telecomunicaciones y Tecnologías de la Información y Comunicación (Reglamento TIC boliviano) el cual, de acuerdo a Ildefonso & Aruquipa (2020), está inspirado en el RGPD de la UE, pero con la diferencia de que este último reconoce a la persona física, mientras que la normativa boliviana reconoce a la persona natural o jurídica, su influencia es evidente, como se puede apreciar en la tabla 2.

Tabla 2
Similitudes entre el RGPD y TIC boliviano

Tópico	RGPD	TIC boliviano
Licitud, lealtad y transparencia	5.1a	4.IIc, 56. D
Limitación de la finalidad	5.1b	4.II. a
Minimización de datos	5.1c	
Calidad	5.1d	4.II. b
Limitación del plazo de conservación	5.1e	
Integridad y confidencialidad	5.1f	4.II. d, 4. II. e
Responsabilidad proactiva	5.2	
Licitud del tratamiento	6	
Condiciones para el consentimiento	7	56.b
Consentimiento a menores de edad	8	
Datos sensibles	9	
Datos personales relativos a infracciones penales	10	

Nota: Elaboración propia, adaptado de Mapeo del Reglamento TIC boliviano, RGPD y Estándares RIPD en materia de Protección de Datos Personales, por Ildefonso y Aruquipa, 2020

Si bien es cierto que no todos los aspectos cubiertos por el RGPD se encuentran positivizados en el TIC boliviano, es clara la relación entre los dos. Especialmente en lo que a aspectos generales se refiere.

Por su parte, Perú cuenta con la Ley No. 29733, Ley de Protección de Datos Personales (LPDP), que fue influenciada por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. La investigación de Vásquez Rodríguez (2022), ejemplifica cómo el artículo 5 del LPDP, sobre el principio de consentimiento, es una clara referencia al RGPD. Una parte esencial a tomar en cuenta del LPDP es que este cuerpo normativo y su reglamento son normas infra constitucionales que desarrollan derechos a las personas mediante la derivación del derecho fundamental a la protección de datos personales (Vásquez Rodríguez, 2022).

De acuerdo a Albornoz (2022), en Ecuador en su Ley Orgánica de Protección de Datos Personales del 2021 se observa que los incisos 2, 3 y 4 del artículo 3 contemplan criterios consagrados por el artículo 3.1 del RGPD. Siendo este el ejemplo más claro de como el RGPD ha influencia a las normativas de los países andinos. Un ejemplo adicional de este avance en la protección de datos es la Agencia de Protección de Datos de Ecuador (APD) la cual en 2022 ayudó a una ciudadana a recuperar datos que habían sido usados ilegalmente luego de que su ex pareja los había compartido si su autorización; ordenando la eliminación de los datos y prohibiendo volver a contactar con esta ciudadana.

El caso de Colombia se puede ejemplificar de mejor forma con la actual sanción de la Superintendencia de industria y comercio de Colombia a Claro por vulnerar el Régimen de Protección de datos, imponiendo la sanción más alta posible; Claro omitió la implementación de medidas adecuadas y la cantidad necesarias de ellas a través de una de sus campañas comerciales (Superintendencia de Industria y Comercio, 2023). Este caso refleja la normativa colombiana, que coincidiendo con la boliviana es infra constitucional y se ve influenciada por el RGPD.

Para Bosque & Villan (2018), el impacto que el RGPD ha tenido algunos países andinos, ha impulsado leyes y reformas mediante el fortalecimiento de instituciones y sensibilizando a los ciudadanos. Reformas que se ven positivizadas en varios cuerpos legales como lo son el COIP en el caso ecuatoriano la nueva ley orgánica de Protección de datos, la LPDP de Perú y el Régimen de Protección de Datos de Colombia. A pesar de no utilizarse de manera directa al RGPD, no se puede negar que este ha influenciado a los países mencionados al momento de establecer marcos jurídicos que protejan a los datos de las personas.

1.3.10 Privacidad de datos en los Estados Unidos de América

Según Pérez (2022), el derecho constitucional de Estados Unidos, generalmente no positiviza los derechos de las personas, sino que más bien prohíbe la negación de libertad, en donde residen los derechos de privacidad. Esto se relaciona estrechamente con la preocupación creciente por la protección de datos en el país ya que la privacidad está estrechamente relacionada con las libertas. Barrio Andrés (2022), señala que esta preocupación ha llevado al surgimiento de propuestas de protección de datos en Estados Unidos, las cuales buscan abordar los desafíos y garantizar la salvaguarda de la privacidad de los individuos en un entorno digital en constante evolución.

Por exponer unos ejemplos de la positivización de leyes de protección de datos, en junio de 2022, California, Virginia, Colorado, Utah y Connecticut han promulgado con éxito leyes de privacidad estatales

completas que regulan la protección de los datos de los consumidores. Un ejemplo notable es la California Consumer Privacy Act (CCPA por sus siglas en inglés), la cual entró en vigor en 2020 (CCPA, 2024). Esta ley protege a todas las personas físicas dentro del estado de California y otorga a los consumidores tres derechos principales: conocer los datos que las empresas han recopilado, optar por la venta de la información recopilada y eliminar los datos personales recogidos en ciertas circunstancias (Duties et al., 2024). Estos casos ejemplifican cómo la preocupación por proteger datos se ha convertido en leyes de protección de datos.

Un caso de análisis sobre la protección de datos es el incidente de Ashley Madison, una red social de aventuras extramatrimoniales que fue hackeada en julio de 2015 (Platero Alcón, 2017). La exposición de la información de los usuarios generó preocupación sobre la protección de datos. Según Platero Alcón (2017), la declaración de privacidad de Ashley Madison autoriza a la red social para compartir o vender todos los datos personales recopilados, incluso información tan trascendente como el origen étnico o la vida sexual con terceros, así como reservarse el derecho de compartir información financiera de los clientes, dado que la plataforma es de pago. Al evidenciar el uso de información personal en un entorno de big data, como en el caso de la red social Ashley Madison, se revela cómo esta red aprovecha los datos de los usuarios a través de términos y condiciones que frecuentemente pasan desapercibidos para aquellos que comparten su información en estas plataformas.

Otro caso destacado es el de Cambridge Analytica. Tras el escándalo de la filtración de información, el CEO de Facebook, Mark Zuckerberg, se vio obligado a establecer un comité independiente sobre privacidad, despojado de su control directo, y a fortalecer la supervisión de aplicaciones de terceros. Según Vera (2019), este caso se percibe como un ataque a la democracia, dado que los datos obtenidos de Facebook se utilizaron para influir en las elecciones estadounidenses, resultando en la victoria de Trump. Según Vera (2019), este caso se percibe como un ataque a la democracia, dado que los datos obtenidos de Facebook se utilizaron para influir en las elecciones estadounidenses, resultando en la victoria de Trump. Este incidente no solo vulnera la privacidad individual, sino que también afecta la libertad, un derecho humano fundamental protegido por Estados Unidos para sus ciudadanos. La crítica se centra en la acusación contra Zuckerberg de haber compartido datos con Cambridge Analytica, que luego utilizó en una estrategia de campaña para influir en diversos procesos políticos, como las elecciones presidenciales de EE. UU. y el Brexit.

Teniendo en cuenta que el mal uso de los datos no solo vulnera la individualidad de las personas, sino que también puede afectar la democracia y las relaciones internacionales al influir en ellas a través del uso de big data. Estos casos ejemplifican la urgente necesidad de una legislación específica de protección de datos con alcance nacional, que no se limite únicamente a los estados, sino que tenga un carácter federal.

2. Métodos

2.1 Revisión Sistemática

La metodología seleccionada para este estudio de investigación es la declaratoria PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) reconocido por su eficacia en el análisis cualitativo en campos sociales, a pesar de haber sido diseñado originalmente para estudios médicos (Samala et al., 2023). Además, esta metodología facilita la verificación inversa, lo que significa que los resultados obtenidos pueden ser corroborados.

2.2 Aplicación de la metodología Prisma

Para llevar a cabo esta investigación, se siguieron los siguientes pasos estructurados de Yepes-Nuñez et al. (2021), según la metodología PRISMA:

- Definición de preguntas y objetivos: Se estableció como pregunta principal: ¿Cómo la inteligencia artificial viola el derecho a la privacidad en las redes sociales? Esta se subdividió en tres sub-preguntas para facilitar la búsqueda y análisis de literatura: ¿Qué técnicas emplea la inteligencia artificial para recolectar y analizar datos personales en las redes sociales? ¿Cómo contribuyen estas técnicas a violaciones de privacidad como la creación de identidades falsas y hackeos? ¿Cuáles son las medidas regulatorias vigentes destinadas a proteger la privacidad de los usuarios frente a estas tecnologías?
- Selección de bases de datos: Las búsquedas se realizaron en bibliotecas digitales de alta relevancia académica: Scopus y Web of Science
- La cadena de búsqueda es: Artificial AND intelligence AND human AND rights AND privacy
- Creación de una matriz de análisis: Se elaboró una matriz para clasificar y evaluar todos los artículos recolectados según su relevancia y aporte a las preguntas de investigación.

- Criterios de elegibilidad: Se implementaron los criterios de inclusión y exclusión para seleccionar estudios pertinentes y fiables como se puede observar en la tabla 3.

Tabla 3
Criterios de Inclusión y Exclusión de artículos

Criterios	Inclusión	Exclusión
Bibliotecas digitales	Web of Science y Scopus	
Idioma	Inglés y español	Artículos escritos en idiomas diferentes a inglés y español
Tipo de documento		Material editorial, corrección, libros, páginas, revistas, opiniones sobre revisiones de literatura, acceso temprano, reporte, actas de conferencias, revista comercial, cartas, serie de libros, notas.
Años de publicación	2018-2024	
*Países/Regiones	Todos los países	
Tipo de acceso	Artículos de todo tipo, disponibles para descarga	
Área temática	Temáticas relacionadas con el título de la investigación	Casos específicos que no sea posible descargar.

2.3 Palabras Claves

La estrategia de cadena de búsqueda es: Artificial AND intelligence AND human AND rights AND privacy. Se aplicarán filtros de año para seleccionar estudios desde 2018 en adelante, reflejando el impacto del escándalo de Cambridge Analytica como punto de inflexión. Este incidente marcó un cambio significativo en la percepción pública sobre la privacidad digital y destacó las complejas interacciones entre la inteligencia artificial y la protección de datos personales en redes sociales, desencadenando un debate crítico sobre la privacidad digital y los principios éticos en la inteligencia artificial.

2.4 Proceso de Selección de Estudios

El proceso de selección de estudios para esta investigación se llevó a cabo en tres fases, basadas en la metodología PRISMA, utilizando un total de 90 artículos seleccionados, como se puede ver en los anexos. A continuación, se describen las fases y criterios aplicados en cada una:

Screening inicial:

- Ingresando la cadena de búsqueda: Artificial AND intelligence AND human AND rights AND privacy en Web of Science, se obtuvo un total de 158 artículos. En Scopus, se obtuvieron 364 artículos.
- Se realizó un filtro inicial basado en los títulos y resúmenes de los artículos para identificar aquellos potencialmente relevantes para el tema de investigación: "La injerencia de la IA en la violación al derecho a la privacidad en redes sociales".
- Se incluyeron artículos publicados entre 2018 y 2024 en inglés y español, disponibles en las bases de datos Web of Science y Scopus.

Revisión completa:

- Los textos completos de los artículos seleccionados en la fase de screening fueron revisados en detalle para evaluar su conformidad con los criterios de inclusión y exclusión definidos en la tabla 3.
- Se excluyeron artículos que no cumplían con los criterios de relevancia temática, idioma o tipo de documento.
- Esta revisión redujo el número de artículos a 90, que cumplían con todos los criterios establecidos.

Descarga de metadatos:

- Se descargaron los metadatos de los 90 artículos seleccionados en formato CSV para su posterior análisis sistemático.
- Estos datos incluían información relevante como título, autor, año de publicación, base de datos de origen y contenido específico relacionado con el tema de estudio.

2.5 *Extracción de Datos*

Para la fase de extracción de datos, se utilizaron las opciones de exportación de las bases de datos Web of Science y Scopus, las cuales permiten descargar los resultados en formato CSV y Excel, tal y como detalla la metodología prisma y de acuerdo a un artículo de revisión sistemática respectivamente. Estas herramientas de exportación facilitaron el filtrado inicial de los estudios según criterios predefinidos como autores, año de publicación, metodología empleada y hallazgos principales. Una vez completada la extracción de datos, se procedió a organizar la información en dos archivos Excel. En la primera hoja de cada archivo, se incluyeron los datos descargados en formato CSV. En la segunda hoja, se redactó la información siguiendo el ejemplo de matriz de revisión de literatura proporcionado por la Biblioteca UDA. Esta matriz permitió clasificar y sintetizar los estudios de manera coherente y estructurada. Finalmente, la información organizada en las hojas de Excel se convirtió en una tabla de Word, misma que es el Anexo 1. Esta combinación de procesos automatizados y revisión manual garantizó la relevancia y calidad de los datos extraídos.

3. Resultados

3.1 *Análisis y selección de datos*

La selección y análisis de datos se llevó a cabo utilizando una metodología de revisión sistemática de literatura. Se llegó a un total de 90 artículos relevantes que abordan la injerencia de la inteligencia artificial en la violación de la privacidad en las redes sociales (véase Anexo1). A continuación, se presentan los resultados obtenidos.

3.2 Análisis de origen geográfico de las publicaciones

Tabla 4
Distribución de publicaciones por regiones

Región	Número de Artículos
América del Norte	40
Europa	25
Asia	15
África	5
Otros	5

Como se expone en la tabla 4, la mayoría de las publicaciones provienen de América del Norte y Europa, lo cual tiene sentido debido a la alta concentración de estudios sobre violaciones a la privacidad y la inteligencia artificial en estas regiones. En los Estados Unidos, la preocupación por la protección de datos está estrechamente relacionada con las libertades constitucionales. Es por ello que incidentes como el de Cambridge Analytica, según Vera (2019), en su artículo “Nada es privado”, un documento sobre ese caso, resalta la gravedad del uso indebido de datos personales a través de Facebook de millones de usuarios, convirtiéndose en uno de los ejemplos más notables de violación al consentimiento informado. En 2023, aproximadamente el 81% de los adultos en los Estados Unidos utilizan YouTube y el 69% usan Facebook, lo que indica una alta penetración de las redes sociales en la población adulta. Este amplio uso de redes sociales facilita la recolección masiva de datos, lo que incrementa el riesgo de violaciones de privacidad (Pew Center, 2024).

En Europa, con 25 publicaciones, se ha observado una influencia significativa del RGPD en las normativas de protección de datos en varios países europeos. Esta regulación ha establecido un estándar para la protección de datos personales y ha servido de modelo para otras jurisdicciones. Albornoz (2022), destaca cómo el RGPD ha sido fundamental en la creación de políticas de protección de datos robustas en Europa. En Asia, con 15 publicaciones, se observa un enfoque creciente en la regulación de la privacidad y la protección de datos. En Japón, por ejemplo, las leyes de protección de datos centradas en el ser humano subrayan la dignidad y la privacidad individual. Estas leyes reflejan un compromiso con la protección de los derechos de los ciudadanos en un contexto digital cada vez más complejo (Miyashita, 2021).

En África, aunque solo hay 5 publicaciones, la regulación de la IA debe considerar tanto los beneficios como los riesgos para los derechos humanos. Abe & Eurallyah (2022), destacan que la ausencia de derechos humanos robustos en algunos países africanos incrementa la vulnerabilidad a las violaciones de privacidad. Sin embargo, también existe un interés en utilizar la IA para mejorar las regulaciones y proteger a la población, como lo señala Brand (2022), en su artículo "Responsible Artificial Intelligence in Government: Development of a Legal Framework for South Africa", donde resalta tanto la falta de protección como el potencial de la IA para mejorar las condiciones de derechos humanos en la región. En América Latina, la influencia del RGPD ha sido notable en la formulación de leyes de protección de datos (Enríquez Álvarez, 2020). Este esfuerzo por alinear las normativas locales con los estándares internacionales refleja un compromiso por mejorar la privacidad de los usuarios y proteger mejor sus datos personales en un entorno digital global.

3.3 Análisis de las áreas temáticas

La revisión de los 90 artículos seleccionados revela en la tabla 5 una diversidad de enfoques temáticos.

Tabla 5
Distribución de publicaciones por áreas temáticas

Área Temática	Número de Artículos
Ética Informática	25
Regulación de Datos	20
Derechos Humanos	18
Inteligencia Artificial y Privacidad	27

Los estudios en el área de Ética Informática (25 artículos) exploran las implicaciones éticas del uso de la inteligencia artificial, abarcando temas como la equidad, la transparencia y la responsabilidad en el diseño y la implementación de sistemas de IA. En cuanto a la Regulación de Datos (20 artículos), esta área se centra en las políticas y las leyes relacionadas con la protección de datos y la privacidad, evaluando la efectividad de las regulaciones existentes y proponiendo nuevas estrategias para mejorar la seguridad de los datos. Los artículos en la categoría de Derechos Humanos (18 artículos) analizan cómo la inteligencia artificial puede afectar los derechos humanos fundamentales, incluyendo el derecho a la privacidad y la libertad de expresión. Por último, el área de Inteligencia Artificial y Privacidad (27 artículos) examina directamente la relación entre la IA y la privacidad, evaluando cómo las tecnologías de IA recopilan, procesan y utilizan datos personales.

También se muestra una diversidad de instituciones académicas de todo el mundo, con una concentración notable en universidades de alto prestigio. Estas universidades se destacan no solo por su cantidad de publicaciones, sino también por la calidad y el impacto de sus investigaciones. Las universidades de alto prestigio, como la Universidad de Harvard, Universidad de Stanford, y la Institución Tecnológica de (MIT) en los Estados Unidos, lideran en términos de contribuciones. Según el QS World University Rankings , estas instituciones se encuentran entre las mejores del mundo debido a su desempeño en áreas clave como la enseñanza, la investigación, la transferencia de conocimiento y la perspectiva internacional (Universities, 2023). Este reconocimiento se basa en indicadores rigurosos que incluyen la reputación académica y la cantidad de citaciones recibidas, lo que subraya la relevancia y el rigor académico de sus investigaciones.

Estos artículos contribuyen significativamente a este artículo de revisión sistemática de literatura debido a su infraestructura avanzada, acceso a recursos y redes de colaboración global. La participación de estas instituciones en la investigación sobre la inteligencia artificial y la privacidad es importante porque valida la selección de los artículos revisados, asegurando que los estudios provienen de fuentes confiables y de alta calidad. El Times Higher Education World University Rankings 2023 destaca que las universidades estadounidenses son las más representadas en el top 200, con 58 instituciones, lo que refleja su liderazgo en investigación y educación superior (Education, 2022).

3.4 Análisis del Rango Temporal

La revisión de los artículos publicados entre 2018 y 2024 esto coincide con los criterios de inclusión que fueron establecidos anteriormente, muestra una tendencia significativa en el aumento de publicaciones desde el año 2020, coincidiendo con el inicio de la pandemia de COVID-19, tal y como se muestra en la tabla 6.

Tabla 6
Número de artículos por año

Año	Número de Artículos
2018	2
2019	4
2020	8
2021	22
2022	21
2023	20
2024	13

El incremento notable en el número de artículos publicados a partir de 2020 puede atribuirse a la pandemia de COVID-19, que provocó un confinamiento global y una dependencia mucho mayor de las redes sociales y las tecnologías de la información. Durante este período, las personas estuvieron más interconectadas a través de plataformas digitales debido al encierro, lo que aumentó la recolección y el uso de datos personales, y con ello, la preocupación por la privacidad y la seguridad de la información.

Según un estudio publicado por Bilisli & Tuzcu (2021), las redes sociales jugaron un papel vital en la diseminación de información sobre la salud pública durante la pandemia, pero también se usaron en exceso, lo que incrementó los problemas de salud mental debido a la propagación de noticias falsas y el pánico social. Este contexto global de mayor interconexión y exposición a las redes sociales justifica el aumento en las investigaciones sobre la privacidad y la inteligencia artificial durante estos años.

3.5 Interpretación de los Resultados

Tras llevar a cabo un análisis minucioso de las fuentes de información recopiladas, se estableció un marco regulador que responde a los retos del entorno digital actual, especialmente en relación con la inteligencia artificial y la privacidad en las redes sociales. Los resultados obtenidos muestran una creciente preocupación por la violación de la privacidad debido a la inteligencia artificial en las redes sociales. La mayoría de los estudios revisados destacan la necesidad de establecer marcos regulatorios más estrictos y claros para proteger los derechos de privacidad de los usuarios. Por ejemplo, Vásquez & José Alberto (2021), señalan que la IA puede violar derechos fundamentales y proponen la necesidad de supervisión humana para proteger estos derechos. Esta perspectiva es compartida por varios autores que enfatizan la importancia de la ética informática y el consentimiento informado en el uso de IA en redes sociales. Sin embargo, los artículos revisados abordan estos temas desde diferentes ángulos. Mientras que algunos estudios, como el de Lane (2022), se centran en la necesidad de claridad en los estándares de derechos humanos, otros, como Miernicki & Ng (2021), exploran los derechos morales en el contexto de la IA.

La diversidad en las áreas temáticas de los artículos revisados refleja la complejidad del tema y la necesidad de un enfoque multidisciplinario para abordar las implicaciones de la IA en la privacidad. Por ejemplo, los estudios sobre regulación de datos y ética informática subrayan la importancia de establecer políticas y prácticas que protejan adecuadamente la privacidad de los usuarios en el entorno digital. Por otro lado, algunos estudios como el de Abe & Eurallyah (2022), abordan la IA desde una perspectiva más positiva, destacando sus beneficios potenciales en regiones como África, donde la tecnología podría ayudar a superar desafíos locales significativos. Sin embargo, estos estudios también reconocen los riesgos y la necesidad de una regulación adecuada para proteger los derechos humanos. En contraste, artículos como el de Villaronga et al. (2018), discuten los riesgos de la IA en términos de privacidad, señalando que la tecnología puede ser utilizada para la vigilancia masiva y la recopilación de datos sin el consentimiento adecuado de los usuarios. Este tipo de investigación resalta la importancia de abordar la ética y la moral tanto de los desarrolladores de IA como de los usuarios que aceptan términos y condiciones sin considerar las implicaciones a largo plazo.

En el contexto europeo, la protección de datos ha sido ampliamente desarrollada. Por ejemplo, Castillo Parrilla (2023), destaca que esta protección debe ser parte de la cuarta ola de los derechos humanos, centrándose en cómo la digitalización afecta los derechos individuales. En contraste, Martínez Martínez (2007),considera la protección de datos un derecho fundamental, respaldado por la legislación nacional, lo que le otorga un carácter vinculante. Esta perspectiva es compartida por Contreras (2020), quien señala que la última reforma de la constitución chilena reconoce la protección de datos como un derecho fundamental. Bowser et al. (2017), plantean que el uso de datos, inteligencia artificial, algoritmos y redes neuronales presenta grandes obstáculos éticos y sociales, como lo demuestran casos como Cambridge Analytica y Ashley Madison. La discriminación algorítmica es otro problema identificado por Castillo Parrilla (2023),

quien explica que los algoritmos pueden perpetuar sesgos, resultando en decisiones injustas o discriminatorias. Esta preocupación es compartida por Obermeyer et al. (2019), quienes resaltan la necesidad de una regulación cuidadosa para garantizar la equidad y la justicia.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea ha tenido un impacto significativo en otros países. En América Latina, leyes como la LPDP de Perú y la Ley Orgánica de Protección de Datos de Ecuador han sido influenciadas por el RGPD. Vásquez Rodríguez (2022), ejemplifica cómo el artículo 5 del LPDP es una clara referencia al RGPD. Albornoz (2022), menciona que la ley ecuatoriana incorpora criterios del RGPD, demostrando su influencia en la región. En Estados Unidos, la adopción de medidas regulatorias en estados como Utah, Virginia, Colorado y Connecticut refleja la creciente preocupación por la protección de datos personales. Chander (2017), subraya la falta de ética en la inteligencia artificial, destacando la necesidad de una regulación que contemple tanto aspectos técnicos como éticos.

4. Discusión

La convergencia entre la inteligencia artificial (IA) y la protección de la privacidad en las plataformas de redes sociales emerge como un tema de primordial interés tanto en el ámbito académico como en el legislativo y social. Este estudio se centra en explorar esta relación y sus implicaciones, considerando el crecimiento exponencial de la IA en distintos aspectos de la vida contemporánea y los desafíos sustanciales que esto plantea para salvaguardar la información personal de los usuarios. La sección que sigue se erige como un espacio de diálogo entre diversos investigadores que han abordado esta temática, examinando los mecanismos subyacentes a la vulneración de la privacidad y las medidas regulatorias concebidas para mitigar sus efectos.

Este análisis permite entender cómo la expansión continua de la IA en diferentes ámbitos de la cotidianidad, desde la publicidad en línea hasta la toma de decisiones automatizada, generan una red compleja de interacciones que impactan directamente en la privacidad de los individuos. En este contexto, la presente discusión busca profundizar en la comprensión de las dinámicas que subyacen a esta intersección entre IA y privacidad, reconociendo la necesidad imperiosa de adoptar enfoques integrales y efectivos para proteger la información personal en el entorno digital.

Mediante un revisión sistemática de 90 estudios seleccionados, se ha abordado la pregunta principal de investigación junto con sus subinterrogantes asociadas, mismas que son las siguientes: ¿Cómo la inteligencia artificial viola el derecho a la privacidad en las redes sociales?; ¿Qué técnicas emplea la inteligencia artificial para recolectar y analizar datos personales en las redes sociales?;¿Cómo contribuyen estas técnicas a violaciones de privacidad como la creación de identidades falsas y hackeos? y ¿Cuáles son las medidas regulatorias vigentes destinadas a proteger la privacidad de los usuarios frente a estas tecnologías?

En este sentido, este aporte genera un cruce entre teorías y estudios para generar conocimientos existentes sobre la intersección entre IA y privacidad en las redes sociales, ofreciendo una visión crítica y contextualizada de las implicaciones éticas, legales y sociales de este fenómeno emergente. A través de una evaluación rigurosa de la literatura académica pertinente, se espera contribuir al desarrollo de marcos regulatorios y políticas públicas que garanticen la protección adecuada de los derechos individuales en el entorno digital en evolución constante. La presente discusión parte de responder a las preguntas planteadas en el estudio en consonancia de las diferentes voces de los autores de los textos recuperados en el proceso de búsqueda, filtración y selección de los textos de estudio.

Pregunta 1: ¿Cómo la inteligencia artificial viola el derecho a la privacidad en las redes sociales?

La cuestión de cómo la inteligencia artificial (IA) viola el derecho a la privacidad en las redes sociales es un tema complejo y multifacético, como lo demuestran varios estudios recientes que, aunque abordan diferentes aspectos, convergen en la necesidad de un enfoque holístico para abordar estos desafíos. Villaronga et al. (2018),destacan que la eliminación de datos en entornos impulsados por bases de datos presenta desafíos significativos, especialmente en términos de la calidad de los resultados obtenidos. En su estudio, la eliminación de puntos de datos individuales no mostró un impacto considerable a gran escala; sin embargo, resaltan que la eliminación aleatoria utilizada en los experimentos no refleja adecuadamente los casos reales, donde los individuos que solicitan la eliminación pueden compartir características comunes que, al ser eliminadas, podrían afectar de manera diferente el conjunto de datos. Este hallazgo sugiere que la eliminación de datos no solo es una cuestión técnica, sino también un desafío ético y práctico en la protección de la privacidad.

En paralelo, Vásquez & José Alberto (2021), abordan la importancia del control humano como un derecho emergente en el contexto de la IA. Destacan que la inteligencia artificial puede tener un impacto significativo en derechos fundamentales como la igualdad, la privacidad, el debido proceso y la libertad de expresión. Según su estudio, considera crucial la protección de datos personales en el uso de la IA y expresa preocupación por posibles violaciones de privacidad debido a la recopilación masiva de datos por parte de sistemas de IA. Este estudio subraya la necesidad de regulaciones más estrictas y la capacitación de los usuarios para entender el funcionamiento de los algoritmos que impactan sus vidas diarias. Estos resultados complementan los hallazgos de Villaronga et al., mostrando que la preocupación por la privacidad y la integridad de los datos no solo es una cuestión técnica, sino también una demanda social ampliamente reconocida. Ambos estudios coinciden en la urgencia de proteger la privacidad, aunque difieren en el enfoque: uno se centra en los desafíos técnicos y el otro en la necesidad de control humano y regulaciones.

Por otro lado, el estudio de Biesaga et al. (2023), ofrecen una perspectiva sobre cómo la pandemia ha influido en las narrativas europeas sobre ciudades inteligentes y vigilancia, utilizando un análisis cuantitativo de 184 artículos de prensa. Se identificaron narrativas dominantes que incluyen la regulación de la inteligencia artificial y el reconocimiento facial, la lucha tecnológica contra la emergencia climática, las aplicaciones de rastreo de contactos y el potencial de la tecnología 5G para impulsar los procesos de digitalización. El estudio destaca que las preocupaciones sobre la privacidad y la vigilancia son centrales en dos de las cuatro narrativas descubiertas, y que, a menudo, la privacidad y la vigilancia se consideran un "mal necesario" para mantener la competitividad de la UE en la rivalidad tecnológica global. Sin embargo, las narrativas relacionadas con el bienestar social y la transparencia de las nuevas políticas son casi inexistentes. Este análisis revela una polarización en las percepciones sobre la vigilancia, indicando que el debate sobre la privacidad y la IA es tanto mediático como social. Los hallazgos de Biesaga complementan los estudios anteriores al agregar una dimensión mediática y social, mostrando cómo la privacidad y la vigilancia son percibidas y discutidas en la esfera pública.

Sin embargo, Raab (2020) y Kosta (2022), acentúan sus estudios e indican que la problemática radica en que esta privacidad es corrompida debido al mal uso que la sociedad hace de esta herramienta tecnológica, lo que pone en riesgo la seguridad y la integridad de los usuarios. Además, señalan que es necesario establecer regulaciones más estrictas para proteger la privacidad en línea y prevenir posibles abusos por parte de las empresas tecnológicas. Esto concuerda Vera (2019), Hueso & Valencia (2020), que manifiestan que las redes sociales, especialmente Facebook, tiene un uso indebido de los datos personales de sus usuarios que junto con el manejo de la inteligencia artificial (IA) en las redes sociales y uso de técnicas avanzadas de procesamiento de datos, ha planteado serios desafíos para la privacidad. En este sentido, es indispensable de acuerdo a los criterios de los autores antes citados una revisión ética y legal para la utilización de algoritmos, análisis de datos y tratamientos de la base de datos de los usuarios de redes sociales sin el consentimiento explícito de estos (Kosta, 2022). Es indispensable que las empresas obtengan un consentimiento claro e informado de los usuarios, asegurando así la confidencialidad y seguridad de la información. Además, Pew Center (2024), indica que es crucial implementar mecanismos de transparencia y rendición de cuentas, permitiendo que los usuarios comprendan y cuestionen las decisiones algorítmicas. La promoción de la conciencia ética mediante la educación y el desarrollo de políticas claras también es esencial para abordar temas como el sesgo algorítmico y la responsabilidad social.

Finalmente, Hoxhaj (2023), se enfoca en el marco legal del Reglamento General de Protección de Datos en la Unión Europea, destacando la necesidad de un enfoque responsable y compatible con el RGPD para el desarrollo de la IA. Subraya que los principios de legalidad, equidad, transparencia y minimización de datos son fundamentales para garantizar que las aplicaciones de IA respeten la privacidad individual y los derechos de protección de datos. Este estudio enfatiza la urgencia de adoptar directrices éticas y medidas regulatorias, abogando por la salvaguardia de los derechos humanos y la dignidad en un mundo impulsado por la IA. De tal forma, la IA plantea desafíos significativos para el derecho a la privacidad en las redes sociales, que van más allá de los aspectos técnicos para incluir dimensiones éticas, sociales y legales. Mientras se destacan los problemas técnicos de la eliminación de datos, también se enfatiza en la necesidad de control humano y la protección de datos, y se muestra la complejidad de las narrativas sociales sobre la privacidad y la vigilancia. Finalmente, se plantea la necesidad de ofrecer un marco legal y ético claro para abordar esta problemática.

Pregunta 2: ¿Qué técnicas emplea la inteligencia artificial para recolectar y analizar datos personales en las redes sociales?

De acuerdo a los resultados de Zhang et al. (2021), donde analizaron un vasto corpus de literatura sobre ética y privacidad en IA, identificando múltiples técnicas y preocupaciones éticas. En su estudio, se destacaron 27 técnicas de IA y la interconexión entre técnicas, preocupaciones éticas y temas sociales en el

ámbito médico y de la salud. Este enfoque coincide con el estudio de Goncalves et al. (2024), que también resaltan la utilización de algoritmos de aprendizaje automático en neuromarketing, un ámbito que se beneficia significativamente de la IA para la segmentación y orientación de preferencias del consumidor. Ambas investigaciones subrayan la importancia y el impacto positivo de la IA en la optimización de procesos y decisiones basadas en datos.

Por otro lado, Kosta (2022), Kim & Routledge (2022), abordan los desafíos éticos y de privacidad que plantean los algoritmos de aprendizaje automático. Kosta destaca las limitaciones de las salvaguardias tradicionales frente a la vigilancia algorítmica y los sesgos incorporados en los algoritmos, lo que coincide con la preocupación de Kim y Routledge sobre la necesidad de explicaciones ex post y la transparencia en el uso de datos. Ambos estudios sugieren que, aunque las técnicas de IA ofrecen ventajas significativas, su aplicación en la recolección y análisis de datos personales debe gestionarse cuidadosamente para proteger los derechos individuales y asegurar la equidad en los resultados algorítmicos.

En cambio, Devia (2019), proporciona una visión general de cómo la IA y el Big Data han transformado el análisis de datos a gran escala, destacando la capacidad predictiva de la IA en áreas como la personalización de contenidos y la toma de decisiones automatizadas. Este punto de vista es complementario a los hallazgos de Zhang et al. y Goncalves et al., ya que todos reconocen el potencial de la IA para mejorar la precisión y la efectividad en diversas aplicaciones mediante el análisis avanzado de datos. Sin embargo, Devia también enfatiza la necesidad de un uso ético y responsable, una preocupación compartida por Kosta y Kim y Routledge.

Por otro lado, Shaik et al. (2022), introducen el concepto de aprendizaje federado, una técnica avanzada que permite la recolección y análisis de datos personales sin centralizarlos. Esta metodología ofrece una solución innovadora para abordar las preocupaciones de privacidad destacadas por Kosta y Kim y Routledge. Al descentralizar el análisis de datos, el aprendizaje federado puede mitigar algunos de los riesgos asociados con la vigilancia estatal y la manipulación de datos por parte de empresas, proporcionando una capa adicional de protección a la privacidad de los individuos.

En cambio, las transacciones económicas involucran la venta de datos personales a terceros, quienes los utilizan para diversos fines comerciales. Estas transacciones pueden incluir desde la venta de información a empresas de marketing hasta el intercambio de datos con entidades financieras para evaluar la solvencia crediticia de los individuos. Este uso económico de los datos plantea serios riesgos para la privacidad, ya que a menudo se realiza sin el conocimiento o el consentimiento explícito de los usuarios (Van Bekkum & Borgesius, 2021).

Además, Lamchek (2023), indica cómo la monetización de datos personales puede llevar a abusos significativos sin un marco regulatorio adecuado que proteja a los individuos. Van Bekkum & Borgesius (2021), añaden que los sistemas de detección de fraude, aunque bien intencionados, a menudo comprometen la privacidad al procesar datos de manera indiscriminada. Estos sistemas pueden analizar grandes volúmenes de datos personales para identificar patrones sospechosos, lo que puede resultar en la vigilancia excesiva y la toma de decisiones automatizadas que afectan negativamente a los usuarios sin que ellos tengan la oportunidad de intervenir o corregir errores.

La implementación de sistemas de IA en la detección de fraudes, como el caso SyRI en los Países Bajos analizado por Van Bekkum & Borgesius (2021), muestran cómo estas tecnologías pueden violar la privacidad si no se implementan con las salvaguardas adecuadas. El tribunal determinó que el sistema SyRI era ilegal porque no respetaba el derecho a la privacidad bajo la Convención Europea de Derechos Humanos. Aloisi & De Stefano (2023), profundizan en cómo la falta de transparencia en los algoritmos de IA puede resultar en la creación de perfiles detallados de usuarios, lo que a veces conduce a la discriminación y manipulación. Finalmente, Miyashita (2020), enfatiza que las normativas actuales, aunque progresistas, no siempre se adelantan a las capacidades emergentes de la IA, lo que deja brechas significativas en la protección de la privacidad. De tal forma que la creciente integración de la inteligencia artificial en diversas aplicaciones de redes sociales y sistemas de detección de fraude resalta la necesidad urgente de marcos regulatorios sólidos que aborden los desafíos éticos y legales asociados. La falta de transparencia y el uso indiscriminado de datos personales sin el consentimiento adecuado socavan la confianza de los usuarios y pueden llevar a abusos significativos. Es imperativo que las legislaciones evolucionen a la par del desarrollo tecnológico para garantizar que los derechos a la privacidad sean respetados y protegidos de manera efectiva.

En este sentido, existen técnicas que la IA utiliza para recolectar y analizar datos personales en las redes sociales. El aprendizaje automático y el procesamiento de lenguaje natural son ampliamente utilizados por la IA para recolectar y analizar grandes volúmenes de datos en redes sociales. Kim & Routledge (2022), examinan cómo estos métodos pueden comprometer la privacidad al monitorizar y predecir

comportamientos sin el conocimiento explícito del usuario. Kosta (2022), añade que la recolección de datos a través de la IA a menudo carece de las salvaguardas necesarias para proteger contra el uso indebido de información. Además, Raab (2020) y Lamchek (2023), discuten cómo la falta de regulaciones claras permite que las entidades exploten estos datos sin restricciones éticas adecuadas.

Pregunta 3: ¿Cómo contribuyen estas técnicas a violaciones de privacidad como la creación de identidades falsas y hackeos?

La evolución de las técnicas de inteligencia artificial (IA) y su creciente adopción en diversos ámbitos han generado preocupaciones significativas respecto a la privacidad y seguridad de los datos personales. Diversos estudios y autores han explorado cómo estas tecnologías pueden contribuir a violaciones de privacidad, como la creación de identidades falsas y hackeos.

Según Vásquez & José Alberto (2021), el diseño de inteligencia artificial que cumpla con las leyes vigentes y proteja la privacidad de los usuarios es crucial. Además, se destaca la importancia de comprender claramente los procesos utilizados en la construcción de sistemas de IA para garantizar la transparencia y el respeto a los derechos humanos. Esto coincide con lo que dicen Villaronga et al. (2018), quienes analizan la efectividad del derecho al olvido en un entorno donde la IA juega un papel crucial. A pesar de que muchos esfuerzos se han centrado en procesar las solicitudes de eliminación de datos mediante algoritmos de IA, persisten preocupaciones significativas sobre la privacidad de los datos. Este estudio resalta cómo, aunque las tecnologías de IA pueden cumplir con ciertas normativas de privacidad, persisten inquietudes sobre su capacidad para proteger verdaderamente los datos personales en un contexto de vigilancia continua y potencial abuso. Este énfasis en la transparencia y la legalidad subraya una preocupación creciente por las implicaciones éticas y legales de la IA, particularmente en términos de privacidad y seguridad de los datos. La transparencia es un factor recurrente en el uso sobre cómo las técnicas de IA pueden llevar a la creación de identidades falsas y hackeos, ya que una falta de claridad en los procesos de IA puede facilitar el mal uso de datos personales. En este sentido, coinciden en la necesidad de transparencia y cumplimiento normativo para asegurar la privacidad, aunque se señala un matiz adicional en Villaronga et al. sobre la eficacia percibida de la IA en la protección de datos.

Por otro lado, Milossi et al. (2021), abordan la importancia de la explicabilidad y transparencia en los sistemas de IA, especialmente en decisiones automatizadas. La capacidad de la IA para tomar decisiones de forma autónoma requiere un proceso transparente que permita a los individuos comprender y, potencialmente, cuestionar estas decisiones. De la misma forma, como destaca Raab (2020), el estudio de la evaluación del impacto de la privacidad y la ética en las tecnologías emergentes es otro punto clave. Su estudio revisa cómo los documentos en este campo incorporan principios éticos y normativos, enfocándose en la transparencia y rendición de cuentas. Este enfoque ético es esencial para mitigar riesgos de violaciones de privacidad, ya que promueve la responsabilidad y supervisión en el desarrollo y aplicación de tecnologías de IA. La insistencia en la ética y la normativa de Raab en, "Information Privacy, Impact Assessment, and the Place of Ethics" se alinea con los hallazgos de Milossi y colegas en "I Ethics: Algorithmic Determinism or Self-Determination? The GDPR Approach" y Vásquez y Toro en "The Right to Human Control: A Legal Response to Artificial Intelligence", consolidando la idea de que la transparencia y la adherencia a principios éticos son fundamentales para la privacidad en la IA. Esta transparencia es fundamental para evitar abusos, como la creación de identidades falsas y hackeos, que pueden ocurrir cuando los sistemas de IA operan sin supervisión adecuada y sin explicación clara. Este punto también resuena con las observaciones de Vásquez y Toro sobre la necesidad de una comprensión clara de los procesos de IA por parte de los usuarios, fortaleciendo la relación entre transparencia y seguridad de datos.

Además, Devia (2019), evidencia cómo la recopilación y uso abusivo de datos personales pueden llevar a violaciones de privacidad. Un test completado por 265,000 usuarios permitió la extracción de datos sensibles sin su conocimiento, demostrando cómo la IA y el Big Data pueden ser explotados para crear perfiles de usuarios y tratar datos de manera abusiva. Este ejemplo subraya la necesidad de una regulación efectiva que proteja a los individuos de prácticas invasivas y potencialmente dañinas. La evidencia presentada por Devia, (2019), contrasta con las aspiraciones de transparencia y protección normativa mencionadas por autores como Vásquez & José Alberto (2021), y Milossi et al. (2021), destacando las brechas prácticas que aún existen en la implementación y supervisión de estas normativas.

Kosta (2022), aborda los desafíos que los algoritmos de aprendizaje automático plantean para la protección de los derechos individuales. Las salvaguardias tradicionales son insuficientes para enfrentar las complejidades de la vigilancia algorítmica, que puede incluir sesgos y falta de transparencia. Estos problemas pueden facilitar la creación de identidades falsas y hackeos, ya que los algoritmos sesgados pueden malinterpretar o manipular datos de manera que comprometan la privacidad y seguridad de los usuarios. Este análisis se alinea con las preocupaciones éticas y de transparencia destacadas por Raab, así

como con la necesidad de explicabilidad mencionada por Milossi y sus colegas, subrayando que las soluciones tradicionales pueden ser insuficientes para los nuevos desafíos de la IA.

En un caso práctico, el fallo judicial sobre la legislación SyRI en los Países Bajos, analizado por Van Bekkum & Borgesius (2021), revela cómo la falta de transparencia en la tecnología puede llevar a violaciones de privacidad. La legislación fue declarada ilegal debido a su opacidad y la invasión de la vida privada de los ciudadanos, destacando el alto riesgo de violaciones de privacidad asociado con el uso de tecnologías de aprendizaje profundo y minería de datos. Este caso práctico ilustra de manera concreta los riesgos teóricos mencionados por otros autores, consolidando la preocupación compartida sobre la falta de transparencia y su impacto directo en la privacidad. Finalmente, Cardiell (2021), discute el impacto de los robots humanoides en la privacidad humana, destacando cómo la interacción con estas tecnologías puede exponer información personal. Los robots humanoides, equipados con múltiples funcionalidades, aumentan la exposición de datos personales, planteando preocupaciones sobre el control de la información y la privacidad. Este análisis complementa los estudios previos al introducir una dimensión más tangible de interacción humano-tecnológica y sus implicaciones para la privacidad.

Este análisis demuestra que un consenso sobre la necesidad de transparencia y regulación efectiva para proteger la privacidad en el uso de técnicas de IA. Aunque estas tecnologías pueden cumplir con ciertas normativas y ofrecer beneficios significativos, la falta de supervisión adecuada y transparencia puede facilitar violaciones de privacidad, como la creación de identidades falsas y hackeos. La integración de principios éticos y la adopción de salvaguardias robustas son esenciales para mitigar estos riesgos y proteger los derechos de los individuos en un entorno digital cada vez más complejo. Las coincidencias entre los autores destacan la importancia de la transparencia y la ética, mientras que las discrepancias señalan las brechas prácticas que aún deben abordarse para lograr una protección efectiva de la privacidad en el ámbito de la IA.

Pregunta 4: ¿Cuáles son las medidas regulatorias vigentes destinadas a proteger la privacidad de los usuarios frente a estas tecnologías?

La protección de la privacidad de los usuarios frente a las tecnologías de inteligencia artificial (IA) es un tema crítico en la era digital. Diversos estudios han explorado las medidas regulatorias vigentes y las percepciones de los usuarios sobre la privacidad, revelando tanto desafíos como avances significativos en este ámbito. Por ejemplo, para Moratinos & Parrilla (2020), abordan la importancia de la transparencia y la adherencia a principios éticos en el uso de sistemas de IA, destacando la necesidad de proporcionar información comprensible sobre el funcionamiento de estos sistemas para garantizar la protección de la privacidad. Esta necesidad de transparencia también se refleja en los hallazgos de Adams et al. (2023), quienes señalan que muchos usuarios desconocen cómo se utilizan sus datos personales en plataformas en línea. Ambos estudios subrayan la importancia de la transparencia y el control humano en el desarrollo y uso de tecnologías de IA, sugiriendo que las medidas regulatorias deben incluir requisitos claros para la divulgación de información sobre el funcionamiento de estos sistemas y el uso de datos personales.

También, Niklas (2021), refuerza la necesidad de implementar regulaciones claras y salvaguardas éticas para proteger a los usuarios y garantizar que la IA se utilice de manera responsable y equitativa. Este llamado a la acción se fundamenta en la creciente preocupación por la privacidad y los posibles abusos en la recolección de datos. Los resultados de (Miyashita, 2021) sobre los riesgos asociados con la explotación de datos personales subrayan la importancia de dichas regulaciones. Además, Devia (2019), argumenta que, sin un consentimiento informado adecuado, las prácticas de recolección de datos pueden ser vistas como invasivas y éticamente cuestionables.

En este sentido, la importancia del consentimiento informado es otro tema recurrente. Miyashita (2021) destaca que las políticas de privacidad son tan extensas y complejas que una persona necesitaría dedicar 244 horas al año para leerlas, lo que dificulta el control efectivo de su consentimiento. Este desafío se complementa con los hallazgos de Adams et al. (2023), donde muchos usuarios entregan información personal sin conocer completamente sus derechos. Ambos estudios sugieren que las medidas regulatorias deben simplificar y hacer más accesibles las políticas de privacidad para facilitar un consentimiento informado real. Esto podría incluir el desarrollo de formatos estandarizados y resúmenes ejecutivos que permitan a los usuarios comprender rápidamente cómo se utilizarán sus datos. Además, es importante que las empresas implementen medidas claras y transparentes para proteger la privacidad de los usuarios, como el cifrado de datos y la limitación del acceso a la información personal. De esta manera, se promoverá una cultura de respeto a la privacidad y se garantizará que los usuarios puedan tomar decisiones informadas sobre el uso de sus datos personales.

Por otro lado, Haitsma y Miyashita abordan el riesgo de discriminación algorítmica. Haitsma (2023), señala los desafíos en la exclusión de datos sensibles en el perfilado basado en datos PNR y la dificultad

para garantizar la exactitud y no discriminación de los datos recopilados. Miyashita (2021), también menciona el riesgo de discriminación involuntaria debido a sesgos incorporados en los sistemas de IA. Ambos estudios sugieren que las medidas regulatorias deben incluir requisitos para el análisis estadístico y auditorías regulares de los sistemas de IA para identificar y mitigar posibles discriminaciones. La implementación de técnicas de análisis de sesgos y la inclusión de evaluaciones de impacto sobre la privacidad y la discriminación en el desarrollo de estos sistemas son cruciales para abordar estos desafíos.

Además, los estudios de Villaronga et al. (2018), exploran los desafíos técnicos para cumplir con los requisitos del derecho al olvido en entornos de IA, destacando que las empresas de tecnología enfrentan dificultades técnicas y consideran imposible cumplir completamente con estos objetivos legales. Estos desafíos técnicos y legales resaltan la necesidad de un enfoque interdisciplinario para desarrollar soluciones efectivas. Las medidas regulatorias podrían incluir el desarrollo de nuevas tecnologías que faciliten la eliminación de datos y la creación de marcos legales que consideren las limitaciones técnicas actuales.

En cuanto al impacto social y económico de la IA, Abe & Eurallyah (2022), se centran en el impacto de la IA en el mercado laboral y los derechos humanos en África, señalando que los sistemas de vigilancia limitan la privacidad y que la automatización podría resultar en una pérdida significativa de empleos. Estos hallazgos sugieren que las regulaciones deben considerar no solo la protección de la privacidad, sino también el impacto social y económico de la IA. Es necesario desarrollar políticas que equilibren la innovación tecnológica con la protección de los derechos fundamentales y la promoción de oportunidades laborales. Además, Brand (2022), plantea que muchos documentos éticos de IA resaltan la transparencia y la privacidad como principios clave. Se observó que varios documentos también enfatizan la responsabilidad, la justicia y la no causación de daño. Estos resultados indican que la mayoría de los documentos éticos de IA se centran en el impacto en los derechos humanos. Este estudio se aplicó a nivel internacional, específicamente en Sudáfrica, abarcando diversas iniciativas regulatorias y éticas en el uso de la IA en gobiernos de diferentes países de este continente, lo que destaca la relevancia global de abordar los desafíos éticos y legales en este ámbito.

Finalmente, estudios como el de Gorbalinskiy et al. (2023) y Autili et al. (2019), sugieren la importancia de un marco legal robusto y el desarrollo de soluciones tecnológicas éticas. Gorbalinskiy propone el desarrollo de aspectos jurídicos de la protección de los derechos humanos en el contexto de la IA, mientras que Autili y sus colegas demuestran la efectividad de herramientas como EXOSOUL en mejorar la protección de datos personales y la conciencia ética. EXOSOUL, también conocido como EXOALMA en español, es una herramienta que crea un exoesqueleto de software diseñado para gestionar las preferencias éticas y de privacidad de los usuarios en el mundo digital. Este exoesqueleto encapsula los datos personales con reglas que gobiernan su creación, uso y destrucción según las preferencias del propietario, promoviendo así la transparencia y el control sobre los datos personales. Estos enfoques proactivos, que empoderan a los individuos para tomar decisiones informadas y proteger sus derechos digitales, deben ser integrados en las medidas regulatorias.

También, existen varias medidas regulatorias en vigencia para proteger la privacidad de los usuarios frente a estas tecnologías. Aunque existen marcos regulatorios como el RGPD en Europa, estos a menudo se quedan cortos frente a las complejidades introducidas por la IA. Villaronga et al. (2018), argumentan que las regulaciones existentes no abordan adecuadamente las complejidades introducidas por la IA. lo que sugiere la necesidad de una mayor actualización y adaptación de las leyes actuales para proteger de manera efectiva la privacidad de los usuarios en un mundo cada vez más dominado por la inteligencia artificial. Además, es fundamental que los gobiernos y las organizaciones trabajen en conjunto para desarrollar regulaciones más específicas y efectivas que aborden los desafíos éticos y legales planteados por el uso creciente de la IA. En este sentido, es crucial establecer estándares claros y mecanismos de supervisión para garantizar que la IA se utilice de manera ética y responsable en todos los sectores. De lo contrario, existe el riesgo de que se produzcan violaciones de la privacidad y otros problemas éticos que podrían socavar la confianza en esta tecnología emergente.

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD) es la principal regulación para garantizar la privacidad y la integridad de los datos personales de los ciudadanos. Esta ley, inspirada en el RGPD, establece principios fundamentales para el tratamiento transparente, justo y seguro de los datos personales e introduce la figura del Delegado de Protección de Datos (DPO) (Rodríguez Ayuso, 2020). La Constitución del Ecuador de 2008 también garantiza diversos derechos fundamentales relacionados con la privacidad y la protección de datos personales, reforzando el compromiso del Estado con la protección de la privacidad de sus ciudadanos.

En otros países de Latinoamérica, como Brasil y Chile, se han promulgado leyes similares inspiradas en el RGPD para proteger la privacidad de los datos personales. La Ley General de Datos Personales de

Brasil (LGPD) y las recientes reformas respecto al uso ético de la inteligencia artificial en la constitución chilena reflejan un esfuerzo continuo por adaptar las mejores prácticas internacionales en materia de protección de datos (Contreras, 2020). A pesar de estos avances, es evidente que las regulaciones deben seguir evolucionando para abordar los nuevos desafíos presentados por la IA. En mi interpretación, la IA, sin duda, viola el derecho a la privacidad en las redes sociales, y las actuales medidas regulatorias, aunque necesarias, deben ser continuamente reforzadas y adaptadas para proteger eficazmente los derechos de los usuarios en el entorno digital. A pesar de abordar diferentes aspectos de esta problemática, todos coinciden en la necesidad urgente de una regulación más efectiva y adaptada a las capacidades tecnológicas emergentes. La comparación entre los estudios resalta una preocupación común: la IA, sin las salvaguardas adecuadas, puede facilitar violaciones de privacidad a una escala sin precedentes.

En definitiva, los estudios analizados coinciden en la necesidad de garantizar la transparencia, el consentimiento informado y la protección contra la discriminación algorítmica. Las medidas regulatorias vigentes deben evolucionar para abordar estos desafíos y asegurar un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales de los individuos. La implementación de soluciones tecnológicas éticas y centradas en la privacidad, como el software EXOSOUL, demuestra la efectividad de enfoques proactivos para empoderar a los individuos en la protección de sus derechos digitales. La evolución de las políticas de privacidad y la inclusión de evaluaciones de impacto ético en el desarrollo de la IA son pasos esenciales para avanzar hacia una regulación más efectiva y justa.

De este modo, las violaciones de privacidad como la creación de identidades falsas y hackeos debido a la sofisticación de los algoritmos de IA y la falta de regulaciones adecuadas. La capacidad de la IA para generar perfiles falsos y realizar hackeos con alta precisión ha crecido exponencialmente, facilitada por el hecho de que los términos y condiciones de las plataformas sociales a menudo no son completamente entendidos por los usuarios. Esta situación pone a los usuarios en una posición vulnerable, donde deben aceptar términos que permiten un amplio uso de sus datos personales sin tener la opción de negarse. La evolución de las redes sociales ha mostrado que, en el pasado, la información y el consentimiento informado no eran tan violados como hoy en día. Antes, los usuarios podían entender y consentir más fácilmente el uso de sus datos. Hoy, las redes sociales no permiten negar los términos de aceptación de consentimiento sin perder el acceso a la funcionalidad completa de las plataformas, lo que agrava la situación. Es crucial que las plataformas mejoren la transparencia y la comprensión de estos términos para proteger la privacidad de los usuarios de manera efectiva. A medida que la tecnología avanza, las regulaciones se deben adaptar para abordar estos desafíos éticos y garantizar que los derechos de los usuarios sean respetados.

Los resultados de los artículos revisados destacan una preocupación universal sobre las implicaciones éticas y legales de la IA en la privacidad. Raab (2020) y Lamchek (2023) ilustran cómo las directrices actuales aún luchan por mantenerse al día con las tecnologías emergentes que operan a través de las redes sociales. Kosta (2022), señala que los desafíos planteados por la vigilancia algorítmica y la acumulación de datos requieren un enfoque normativo renovado. Estos estudios subrayan la necesidad de políticas dinámicas que puedan adaptarse rápidamente a los cambios tecnológicos. También se resalta una falta de coherencia en la aplicación de las regulaciones existentes. Van Bekkum & Borgesius (2021), discuten que, a pesar de esfuerzos legislativos como el RGPD, estas medidas son insuficientes para abordar todas las formas en que la IA puede explotar los datos personales. Miyashita (2021), refuerza este punto al analizar el caso japonés, demostrando que incluso en contextos con fuertes tradiciones en la protección de datos, existen brechas significativas. Estos hallazgos indican que las regulaciones actuales no son lo suficientemente robustas para enfrentar los desafíos presentados por la IA.

Finalmente, es importante mencionar que la cuestión de la privacidad en las redes sociales y la inteligencia artificial (IA) es indudablemente compleja. Los términos y condiciones de uso de estas plataformas son extensos y, a menudo, invasivos, permitiendo a las empresas recolectar, analizar y utilizar datos personales de maneras que muchos usuarios podrían considerar intrusivas. Sin embargo, se destaca que la aceptación de estos términos es voluntaria. Los usuarios eligen aceptar estas condiciones al decidir utilizar las plataformas, conscientes o no de las implicaciones.

Un aspecto crucial en este debate es que la mayoría de los usuarios no dedican tiempo a leer estos términos y condiciones. Esta omisión se debe en parte a la longitud y complejidad de los documentos, pero también refleja una falta de responsabilidad ética y moral. Muchos usuarios prefieren disfrutar de los beneficios de las redes sociales sin interrupciones, pasando por alto las posibles consecuencias para su privacidad. Sin embargo, es importante recordar que, al aceptar estos términos y condiciones, se están otorgando ciertos derechos a las plataformas para recopilar y utilizar datos personales. Los usuarios se deben informar sobre cómo proteger su privacidad en línea y tomar decisiones conscientes respecto a qué información comparten en internet. Además, revisar periódicamente la configuración de privacidad en las redes sociales y limitar la cantidad de información personal que se comparte. En última instancia, la

responsabilidad recae en cada individuo para proteger su privacidad en línea y tomar medidas proactivas para garantizar su seguridad digital.

La privacidad en las redes sociales y la IA no es solo un problema tecnológico o de políticas corporativas, sino también un reflejo de las decisiones y prioridades de los usuarios. A menudo se quejan de las invasiones de privacidad, pero son los usuarios quienes aceptan los términos sin leerlos y deciden que las ventajas de estar en las redes sociales superan los riesgos. Esta actitud revela una desconexión entre el deseo de privacidad de los usuarios y su disposición para tomar medidas que la protejan. Es importante reflexionar sobre las propias acciones y hábitos en línea para proteger la privacidad de manera más efectiva. De igual manera, educarse sobre las implicaciones de compartir información personal en las redes sociales puede ayudar a los usuarios a tomar decisiones más informadas y conscientes. Algunas medidas que se pueden tomar incluyen revisar y ajustar la configuración de privacidad en las cuentas, limitar la cantidad de información personal que se comparte y ser conscientes de quién tiene acceso a la información. También es fundamental recordar que una vez que algo se comparte en línea, puede ser difícil o imposible de eliminar por completo. Por ello, la problemática de la privacidad en la era de la IA y las redes sociales es multifacética. Si bien las políticas de las plataformas pueden parecer invasivas, también es cierto que los usuarios tienen la responsabilidad de informarse y tomar decisiones conscientes. La ética y la moral juegan un papel crucial en este equilibrio, y es deber de cada individuo encontrar un balance entre el deseo de estar conectados y la necesidad de proteger su privacidad. Se debe reflexionar sobre cómo se utilizan las redes sociales y qué información se comparte, considerando siempre los posibles riesgos y consecuencias. Y abogar por regulaciones más estrictas que protejan la privacidad de los usuarios en un mundo cada vez más digitalizado. Tener en cuenta, ser proactivo en la protección de la privacidad en línea y abogar por leyes que garanticen la seguridad de los datos personales. Al mismo tiempo, es esencial educar a otros sobre los riesgos y beneficios de compartir información en plataformas digitales para fomentar una cultura de responsabilidad y conciencia en línea.

5. Conclusión

La presente investigación ha abordado la injerencia de la IA en la violación de la privacidad de los individuos y en las redes sociales, un tema de creciente relevancia en el contexto digital contemporáneo alegado a la cuarta ola de los DDHH. A través de la revisión sistemática de la literatura en respuesta a el objetivo general de este estudio, la influencia de la IA en las redes sociales y su afectación a los derechos individuales se identificó y analizó las consecuencias de la utilización de la IA en la privacidad, delimitando las características de los datos utilizados por esta tecnología y explorando los aspectos sociales, legales y éticos implicados llegando a exponer que es el mal uso y la no lectura de los términos y condiciones del usuario lo que desemboca en . La metodología implementada permitió responder a las preguntas de investigación, exponiendo las técnicas empleadas por la IA para recolectar y analizar datos personales, las formas en que estas técnicas contribuyen a violaciones de privacidad como la creación de identidades falsas y hackeos; siendo estos los medios principales por los cuales la información y por consecuencia la privacidad de los usuarios sea violada. Las medidas regulatorias vigentes destinadas a proteger la privacidad de los usuarios se han basado en el RGPD, pero regiones como Sudamérica aún son un reto.

Además, se discutieron las implicaciones éticas de estas prácticas, enfatizando la responsabilidad de las plataformas digitales en garantizar la protección de los datos de sus usuarios. Las medidas regulatorias vigentes destinadas a proteger la privacidad de los usuarios se han basado en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece un marco legal riguroso para el manejo de datos personales. Sin embargo, se destacó que regiones como Sudamérica aún enfrentan desafíos significativos en la implementación y el cumplimiento de normativas de privacidad robustas. La falta de regulaciones equivalentes en estas regiones expone a los usuarios a mayores riesgos de explotación y violación de su privacidad.

Por otro lado, existe la necesidad de fortalecer las políticas de privacidad y la educación del usuario sobre la importancia de los términos y condiciones. Las soluciones deben incluir no solo mejoras tecnológicas para la protección de datos, como la implementación de algoritmos más seguros y técnicas avanzadas de cifrado, sino también esfuerzos legislativos y educativos que promuevan una mayor conciencia y comprensión entre los usuarios sobre cómo se utilizan sus datos. Es crucial que las plataformas digitales proporcionen términos y condiciones claros y comprensibles, evitando el uso de lenguaje técnico y legal complejo que dificulta la comprensión por parte del usuario promedio. En este sentido, los esfuerzos legislativos deben centrarse en la creación y aplicación de normativas que obliguen a las empresas a ser transparentes en sus prácticas de recolección y uso de datos. Esto incluye la implementación de auditorías regulares y la imposición de sanciones significativas para las organizaciones que violen las regulaciones de privacidad. A nivel educativo, es fundamental integrar la alfabetización digital en los currículos escolares

y realizar campañas de sensibilización para todas las edades, enseñando a los individuos cómo proteger su información personal en línea y qué prácticas seguir para mantener su privacidad.

Este enfoque holístico es esencial para mitigar los riesgos asociados con la IA en las redes sociales y proteger de manera efectiva los derechos de privacidad en la era digital. Al combinar soluciones tecnológicas avanzadas con marcos regulatorios sólidos y una ciudadanía bien informada, se puede crear un entorno digital más seguro y ético. Las soluciones tecnológicas deben incluir el desarrollo de sistemas de IA transparentes y explicables, que permitan a los usuarios entender cómo se procesan sus datos y cómo se toman las decisiones automatizadas que les afectan. Además, es crucial implementar tecnologías de protección de datos, como el cifrado de extremo a extremo, técnicas de anonimización y herramientas de gestión de consentimiento. Los marcos regulatorios sólidos deben garantizar que las leyes y políticas de protección de datos estén actualizadas y sean adecuadas para enfrentar los desafíos emergentes de la IA. Esto incluye la creación de normativas específicas para la IA que aborden cuestiones como la responsabilidad algorítmica, la transparencia y la rendición de cuentas. Los reguladores deben trabajar de la mano con expertos en tecnología y ética para desarrollar directrices que aseguren el uso responsable y seguro de la IA.

Con esto, la educación del usuario es igualmente crucial. Una ciudadanía bien informada sobre sus derechos de privacidad y las prácticas de protección de datos puede tomar decisiones más conscientes y proactivas. Es necesario promover la alfabetización digital y la concienciación sobre la privacidad desde una edad temprana, incorporando estos temas en los currículos escolares y ofreciendo recursos educativos accesibles para todas las edades. Las campañas públicas de sensibilización pueden ayudar a aumentar la comprensión sobre cómo se utilizan los datos personales y cómo protegerlos. La contribución de esta investigación radica en su enfoque integral y actualizado sobre el uso de la IA, redes sociales y sus consecuencias en la privacidad. A través del análisis de 90 artículos seleccionados, se ha proporcionado una visión detallada de las prácticas actuales y los desafíos emergentes en este ámbito. Además, se ha subrayado la importancia de establecer marcos regulatorios robustos y transparentes, como el Reglamento General de Protección de Datos en Europa y la Ley Orgánica de Protección de Datos Personales en Ecuador, por mencionar algunos, que protejan los derechos de privacidad en un entorno digital cada vez más complejo.

Asimismo, este estudio ha resaltado la necesidad de una ética informática sólida y del consentimiento informado como pilares para proteger la autonomía y la integridad del individuo en el uso de las redes sociales. Una ética informática robusta debe ser integral, abarcando desde la etapa de diseño y desarrollo de las tecnologías de IA hasta su implementación y uso. Los desarrolladores y las empresas tecnológicas deben adherirse a principios éticos que prioricen la privacidad, la seguridad y el bienestar de los usuarios. Esto incluye la creación de algoritmos que no solo sean eficientes, sino también justos y transparentes, evitando cualquier forma de discriminación o sesgo.

El consentimiento informado es igualmente crucial. Los usuarios deben ser plenamente conscientes de cómo se recopilan, utilizan y almacenan sus datos, y deben tener la capacidad de dar o retirar su consentimiento de manera clara y sencilla. Las plataformas de redes sociales deben esforzarse por presentar sus políticas de privacidad y términos de servicio de manera accesible y comprensible, eliminando el lenguaje técnico y legal complicado que a menudo confunde a los usuarios. El consentimiento informado no debe ser un trámite burocrático, sino un proceso continuo y significativo que empodere a los usuarios para tomar decisiones informadas sobre su información personal.

Las implicaciones éticas y sociales de la IA en la privacidad individual requieren una atención continua y un enfoque multidisciplinario para garantizar que la evolución tecnológica beneficie a la sociedad sin comprometer los derechos fundamentales. Esto implica la colaboración entre tecnólogos, legisladores, académicos, defensores de la privacidad y otros actores relevantes para abordar los desafíos éticos de manera integral. Los comités de ética y las auditorías externas pueden desempeñar un papel importante en la supervisión de las prácticas de IA, asegurando que se respeten los estándares éticos y se protejan los derechos de los individuos.

Además, es esencial considerar las diversas perspectivas y contextos culturales en la discusión sobre la privacidad y la ética de la IA. Lo que puede ser considerado aceptable en una cultura o región puede no serlo en otra, por lo que es fundamental adoptar un enfoque inclusivo y respetuoso de las diferencias culturales. La participación de diversos grupos de interés en el desarrollo y la regulación de las tecnologías de IA puede ayudar a asegurar que se consideren y respeten estas variaciones. La educación y la concienciación pública también juegan un papel vital en este contexto. Al aumentar la alfabetización digital y la comprensión de los derechos de privacidad, los individuos pueden participar de manera más activa y crítica en el ecosistema digital. Programas educativos, talleres y campañas de sensibilización pueden ayudar

a equipar a los usuarios con las herramientas y el conocimiento necesarios para proteger su privacidad y ejercer sus derechos.

6. Referencias

Abe, O., & Eurallyah, A. J. (2022). Regulating Artificial Intelligence through a human rights-based approach in Africa. *African Journal of Legal Studies*, 22.

Adams, C., Pente, P., Lemermeyer, G., & Rockwell, G. (2023). Computers and Education : Artificial Intelligence Ethical principles for artificial intelligence in K-12 education. *Computers and Education: Artificial Intelligence*, *4*(April 2022), 100131. https://doi.org/10.1016/j.caeai.2023.100131

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2020). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *Information Society*, *37*(2). https://doi.org/10.1080/01972243.2020.1870596

Albornoz, M. M. (2022). Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina? *Latin American Law Review*, *9*. https://doi.org/10.29263/lar09.2022.08

Aloisi, A., & De Stefano, V. (2023). Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens. *European Labour Law Journal*, *14*(2), 283–307. https://doi.org/10.1177/20319525231167982

Alston, P., & Gillespie, C. (2012). Global human rights monitoring, new technologies, and the politics of information. *European Journal of International Law*, *23*(4). https://doi.org/10.1093/ejil/chs073

Álvarez Caro, M., & Piñar Mañas, J. L. (2015). Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital. *Doxa Comunicación: Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales, ISSN 1696-019X, Nº. 21, 2015, Págs. 226-227*, *21*.

Andrés, M. B. (2022). The regulation of data protection law in the United States: towards an American GDPR. *Cuadernos de Derecho Transnacional*, *14*(2). https://doi.org/10.20318/cdt.2022.7181

Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador 2008 - Reformada*. https://www.asambleanacional.gob.ec/es/contenido/constitucion-de-la-republica-del-ecuador-2008-reformada](https://www.asambleanacional.gob.ec/es/contenido/constitucion-de-la-republic

Codigo Orgánico Integral Penal del Ecuador, Registro Oficial - Ógano del Gobierno del Ecuador (2021).

Autili, M., Ruscio, D. D. I., Inverardi, P., Pelliccione, P., & Tivoli, M. (2019). *A Software Exoskeleton to Protect and Support Citizen ' s Ethics and Privacy in the Digital World*. *7*.

Beauchamp, T. L., & Childress, J. F. (2009). Principles of Biomedical Ethics: Respect for Autonomy. In *Angewandte Chemie International Edition*, *6(11)*, *951–952*.

Bernal, C. (2023). *I•con (2022),*. *20*(4), 1431–1446. https://watermark.silverchair.com/moac099.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAA00wggNJBgkqhkiG9w0BBwagggM6MIIDNgIBADCCAy8GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMhhy8gUHFZmSKeMlaAgEQgIIDAEj7dl2BbSQsROY1C6eIhEGx8koVpVif8AZCQaghGyklfC4

Biesaga, M., Domaradzka, A., & Roszczyn, M. (2023). *The effect of the pandemic on European narratives on smart cities and surveillance*. *60*(10), 1894–1914. https://doi.org/10.1177/00420980221138317

Bilisli;, Y., & Tuzcu, H. (2021). The Effects of COVID-19 Pandemic on Social Media Usage in the Context of Uses and Gratification Approach. *Revista de Estudios de Comunicación de Turquía*, *37*, 329–344. https://doi.org/10.17829/turcom.861836

Bizberg, I. (1989). Individuo, identidad y sujeto. *Estudios Sociológicos*, *7*(21).

Bobbio, N. (1951). ¿Es la seguridad jurídica un mito? *Revista Internacional de Filosofía Del Derecho*, *28*.

Bosque, L., & Villan, M. A. (2018). Datos personales, marketing digital y los derechos de los ciudadanos

de América Latina. *Ponencias de La VI Congreso Internacional de Ciencias Sociales [Proceedings of the VI International Congress of Social Sciences]*.

Bossmann, J. (2016). Top 9 ethical issues in artificial intelligence. *World Economic Forum*.

Bowser, B. A., Sloan, M., Michelucci, P., Pauwels, E., Chiappa, S., Gillam, T. P. S., Floridi, L., Taddeo, M., Turilli, M., Brundage, M., Avin, S., Clark, J., Allen, G. C., Flynn, C., Farquhar, S., Crootof, R., Bryson, J., By, U., Re, B. A. N. G. A. L. O., … Protection, G. D. (2017). Artificial Intelligence : A Policy-Oriented Introduction. *Wilson Briefs*, *40*(October).

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1). https://doi.org/10.1111/j.1083-6101.2007.00393.x

Brand, D. J. (2022). Responsible Artificial Intelligence in Government: Development of a Legal Framework for South Africa. *EJournal of EDemocracy and Open Government*, *14*(1), 130–150. https://doi.org/10.29379/jedem.v14i1.678

ByteDance. (2023). *ByteDance Company Profile*. https://www.bytedance.com/en/

Cannataci, J. A., Pia, J., & Bonnici, M. (2010). *International Review of Law , Computers & Technology The end of the purpose-specification principle in data protection ? October 2014*, 37–41. https://doi.org/10.1080/13600861003637693

Cardiell, L. (2021). *" A ROBOT IS WATCHING YOU ": HUMANOID ROBOTS AND THE DIFFERENT IMPACTS ON*. 247–278. https://doi.org/10.5817/MUJLT2021-2-5

Carlos, R., Morán, D., Del Carmen, E., & Corzo, A. (2023). *DESAFÍOS ÉTICOS DE LA INTELIGENCIA ARTIFICIAL: IMPLICACIONES PARA LA SOCIEDAD Y LA ECONOMÍA ETHICAL CHALLENGES OF ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR SOCIETY AND THE ECONOMY*. https://orcid.org/0000-0003-3181-8801

Castillo Parrilla, J. A. (2023). Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial. *Derecho Privado y Constitución*, *43*, 53–88. https://doi.org/10.18042/cepc/dpc.43.02

Catalini, M. P. De. (1944). La teoría egológica de Carlos Cossio y el tridimensionalismo jurídico de Miguel Reale. *Cuyo: Anuario de Filosofía Argentina y Americana*, *8*, 49–90.

CCPA. (2024). *California Consumer Privacy Act*. https://oag.ca.gov/privacy/ccpa

Center, P. R. (2021). *Teens, Social Media and Technology 2022*. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

Center, P. R. (2024). *Social Media Fact Sheet*. https://www.pewresearch.org/internet/fact-sheet/social-media/

Chander, A. (2017). The Racist Algorithm? *Michigan Law Review*, *115.6*. https://doi.org/10.36644/mlr.115.6.racist

Civil, C. (2005). *Código civil*. https://www.etapa.net.ec/Portals/0/TRANSPARENCIA/Literal-a2/CODIGO-CIVIL.pdf

Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios Constitucionales*, *18*(2). https://doi.org/10.4067/s0718-52002020000200087

Cruz, B. S., & Dias, M. de O. (2022). Does digital privacy really exist? When the consumer is the product. *Asian Journal of Economics and Business Management*, *1*(1). https://doi.org/10.53402/ajebm.v1i1.53

Cukier, M.-S. & K. (2017). Big data - la revolución de los datos masivos. In *Editorial Houghton Mifflin Harcourt*. https://catedradatos.com.ar/media/3.-Big-data.-La-revolucion-de-los-datos-masivos-Noema-Spanish-Edition-Viktor-Mayer-Schonberger-Kenneth-Cukier.pdf

Devia, A. (2019). *la inteligencia artificial , el*. *2017*, 5–23.

Durán Ramírez, M. F., & Zamora Vázquez, A. F. (2023). Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. *MQRInvestigar*, *7*(1). https://doi.org/10.56048/mqr20225.7.1.2023.330-343

Duties, G., Information, C. P., Information, D. P., Inaccurate, C., Information, P., What, K., Information, P., Collected, B., Information, A. P., What, K., Information, P., Out, O., Information, P., Use, L., Information, S. P., Retaliation, N., Opt, F., Rights, O., Requirements, D., … Provisions, C. (2024). *CALIFORNIA CONSUMER PRIVACY ACT OF 2018*. *April*, 1–63.

Dworkin, R. (1986). *Law's Empire (1986)* (p. 470).

Education, T. H. (2022). *THE World University Rankings 2023*. https://www.timeshighereducation.com/world-university-rankings/2023/world-ranking

Emanuel, E. J. (2014). *Reinventing American Health Care*. https://www.researchgate.net/publication/309022464_Reinventing_American_Health_Care_How_the_Affordable_Care_Act_Will_Improve_Our_Terribly_Complex_Blatantly_Unjust_Outrageously_Expensive_Grossly_Inefficient_Error_Prone_System

Enríquez Álvarez, L. F. (2020). La Visión de América Latina sobre el Reglamento General de Protección de Datos. *Comentario Internacional*. https://doi.org/10.32719/26312549.2019.19.4

Espinosa, C. (2022). *Ecuador is building its future on data (protection)*. https://inplp.com/latest-news/article/ecuador-is-building-its-future-on-data-protection/

Europa, C. de. (2024). *The European Convention on Human Rights*. https://www.coe.int/es/web/compass/the-european-convention-on-human-rights-and-its-protocols

Facebook. (2023). *Data Policy*. https://www.facebook.com/policy.php

Ferrer Sapena, A., & Sánchez Pérez, E. (2013). Open data, big data: ¿hacia dónde nos dirigimos? *Anuario ThinkEPI*, *7*.

Flores, J., Morán, J., & Rodríguez, J. (2007). Sitios de redes sociales: Definición, Historia y Conocimiento. Journal of Computer–Mediated Communication, 12(1). *Journal of Computer–Mediated Communication.*, *12*.

Floridi, L. (2023). The Ethics of Artificial Intelligence. In *The Ethics of Artificial Intelligence*. https://doi.org/10.1093/oso/9780198883098.001.0001

Fowler, G. A. (2020). *TikTok's Woes Multiply as Criticism Over China Ties Mounts*. ttps://www.washingtonpost.com/technology/2020/07/07/tiktok-security-threat-china/

Frenkel, S., & Alba, D. (2020). *Surge of Virus Misinformation Stumps Facebook and Twitter*. https://www.nytimes.com/2020/03/08/technology/coronavirus-misinformation-social-media.html

Frigerio, C. (2018). Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho. *Revista Chilena de Derecho y Tecnología*, *7*(2). https://doi.org/10.5354/0719-2584.2018.50578

García Carrasco, J. (1994). ¿Es necesario un código ético en la informática? *Ensayos: Revista de La Facultad de Educación de Albacete*, *9*.

Gil, E. (2016). Big data, privacidad y protección de datos. In *Agencia Estatal Boletín Oficial del Estado* (Issue June 2016).

Gintis, H., Van Schaik, C., & Boehm, C. (2015). Zoon politikon: The evolutionary origins of human political systems. *Current Anthropology*, *56*(3). https://doi.org/10.1086/681217

Goncalves, M., Hu, Y., Aliagas, I., Cerdá, L. M., Goncalves, M., Hu, Y., Aliagas, I., & Cerdá, L. M. (2024). Neuromarketing algorithms ' consumer privacy and ethical considerations : challenges and opportunities. *Cogent Business & Management*, *11*(1). https://doi.org/10.1080/23311975.2024.2333063

Gorbalinskiy, V., Draliuk, I., Bondarchuk, V., & Serhii Myroslavskyi, V. M. (2023). *Ensuring Human Rights in the Era of Artificial Intelligence: Ukraine and Practice of ECHR*. *38*(3), 519–538. https://doi.org/10.20473/ydk.v38i3.45134

Gruyter, D. (2022). Fundamentación de la metafísica de las costumbres. In *Crítica de la razón pura (1ª ed.). Prolegómenos. Bases de la metafísica de la ética. Inicios metafísicos de las ciencias naturales.* https://doi.org/10.1515/9783112610060-026

Guibert Ucín, J. M. (1998). ¿ Qué es la ética de la informática? In *Tomo* (Vol. 237).

Haitsma, L. M. (2023). Regulating algorithmic discrimination through adjudication: the Court of Justice of the European Union on discrimination in algorithmic profiling based on PNR data. *Frontiers in Political Science*, *5*. https://doi.org/10.3389/fpos.2023.1232601

Hoxhaj, O. (2023). *ETHICAL IMPLICATIONS AND HUMAN RIGHTS VIOLATIONS IN*.

Hu, M. (2020). Cambridge Analytica's black box. In *Big Data and Society* (Vol. 7, Issue 2). https://doi.org/10.1177/2053951720938091

Hueso, L. C., & Valencia, U. De. (2020). *y aplicaciones contra la COVID-19 : privacidad y protección de datos*. *31*, 1–17.

Ildefonso, E., & Aruquipa, M. (2020). *Postgrado en Informática Mapeo del Reglamento TIC boliviano, RGPD y Estándares RIPD en materia de Protección de Datos Personales*.

Instagram. (2023). *Data Policy*. https://privacycenter.instagram.com/policy/?entry_point=ig_help_center_data_policy_redirect

International, A. (2019). *The Great Hack: Facebook, Cambridge Analytica, and Data Exploitation*. https://www.amnesty.org/es/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/

Keltner, D., Kogan, A., Piff, P. K., & Saturn, S. R. (2014). The sociocultural appraisals, values, and emotions (SAVE) framework of prosociality: Core processes from gene to meme. In *Annual Review of Psychology* (Vol. 65). https://doi.org/10.1146/annurev-psych-010213-115054

Khan, G. F. (2017). Social Media Risks Management. In *Social Media for Government*. https://doi.org/10.1007/978-981-10-2942-4_8

Kim, T. W., & Routledge, B. R. (2022). Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach. *Business Ethics Quarterly*, *32*(1), 75–102. https://doi.org/10.1017/beq.2021.3

Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation and Governance*, *16*(1), 212–224. https://doi.org/10.1111/rego.12331

Kubler, K. (2016). The Black Box Society: the secret algorithms that control money and information. *Information, Communication & Society*, *19*(12). https://doi.org/10.1080/1369118x.2016.1160142

Lamchek, J. S. (2023). Ensuring Data Science and Its Applications Benefit Humanity: Data Monetization and the Right to Science. *Human Rights Law Review*, *23*(3), 1–23. https://doi.org/10.1093/hrlr/ngad018

Lane, L. (2022). Clarifying Human Rights Standards Through Artificial Intelligence Initiatives. *International and Comparative Law Quarterly*, *71*(4), 915–944. https://doi.org/10.1017/S0020589322000380

Leach, N. (2022). Architecture in the Age of Artificial Intelligence, An Introduction to AI for Architects. In *Architecture in the Age of Artificial Intelligence*.

LGPD. (2018). *Ley General de Protección de Datos*. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Licklider & Taylor, R.W, J. C. R. (1968). The computer as a communication device. *Science& Technology*, *76*.

Locke, J. (1690). *Second Treatise On Civil Government*. Constitution Society.

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Revista d'Internet, Dret i Política (IDP)*, *5*.

Mayor-Schonberger, V., & Cukier, K. (1981). a Revolution That Big Data Will Transform How We Live, Work, and Think. In *Journal of Chemical Information and Modeling* (Vol. 53, Issue 9).

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1956). *A proposal for the Darmouth summer research project on artificial intelligence*. https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth

McNamee, R. (2019). How to Fix Social Media Before It's Too Late an Early Investor on How Facebook Lost Its Way. (Cover story). *TIME Magazine*, *193*(3).

Medina Guerrero, M. (2022). El derecho a conocer los algoritmos utilizados en la toma de decisiones.

Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales. *Teoría y Realidad Constitucional*, *49*. https://doi.org/10.5944/trc.49.2022.33847

Miernicki, M., & Ng, I. (2021). Artificial intelligence and moral rights. *AI and Society*, *36*(1), 319–329. https://doi.org/10.1007/s00146-020-01027-6

Milossi, M., Alexandropoulou-egyptiadou, E., & Psannis, K. E. (2021). *AI Ethics : Algorithmic Determinism or Self-Determination ? The GPDR Approach*. 58455–58466. https://doi.org/10.1109/ACCESS.2021.3072782

Miyashita, H. (2021). *Human-centric Data Protection Laws and Policies : A Lesson from Japan Author name and affiliation / Corresponding author Hiroshi Miyashita LL . D . Associate Professor Faculty of Policy Studies Address Chuo University , Faculty of Policy Studies Human-cen*. 0–20.

Montori, V. M., Guyatt, G. H., Cosgrove, L., Krimsky, S., Wheeler, E. E., Kaitz, J., Greenspan, S. B., DiPentima, N. L., Thompson, D. F., Rising, K., Bacchetti, P., Bero, L., Campbell, E. G., Gruen, R. L., Mountford, J., Miller, L. G., Cleary, P. D., Blumenthal, D., Grande, D., … Annas, G. J. (2013). Declaración de Helsinki de la Asosicación Medical Mundial. Principios éticos para las investigaciones médicas en seres humanos, enmendada por la Asamblea General, Fortaleza, Brasil, Octubre 2013. *BMJ (Clinical Research Ed.)*, *14*(1).

Moratinos, G. L., & Parrilla, J. A. C. (2020). *Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos : El caso SyRI*. *9*, 207–226. https://doi.org/10.5354/0719-2584.2020.56843

Morozov, E. (2011). Response to Philip N. Howard's review of The Net Delusion: The Dark Side of Internet Freedom. *Perspectives on Politics*, *9*(4). https://doi.org/10.1017/S1537592711004026

Niklas, J. (2021). *What rights matter ? Examining the place of social rights in the EU ' s artificial intelligence policy debate*. *10*.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464). https://doi.org/10.1126/science.aax2342

OKF. (2016). *Open Data Handbook*. https://okfn.org/es/

Pérez, A. F. (2022). *El derecho de la privacidad en los Estados Unidos. Un análisis de los efectos de una nueva política de la privacidad*. https://doi.org/10.14718/9789585133921.2021.2

Platero Alcón, A. (2017). La responsabilidad de las redes sociales: el caso de Ashley Madison. *Boletín Mexicano de Derecho Comparado*, *1*(150). https://doi.org/10.22201/iij.24484873e.2017.150.11839

Platforms, M. (2023). *Meta Privacy Policy*. https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/meta-privacy-policies/

Puccinelli, O. (1999). *El habeas data en indoiberoamerica* (1st ed.). Temis.

Raab, C. D. (2020). Information privacy , impact assessment , and the place of ethics ∗. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *37*, 105404. https://doi.org/10.1016/j.clsr.2020.105404

Rodríguez Ayuso, J. F. (2020). La figura del Data Protection Officer en la contratación pública en España. *Revista Digital de Derecho Administrativo*, *25*. https://doi.org/10.18601/21452946.n25.10

Rodríguez, J. F. R., Núñez, M. P., Romo, A. J., Gómez, M. G., González, S. G. C., Pereyra, B. M., & Felipe, J. A. (2000). The registered population and its characteristics as adjustment element for individualized pharmacy budget allocation. *Atencion Primaria / Sociedad Española de Medicina de Familia y Comunitaria*, *25*(5). https://doi.org/10.1016/S0212-6567(00)78516-7

Roig, A. (2009). E-privacidad y redes sociales. *IDP: Revista de Internet, Derecho y Política = Revista d'Internet, Dret i Política*, *9*.

Rule, J. B., & Greenleaf, G. (2010). *Global Privacy Protection: The First Generation*. Edward Elgar Publishing. https://books.google.com.ec/books?hl=es&lr=&id=L2I2Lrf1BeYC&oi=fnd&pg=PR1&dq=Global+Privacy+Protection:+The+First+Generation&ots=rSlUh3aPsz&sig=5NAVSU-20xgGBA7verkO2yBDx0k&redir_esc=y#v=onepage&q&f=false

Salas, R. (2000). *Redes Neuronales Artificiales-Rodrigo Salas*.

Samala, A. D., Usmeldi, Taali, Ambiyar, Bojic, L., Indarta, Y., Tsoy, D., Denden, M., Tas, N., & Dewi, I. P. (2023). Metaverse Technologies in Education: A Systematic Literature Review Using PRISMA. *International Journal of Emerging Technologies in Learning*, *18*(5). https://doi.org/10.3991/IJET.V18I05.35501

Samuel, A. . (1959). Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Development*, *3*(3).

Schneble, C. O., Favaretto, M., Elger, B. S., & Shaw, D. M. (2021). Social media terms and conditions and informed consent from children: Ethical analysis. *JMIR Pediatrics and Parenting*, *4*(2). https://doi.org/10.2196/22281

Shaik, T., Tao, X., Higgins, N., Gururajan, R., Li, Y., Zhou, X., & Acharya, U. (2022). *FedStack : Personalized Activity Monitoring using Stacked Federated Learning*.

Silva, N., & Espina, J. (2011). Ética Informática en la Sociedad de la Información. *Revista Venezolana de Gerencia*, *11*(36). https://doi.org/10.31876/revista.v11i36.10441

States, U. (1998). *Children's Online Privacy Protection Act of 1998*. https://www.congress.gov/bill/105th-congress/senate-bill/2326/text

Suárez Xavier, P. R. (2022). The Challenge of the Regulation of Artificial Intelligence in the Judicial System and its Environment. *Revista Juridica Portucalense*, *2*(Special Issue). https://doi.org/10.34625/issn.2183-2705(ne2v2)2022.ic-10

Superintendencia de Industria y Comercio. (2023, June 7). *Superindustria impone la sanción más alta por el indebido tratamiento de datos personales a Claro por su campaña "Amigos que te premian."*

Taddicken, M. (2014). *The ' Privacy Paradox ' in the Social Web : The Impact of Privacy Concerns , Individual Characteristics , and the Perceived Social Relevance on Different Forms of Self-Disclosure 1 ∗*. *19*, 248–273. https://doi.org/10.1111/jcc4.12052

TikTok. (2023). *Privacy Policy*. https://www.tiktok.com/legal/privacy-policy?lang=en

Torres, A., Oliveira Domingues Secretaria Nacional del Consumidor Waldemar Gonçalves Ortunho Junior, J., Pereira Sabbat Joacil Basilio Rael Miriam Wimmer Nairane Farias Rabelo Leitão, A., Correa Cardoso, D., Cristina Rayol dos Santos Sobreira Lopes, M., Maria Braga Maranhão, A., Krastins Jeferson Barbosa Gerentes de Proyecto, A., Schertel Mendes, L., Silva Dias Coordinación Janaina Angelina Teixeira, U., & Silvino Batista Neto Proyecto gráfico diagramación, I. (2018). *Jair Messias Bolsonaro Presidente de la República*. www.gov.br/anpd

Twitter. (2023). *Privacy Policy*. https://twitter.com/en/privacy

Union, E. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Official Journal of the European Communities, L 281, 23 November 1995, Pp. 31-50. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

Unión Europa. (2016). *Reglamento general de protección de datos*.

United Nations. (1948). *United Nations Human Rights Declaration*. Human Rights.

Universities, Q. T. (2023). *QS World University Rankings 2023: Top Global Universities*. https://www.topuniversities.com/qs-world-university-rankings

Van Bekkum, M., & Borgesius, F. Z. (2021). Digital welfare fraud detection and the Dutch SyRI judgment. *European Journal of Social Security*, *23*(4), 323–340. https://doi.org/10.1177/13882627211031257

Van der Walt, E., Eloff, J. H. P., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers and Security*, *78*. https://doi.org/10.1016/j.cose.2018.05.015

Van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication*, *1*(1). https://doi.org/10.12924/mac2013.01010002

Vásquez, C. S., & José Alberto, T. V. (2021). The right to human control: A legal response to artificial intelligence. *Revista Chilena de Derecho y Tecnologia*, *10*(2), 211–228. https://doi.org/10.5354/0719-2584.2021.58745

Vásquez Rodríguez, R. (2022). La responsabilidad proactiva en la normativa peruana de protección de datos personales. *YachaQ Revista de Derecho*, *13*. https://doi.org/10.51343/yq.vi13.913

Vera, C. S. A. (2019). *NADA ES PRIVADO: UN DOCUMENTAL SOBRE CAMBRIDGE ANALYTICA*.

Vercelli, A. (2023). Regulaciones e inteligencias artificiales en Argentina. *InMediaciones de La Comunicación*, *19*(1), 105–135. https://doi.org/10.18861/ic.2024.19.1.3549

Villalba, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *FORO. Revista de Derecho*.

Villaronga, E. F., Kieseberg, P., & Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten. *Computer Law and Security Review*, *34*(2), 304–313. https://doi.org/10.1016/j.clsr.2017.08.007

Vincent C. Müller. (2020). *Ethics of Artificial Intelligence and Robotics*. 1–31. https://philarchive.org/archive/MLLEOA-4v2

Wagner, P. (2021). Data Privacy - The Ethical, Sociological, and Philosophical Effects of Cambridge Analytica. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3782821

Wright, E., Deleuze, G., & Tomlinson, H. (1984). Nietzsche and Philosophy. *Poetics Today*, *5*(4). https://doi.org/10.2307/1772274

Yepes-Nuñez, J. J., Urrútia, G., Romero-García, M., & Alonso-Fernández, S. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Revista Espanola de Cardiologia*, *74*(9), 790–799. https://doi.org/10.1016/j.recesp.2021.06.016

Zhang, Y., Wu, M., Tian, G. Y., Zhang, G., & Lu, J. (2021). *Ethics and privacy of artificial intelligence : Understandings from bibliometrics*. https://doi.org/10.1016/j.knosys.2021.106994

7. Anexos

Anexo 1
Matriz de resultados

Título	Autor	Codificación de las fuentes	Año de publicación	Contenido específico	Base de datos
The right to human control: A legal response to artificial intelligence	Vásquez, CS; Toro-Valend, JA	A1	2021	La IA viola derechos fundamentales; se necesita el derecho al control humano para supervisarla y proteger esos derechos.	Web of Science
Clarifying human rights standards through artificial intelligence initiatives	Lane, L	A2	2022	La IA aumenta la certeza legal en DDHH; se necesita más claridad.	Web of Science
Artificial intelligence and moral rights	Miernicki, M; Ng, I	A3	2021	La Inteligencia artificial y derechos morales	Web of Science
Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten	Villaronga, EF; Kieseberg, P; Li, T	A4	2018	La inteligencia artificial y el derecho al olvido	Web of Science
Regulating Artificial Intelligence through a Human Rights-Based Approach in Africa	Abe, O; Eurallyah, AJ	A5	2022	La IA en África: beneficios y riesgos para los derechos humanos.	Web of Science
The Influence on Human Behavior and the Association of Privacy as Contemporary Issue Concerning the Regulations of Trade on Electronic Devices	Ríos, C	A6	2020	La IA viola derechos; se necesita control humano para protegerlos.	Web of Science
Artificial intelligence for human flourishing - Beyond principles for machine learning	Stahl, BC; Andreou, A; Brey, P; Hatzakis, T; Kirichenko, A; Macnish, K; Shaelou, SL; Patel, A; Ryan, M; Wright, D	A7	2021	Los beneficios y problemas de la IA requieren orientación ética basada en DDHH.	Web of Science
AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach	Milossi, M; Alexandropoulou-Egyptiadou, E; Psannis, KE	A8	2021	La ética de la IA según el RGPD: determinismo algorítmico o autodeterminación.	Web of Science
Algorithmic valoration before human rights and the European Convention on Human Rights and the General Data Protection Regulation: The SyRI case	Moratinos, GL; Parrilla, JAC	A9	2020	Valoración algorítmica y DDHH: Caso SyRI y RGPD	Web of Science

Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholder Guidelines	Fukuda-Parr, S; Gibbons, E	A10	2021	Consenso sobre IA ética: crítica de DDHH a guías voluntarias.	Web of Science
Ethics and privacy of artificial intelligence: Understandings from bibliometrics	Zhang, Y; Wu, MJ; Tian, GY; Zhang, GQ; Lu, J	A11	2021	Ética y privacidad de la IA: perspectivas desde la bibliometría.	Web of Science
ALGORITHMIC INEQUALITIES: HIGH-RISK PRACTICES TO HUMAN RIGHTS	Roig, MJA	A12	2022	Desigualdades algorítmicas: prácticas de alto riesgo para los DDHH.	Web of Science
Regulating Artificial Intelligence in International Investment Law	McLaughlin, M	A13	2023	Regulación de la inteligencia artificial en el derecho internacional de inversiones.	Web of Science
Information privacy, impact assessment, and the place of ethics	Raab, CD	A14	2020	Privacidad de la información, evaluación de impacto y ética.	Web of Science
ARTIFICIAL INTELLIGENCE BIG DATA, AND DIGITAL ERA: A THREAT TO PERSONAL DATA?	Devia, AM	A15	2019	IA y big data amenazan datos personales; se necesita regulación ética.	Web of Science
Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach	Kim, TW; Routledge, BR	A16	2022	Derecho a explicar decisiones algorítmicas: enfoque de confianza	Web of Science
Digital welfare fraud detection and the Dutch SyRI judgment	van Bekkum, M; Borgesius, FZ	A17	2021	Detección de fraude digital y el fallo del caso SyRI en Países Bajos.	Web of Science
Responsible innovation ecosystems: Ethical implications of the application of the ecosystem concept to artificial intelligence	Stahl, BC	A18	2022	Ecosistemas de innovación responsable: implicaciones éticas en la IA	Web of Science
What rights matter? Examining the place of social rights in the EU's artificial intelligence policy debate	Niklas, J; Dencik, L	A19	2021	Derechos sociales son marginales en el debate de política de IA de la UE	Web of Science
Ensuring Data Science and Its Applications Benefit Humanity: Data Monetization and the Right to Science	Lamchek, JS	A20	2023	El derecho a la ciencia exige equilibrar monetización de datos y beneficios humano	Web of Science
Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks	Beduschi, A	A21	2022	La IA puede transformar la acción humanitaria, pero conlleva riesgos significativos	Web of Science
Human-centric data protection laws and policies: A lesson from Japan	Miyashita, H	A22	2021	Protección de datos centrada en el ser humano en Japón destaca la dignidad	Web of Science
Algorithmic state surveillance: Challenging the notion of agency in human rights	Kosta, E	A23	2022	La vigilancia algorítmica estatal desafía la noción de agencia en DDHH	Web of Science

From human resources to human rights: Impact assessments for hiring algorithms	Yam, J; Skorburg, JA	A24	2021	Evaluaciones de impacto para algoritmos de contratación protegen DDHH	Web of Science
Applying the ethics of AI: a systematic review of tools for developing and accessing AI-based systems	Ortega-Bolaños, R; Bernal-Salcedo, J; Ortiz, MG; Sarmiento, JG; Ruz, GA; Tabares-Soto, R	A25	2024	Revisión de herramientas para el desarrollo ético de sistemas de IA	Web of Science
FREEDOM OF THOUGHT: LEGAL PROTECTION FROM MANIPULATION	Harutyunyan, D; Yeremyan, L	A26	2020	Libertad de pensamiento: protección legal contra la manipulación	Web of Science
Neuromarketing algorithms' consumer privacy and ethical considerations: challenges and opportunities	Goncalves, M; Hu, YW; Aliagas, I; Cerdá, LM	A27	2024	Privacidad y ética en neuromarketing: desafíos y oportunidades con IA	Web of Science
FedStack: Personalized activity monitoring using stacked federated learning	Shaik, T; Tao, XH; Higgins, N; Gururajan, R; Li, YF; Zhou, XJ; Acharya, UR	A28	2022	FedStack: Monitoreo personalizado de actividad con aprendizaje federado	Web of Science
A Software Exoskeleton to Protect and Support Citizen's Ethics and Privacy in the Digital World	Autili, M; Di Ruscio, D; Inverardi, P; Pelliccione, P; Tivoli, M	A29	2019	Exoesqueleto de software para proteger la ética y privacidad digital de los ciudadanos	Web of Science
Future Smart Connected Communities to Fight COVID-19 Outbreak	Gupta, D; Bhatt, S; Gupta, M; Tosun, AS	A30	2021	Comunidades inteligentes conectadas para combatir brotes de COVID-19	Web of Science
Why converging technologies need converging international regulation	Helbing, D; Ienca, M	A31	2024	Las tecnologías convergentes requieren regulación internacional unificada por desafíos éticos	Web of Science
Please understand we cannot provide further information: evaluating content and transparency of GDPR-mandated AI disclosures	Wulf, AJ; Seizov, O	A32	2024	Divulgaciones de IA según el RGPD son inadecuadas y poco transparentes	Web of Science
Applying ethics to AI in the workplace: the design of a scorecard for Australian workplace health and safety	Cebulla, A; Szpak, Z; Howell, C; Knight, G; Hussain, S	A33	2023	Diseño de una tarjeta para evaluar riesgos de IA en la salud laboral en Australia.	Web of Science
Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens	Aloisi, A; De Stefano, V	A34	2023	Evaluación comparativa de la regulación de la IA en la UE y Norteamérica	Web of Science
How to Create and Foster Sustainable Smart Cities? Insights on Ethics, Trust, Privacy, Transparency, Incentives, and Success	Riedmann-Streitz, C; Streitz, N; Antona, M; Marcus, A; Margetis, G; Ntoa, S; Rau, PLP; Rosenzweig, E	A35	2024	Creación de ciudades inteligentes sostenibles: ética, confianza y transparencia	Web of Science

Regulating algorithmic discrimination through adjudication: the Court of Justice of the European Union on discrimination in algorithmic profiling based on PNR data	Haitsma, LM	A36	2023	Regulación de la discriminación algorítmica: el TJUE y el perfilado basado en datos PNR	Web of Science
Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis	Khan, HU; Malik, MZ; Nazir, S; Khan, F	A37	2023	Utilización de sistemas biométricos para mejorar la ciberseguridad en el sector bancario: i{análisis sistemático	Web of Science
An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems	Mantelero A.	A38	2021	Metodología basada en evidencias para evaluar el impacto en los DDHH en el desarrollo de sistemas de IA intensivos en datos	Scopus
Legal aspects of artificial intelligence in the employment process	Špadina H.	A39	2023	Aspectos legales de la IA en el proceso de empleo	Scopus
Responsible Artificial Intelligence in Government: Development of a Legal Framework for South Africa	Brand D.J.	A40	2022	IA responsable en el gobierno: desarrollo de un marco legal para Sudáfrica	Scopus
Ensuring Data Science and Its Applications Benefit Humanity: Data Monetization and the Right to Science	Lamchek J.S.	A41	2023	Garantizar que la ciencia de datos beneficie a la humanidad: monetización de datos y derecho a la ciencia	Scopus
Personal Identity in the Metaverse: Challenges and Risks	Mitrushchenkova A.N.	A42	2022	Identidad personal en el metaverso: desafíos y riesgo	Scopus
What rights matter? Examining the place of social rights in the EU's artificial intelligence policy debate	Niklas J.	A43	2021	¿Qué derechos importan? Evaluación de los derechos sociales en la política de IA de la UE	Scopus
Social and Legal Risks of Artificial Intelligence: An Analytical Stu	Al-Tkhayneh K.M.	A44	2023	Riesgos sociales y legales de la IA: un estudio analítico	Scopus
Between risk mitigation and labor rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens	Aloisi A.	A45	2023	Mitigación de riesgos y derechos laborales: regulación transatlántica de IA	Scopus
"Humanity's new frontier": Human rights implications of artificial intelligence and new technologies	Nagy N.	A46	2024	Frontera nueva de la humanidad": implicaciones de DDHH de la IA y nuevas tecnologías	Scopus
Artificial intelligence: a claim for strict liability for human rights violations*	Fernandes Barbosa L.V.	A47	2023	IA: demanda de responsabilidad estricta por violaciones de DDHH	Scopus

From human resources to human rights: Impact assessments for hiring algorithms	Yam J.	A48	2021	De recursos humanos a DDHH: evaluaciones de impacto para algoritmos de contratación	Scopus
Exploring the impacts of artificial intelligence on freedom of religion or belief online	Ashraf C.	A49	2022	Impactos de la IA en la libertad de religión o creencias en línea	Scopus
A Framework for Systematically Applying Humanistic Ethics when Using AI as a Design Material	Dent K.	A50	2019	Marco para aplicar sistemáticamente la ética humanista en el uso de IA como material de diseño	Scopus
The Bayes model for the protection of human interest	Zharova A.	A51	2023	El modelo Bayesiano para la protección de los intereses humanos	Scopus
Contesting border artificial intelligence: Applying the guidance-ethics approach as a responsible design lens	La Fors K.	A52	2022	Cuestionando la inteligencia artificial fronteriza: aplicando el enfoque de ética guía como lente de diseño responsable	Scopus
Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten	Villaronga E.F.	A53	2018	La inteligencia artificial y el derecho al olvido	Scopus
Applying the ethics of AI: a systematic review of tools for developing and accessing AI-based systems	Ortega-Bolaños R.	A54	2024	Revisión de herramientas éticas para desarrollar y evaluar sistemas de IA	Scopus
Towards Industrial Revolution 5.0 and Explainable Artificial Intelligence: Challenges and Opportunities	Taj I.	A55	2022	Hacia la Revolución Industrial 5.0 y la Inteligencia Artificial Explicable: Desafíos y Oportunidades	Scopus
Human Rights Dilemma and International Rule of Law in the Age of Digital Intelligence	Xing A.	A56	2024	Dilema de los Derechos Humanos y el Estado de Derecho Internacional en la Era de la Inteligencia Digital	Scopus
Generative AI and deepfakes: a human rights approach to tackling harmful content	Romero Moreno F.	A57	2024	IA Generativa y Deepfakes: Un enfoque de derechos humanos para abordar contenido dañino	Scopus
Regulating around freedom in the “forum Internum”	Alegre S.	A58	2021	Regulación en torno a la libertad en el "forum internum"	Scopus
Information privacy, impact assessment, and the place of ethics ∗	Raab C.D.	A59	2020	Privacidad de la información, evaluación de impacto y el lugar de la ética	Scopus
REPLIKA AND THE EMOTIONAL ARTIFICIAL INTELLIGENCE COMPANY: The ethical and social challenges of company chatbots	Gutiérrez J.L.M.	A60	2022	REPLIKA Y LA COMPAÑÍA DE INTELIGENCIA ARTIFICIAL EMOCIONAL: Los desafíos éticos y sociales de los chatbots de la empresa	Scopus

Why converging technologies need converging international regulation	Helbing D.	A61	2024	Por qué las tecnologías convergentes necesitan una regulación internacional convergente	Scopus
Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations	Malgieri G.	A62	2019	Toma de decisiones automatizada en los Estados miembros de la UE: El derecho a la explicación y otras “garantías adecuadas” en las legislaciones nacionales	Scopus
Platform Law and Platform Solutions in the Fight against the Pandemic	Altoukhov A.V.	A63	2021	Ley de Plataformas y Soluciones de Plataforma en la Lucha contra la Pandemia	Scopus
FREEDOM AS AN ISSUE IN THE CONTEXT OF TRANSHUMANISM AND ARTIFICIAL INTELLIGENCE, DIGITALIZATION, AND ROBOTICS (AIDR)	Dağ A.	A64	2023	LA LIBERTAD COMO CUESTIÓN EN EL CONTEXTO DEL TRANSHUMANISMO Y LA INTELIGENCIA ARTIFICIAL, DIGITALIZACIÓN Y ROBÓTICA (AIDR)	Scopus
Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective	Deeb-Swihart J.	A65	2022	Tensiones Éticas en Aplicaciones de IA para Abordar la Trata de Personas: Una Perspectiva de Derechos Humanos	Scopus
Applying ethics to AI in the workplace: the design of a scorecard for Australian workplace health and safety	Cebulla A.	A66	2023	Aplicando la ética a la IA en el lugar de trabajo: el diseño de un cuadro de mando para la salud y seguridad en el trabajo en Australia	Scopus
The right to the privacy of personal data in the digital age	Díaz M.F.S.	A67	2023	El derecho a la privacidad de los datos personales en la era digital	Scopus
Artificial intelligence, big data and applications against Covid-19, and privacy and data protection	Hueso L.C.	A68	2020	Inteligencia artificial, big data y aplicaciones contra el Covid-19, y privacidad y protección de datos	Scopus
Artificial intelligence in healthcare: Threats to the fundamental values of our society	Zikmundová K.	A69	2022	La inteligencia artificial en el cuidado de la salud: Amenazas a los valores fundamentales de nuestra sociedad	Scopus
The emergence of “truth machines”? Artificial intelligence approaches to lie detection	Oravec J.A.	A70	2022	La aparición de "máquinas de la verdad": Enfoques de la inteligencia artificial para la detección de mentiras	Scopus
Algorithmic valuation before human rights and the European Convention on Human	Moratinos G.L.	A71	2020	Valoración algorítmica ante los derechos humanos y el Convenio	Scopus

Rights and the General Data Protection Regulation: The SyRI case				Europeo de Derechos Humanos y el Reglamento General de Protección de Datos: El caso SyRI	
Ensuring Human Rights in the Era of Artificial Intelligence: Ukraine and Practice of ECHR	Gorbalinskiy V.	A72	2023	Garantizar los Derechos Humanos en la Era de la Inteligencia Artificial: Ucrania y la práctica del TEDH	Scopus
The right to human control: A legal response to artificial intelligence	Vásquez C.S.	A73	2021	El derecho al control humano: Una respuesta legal a la inteligencia artificial	Scopus
“A robot is watching you”: Humanoid robots and the different impacts on human privacy	Cardiell L.	A74	2021	Un robot te está mirando: Robots humanoides y los diferentes impactos en la privacidad humana	Scopus
Ethical principles for artificial intelligence in K-12 education	Adams C.	A75	2023	Principios éticos para la inteligencia artificial en la educación K-12	Scopus
AI in education: learner choice and fundamental rights	Berendt B.	A76	2020	IA en la educación: elección del alumno y derechos fundamentales	Scopus
Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks	Beduschi A.	A77	2022	Aprovechar el potencial de la inteligencia artificial para la acción humanitaria: Oportunidades y riesgos	Scopus
Regulating Artificial Intelligence through a Human Rights-Based Approach in Africa	Abe O.	A78	2021	Regulación de la Inteligencia Artificial a través de un Enfoque Basado en los Derechos Humanos en África	Scopus
The effect of the pandemic on European narratives on smart cities and surveillance	Biesaga M.	A79	2023	El efecto de la pandemia en las narrativas europeas sobre ciudades inteligentes y vigilancia	Scopus
Research design for an integrated Artificial Intelligence ethical framework	Karatzogianni A.	A80	2021	Diseño de investigación para un marco ético integrado de la Inteligencia Artificial	Scopus
Digital welfare fraud detection and the Dutch SyRI judgment	van Bekkum M.	A81	2021	Detección de fraude en el bienestar digital y el juicio de SyRI en los Países Bajos	Scopus
ETHICAL IMPLICATIONS AND HUMAN RIGHTS VIOLATIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE	Hoxhaj O.	A82	2023	IMPLICACIONES ÉTICAS Y VIOLACIONES DE DERECHOS HUMANOS EN LA ERA DE LA INTELIGENCIA ARTIFICIAL	Scopus
Responsible living labs: what can go wrong?	Habibipour A.	A83	2024	Laboratorios vivos responsables: ¿qué puede salir mal?	Scopus

Emerging Consensus on ‘Ethical AI’: Human Rights Critique of Stakeholder Guidelines	Fukuda-Parr S.	A84	2021	Consenso emergente sobre 'IA ética': Crítica de derechos humanos a las directrices de las partes interesadas	Scopus
CLARIFYING HUMAN RIGHTS STANDARDS THROUGH ARTIFICIAL INTELLIGENCE INITIATIVES	Lane L.	A85	2022	ACLARAR LOS ESTÁNDARES DE DERECHOS HUMANOS A TRAVÉS DE INICIATIVAS DE INTELIGENCIA ARTIFICIAL	Scopus
Delineating privacy aspects of COVID tracing applications embedded with proximity measurement technologies & digital technologies	Saheb T.	A86	2022	Delimitación de aspectos de privacidad de las aplicaciones de rastreo de COVID integradas con tecnologías de medición de proximidad y tecnologías digitales	Scopus
Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach	Kim T.W.	A87	2022	Por qué debe existir un derecho a una explicación de la toma de decisiones algorítmica: Un enfoque basado en la confianza	Scopus
How to Create and Foster Sustainable Smart Cities? Insights on Ethics, Trust, Privacy, Transparency, Incentives, and Success	Riedmann-Streitz C.	A88	2024	Cómo crear y fomentar ciudades inteligentes sostenibles: ideas sobre ética, confianza, privacidad, transparencia, incentivos y éxito	Scopus
Video Surveillance and Privacy: A Solvable Paradox?	Cucchiara R.	A89	2024	Vigilancia por video y privacidad: ¿Una paradoja resoluble?	Scopus
Collaboration among recruiters and artificial intelligence: removing human prejudices in employment	Chen Z.	A90	2023	Colaboración entre reclutadores e inteligencia artificial: eliminando los prejuicios humanos en el empleo	Scopus