University of Azuay

Faculty of Law

School of International Studies

THE INTERFERENCE OF ARTIFICIAL INTELLIGENCE IN THE VIOLATION OF PRIVACY ON SOCIAL MEDIA.

Author:

Renata Nicole Lozano Figueroa

Director:

Dr. Ana Isabel Malo Martínez

Cuenca-Ecuador
2024

DEDICATION

I start by dedicating this to my family, whose unconditional love and constant support have been my greatest inspiration and strength throughout my life. To my mother, who has instilled in me the values of dedication, faith, genuine love, and courage. She has also always stood by my side, shaping me into the woman I am today. And to my father, whose perseverance and hard work have been a guiding light in achieving my goals. I deeply appreciate the sacrifice and effort my parents have made to make my studies possible. To my siblings, whose companionship has enriched my life with joy and remarkable memories, I am grateful beyond measure for the blessing of growing up with them. To my grandparents, who have illuminated my path with their wisdom. Especially to Papito Julio, who is now resting in peace but always alive in my heart, I hope to have made him proud. To my best friends, whether near or far, offering their love and encouragement through thick and thin, turning friendships into family. To everyone who has contributed in some way to my academic and personal development, I dedicate this achievement with deep gratitude and affection.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to all the people who have made this academic article possible.

I deeply appreciate the support provided by my parents and siblings, who have been my greatest source of strength and encouragement throughout all time. Thanks to their unconditional love, support and sacrifice, I have found the determination and perseverance necessary to achieve my goals.

I wish to express my profound gratitude to a person who has played a crucial role in this process. To my thesis advisor, Dr. Ana Isabel Malo, for her patience and constant assistance throughout the research process. Her shared knowledge has been fundamental in the guidance of this article and in my growth as a student. My dearest Dra. has been one of the biggest influences that have strengthened my gratitude for this career, especially in the field of human rights. I truly hold my her in a high regard.

I am grateful to my professor, Melita Vega, who has left an indelible mark on my academic journey. She not only provided clear guidance and invaluable insights on the research process but also embodies qualities I deeply admire as a woman—being articulate, well-prepared, and confident in her convictions. Under her mentorship, I have learned invaluable lessons on preparation and effective communication in academia.

I want to extend my recognition to the faculty of the School of International Studies at the University of Azuay, whose commitment to academic excellence has been important in developing dedicated and successful students.

Finally, I want to express my gratitude to all those who, in one way or another, have contributed to the completion of this work. Their collaboration and support have left an indelible mark on my path towards achieving my academic and professional goals.

TABLE OF CONTENTS

INDEX OF TABLES

INDEX OF APPENDICES

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 impacts human rights.

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

THE INTERFERENCE OF ARTIFICIAL INTELLIGENCE IN THE VIOLATION OF PRIVACY ON SOCIAL MEDIA

1. Introduction

This work delves into this crucial field of study, where technological innovation and ethical concerns converge. Privacy, understood as a fundamental right ensured in international documents such as the Universal Declaration of Human Rights of 1948, is threatened by the increasing power of Artificial Intelligence (AI) in the realm of social media. This research aims to explore the interactions between AI and privacy, with a focus on human rights and computer ethics.

In this context, it is essential to understand how AI, through sophisticated algorithms and massive data analysis, impacts the way people interact on social media and how their fundamental rights are compromised. According to Bernal (2023), AI's ability to collect, analyze, and use personal data to reproduce patterns raises serious concerns about individual autonomy, algorithmic discrimination, and mass surveillance, among other aspects.

Moreover, it is important to consider the current regulatory framework and its ability to address emerging challenges related to AI and privacy on social media. Regulations such as the European Union's General Data Protection Regulation (GDPR) represent a significant attempt to protect privacy in the digital age but still face challenges in their implementation and effective application.

Ultimately, this research seeks to explore the ethical and social implications of the interaction between AI, social media, and individual privacy. The goal is to share relevant findings from the literature review to inform and guide decision-making in legislative, business, and academic spheres. It is hoped that this analysis will promote the ethical and responsible use of technology for the benefit of society as a whole.

1.1 Objectives

1.1.1. General Objective

To analyze the influence of artificial intelligence on social media and its impact on individual rights, from a human rights perspective, considering ethical, social, and legal aspects, through the use of databases.

1.1.2. Specific Objectives

1. Analyze the consequences of using social media and AI on individuals' privacy.
2. Define the characteristics of the data used by AI and its relationship with social media.
3. Identify some social, legal, and ethical aspects of the relationship between artificial intelligence and social media.

1.1.3. Purpose of the Study

The purpose of the study is to conduct a systematic literature review to analyze the influence of AI. For this, databases and sources from Web of Science and Scopus were used. This analysis will focus on answering the following research question: How does artificial intelligence violate the right to privacy on social media? Along with three sub-questions:

- What techniques does artificial intelligence use to collect and analyze personal data on social media?
- How do these techniques contribute to privacy violations such as the creation of fake identities and hacks?
- What are the current regulatory measures aimed at protecting user privacy against these technologies?

1.2. Theoretical Framework

The theoretical framework of this research provides a conceptual context for addressing the interaction between artificial intelligence (AI), individual privacy, and social media. To fully understand the challenges and implications posed by the intersection of these fields, it is crucial to establish a set of fundamental definitions and concepts. In this context, fundamental concepts such as AI, individual privacy, social media, human rights, computer ethics, and big data are explored. These elements are essential for understanding the ethical, social, and legal challenges that arise from the growing influence of AI on privacy violations in social media. This theoretical framework establishes the necessary conceptual foundations to comprehensively analyze the implications of AI on individual privacy in the contemporary digital environment.

1.2.1. Artificial Intelligence (AI)

The first mention of Artificial Intelligence (AI) was given by John McCarthy et al. (1956), who expressed the need to create machines capable of thinking like humans. Vincent C. Müller (2020) argues that the advancement of artificial intelligence is inevitable and will have a transformative impact on society, although it will face numerous ethical and social challenges in its implementation. On the other hand, AI faces significant challenges, as noted by Leach (2022), who highlights that one of the greatest challenges lies in the need to understand and respond to human emotions. This implies that AI should not rely exclusively on mathematical and rational aspects in its functioning. For this reason, Bossmann (2016) establishes the amorality of AI as the inability to distinguish between right and wrong, leaving this discernment to the nature of the AI user.

Moreover, AI's machine learning, as described by authors like Samuel (1959), allows machines to progressively improve through instructions provided by users or from their own activities. This machine learning capability raises concerns about the ethical implications of AI and individual privacy, highlighted by Floridi (2023), who points out the main concern is the progressive replacement of human labor by AI.

An aspect that needs to be analyzed when discussing learning is that artificial neural networks (ANN) are a fundamental component in the learning of artificial intelligence (AI). According to Salas (2000), these networks have the capacity to learn according to training patterns, which implies the ability to find models that fit the provided data. Essentially, ANNs function analogously to the human learning process, absorbing information through input data to improve performance and make more accurate decisions in the future. However, it is crucial to recognize that ANNs are tools whose learning is based on the instructions and data provided by their creators and users, which raises important ethical and social implications regarding responsibility, privacy, and fairness in their implementation and use.

1.2.2. Individual Privacy

To understand the concept of individual privacy, it is essential to clarify what is meant by the individual in different philosophical and legal contexts. According to Nietzsche, as cited in Wright et al. (1984), the individual is someone who pursues self-fulfillment through their own will, being a strong and independent being who lives an authentic life. On the other hand, Bizberg (1989) describes the individual as a modern being who establishes certain rules of behavior to live in society. From an Aristotelian perspective, the individual is a "zoon politikon," a social being whose end is found in the political community, as suggested by Gintis et al. (2015).

Individual privacy, in the context of the Ecuadorian legal framework, stands as a fundamental right that encompasses various aspects of personal and family life. Although the Civil Code (2005) does not offer an explicit definition of privacy, Article 66 of this code is a cornerstone in the protection of this right. This article establishes the right to personal integrity, which goes beyond the mere physical protection of the individual, extending to the safeguarding of their private sphere against unwanted intrusions. In this sense, individual privacy, according to the Ecuadorian Civil Code, is intrinsically linked to the protection of personal integrity and reputation. This protection not only defends the individual from undue intrusions but also promotes their full development and dignity within society (Civil Code, 2005).

In the legal field, conceptions of the nature of the individual have evolved over time, reflecting both historical contexts and contemporary concerns. Locke (1690), in his classic work "Second Treatise of Government," outlined a fundamental vision that has resonated in political and legal thought to this day. Locke argued that the individual, by the mere fact of being human, possesses inalienable rights such as life, liberty, and property, which must be protected by the government. This conception laid the foundations for the modern concept of human rights, emphasizing the autonomy and dignity of each individual.

On the other hand, in a more contemporary context, Catalini (1944) offers an innovative perspective on the nature of the individual from a legal standpoint. Catalini argues that the individual cannot be understood in isolation but that their identity and rights are shaped in relation to the legal system and the community in which they are immersed. From this perspective, the interpretation of the law becomes a dialectical process, where legal norms and social reality are intertwined in a constant dialogue, thus reflecting the complexity and dynamics of legal life.

Additionally, the theory of law as integrity, proposed by Dworkin (1986), offers another relevant perspective on the nature of the individual in the legal realm. According to Dworkin, in his work "Justice for Hedgehogs," the law should be based on moral principles that respect the dignity and autonomy of each individual. From this view, the legal system not only seeks to resolve conflicts but also to promote justice and respect for fundamental rights, recognizing the importance of integrity and coherence in the interpretation and application of the law.

Despite the differences in approaches and historical contexts of Locke, Catalini, and Dworkin, they all converge on a fundamental idea: the individual is at the center of the law and possesses inherent rights that must be respected and protected by the legal system to ensure a just and equitable society. This convergence reflects the ongoing relevance of reflections on the nature of the individual in the legal field and underscores the importance of addressing these issues comprehensively and thoughtfully in legal theory and practice.

1.2.3. Social Media

Although social media has its roots in the 1950s, it was in 1968 when Licklider and Taylor envisioned a future where computers would become social environments for humans, facilitating communication among them (Licklider & Taylor, R.W, 1968). However, this promise of connection and communication has also brought significant privacy concerns (Roig, 2009). Boyd & Ellison (2007) define social media as spaces where individuals can create public profiles in a digital interaction environment. In this context, users have the ability to control the amount of information they share and regulate who has access to it. In other words, social media, according to Flores et al. (2007), are not just communication platforms but also social structures where individuals interact and build relationships.

However, this interaction on social media is not free from ethical and practical implications. Public exposure online can lead to vulnerabilities and risks to personal privacy, such as identity theft, online harassment, and data manipulation by companies and governments (Álvarez Caro & Piñar Mañas, 2015). Therefore, it is essential to address these concerns and establish policies and practices that adequately protect individuals' privacy in the digital social media environment.

1.2.4. Human Rights

Human rights, according to the philosophy of Immanuel Kant as mentioned by Gruyter (2022), represent categorical imperatives that must be universally respected due to the inherent dignity of each individual. Bobbio (1951), on the other hand, argues that human rights are subjective rights, that is, prerogatives that individuals have against public authorities and must be guaranteed by the State. These philosophical perspectives highlight the importance of human rights as foundations for justice and equality in society.

At the international level, the United Nations (UN) is the key institution in the protection and promotion of human rights. The UN, through the Universal Declaration of Human Rights, established a global normative framework that recognizes the rights of all human beings, regardless of their origin or situation (United Nations, 1948). Similarly, the Council of Europe (2024), through the European Convention on Human Rights of 1950, seeks to protect human rights in the European context by establishing a system of legal protection at the regional level.

In the American regional context, it is relevant to mention the American Declaration of the Rights and Duties of Man, approved in Bogotá in 1948, which precedes the European Convention and establishes a normative framework for the protection of human rights in the Americas. Adopted by the Ninth International Conference of American States, this declaration emphasizes the importance of safeguarding the fundamental rights of all people in the Americas, recognizing their inherent dignity and their right to freedom, equality, and justice. Highlighting this declaration underscores the historical relevance and influence of human rights principles in the Americas, complementing the international framework established by the United Nations Universal Declaration of Human Rights.

The connection between human rights and individual privacy is evident in the recognition of privacy as a fundamental human right. The Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy" (United Nations, 1948). This recognition reflects the importance of protecting personal privacy as an integral part of human dignity and individual freedom, thereby underscoring the interrelationship between human rights and the protection of the individual's intimate sphere.

1.2.5. Computer Ethics and Informed Consent

For García Carrasco (1994), computer ethics is a set of norms and principles that must be respected by professionals in this field. This new ethics, which aims to restore values in the use of technology and its effects on individuals, also represents an evolutionary process in the development of computer ethics, transitioning from traditional ethics to ethics adapted to the digital reality we live in today (Silva & Espina, 2011). Rodríguez et al. (2000) also refer to the need to develop specific ethics in the field of privacy to prevent crimes that compromise individuals' privacy. Furthermore, computer ethics can be understood, as argued by Guibert Ucín (1998), as the analysis of the social impact of technology and the justification for the use of information that can be obtained through it.

Alongside computer ethics is informed consent, which becomes an ethical pillar to protect the autonomy and integrity of the individual. Beauchamp & Childress (2009) highlight that informed consent implies that individuals must have a complete and clear understanding of how their information will be used on social media, as well as the associated risks, before giving their consent. This aligns with the principles of the World Medical Association's Declaration of Helsinki, which establishes the priority of individual interest over the interest of society or science in any research or medical practice (Montori et al., 2013). For example, Dr. Ezekiel Emanuel (2014), an internationally recognized bioethicist and author of the book "Reinventing American Health Care," emphasizes the importance of respecting informed consent in all medical interventions. Working at the Philadelphia General Hospital, Emanuel addresses issues related to medical ethics and health policy, promoting the understanding and respect of patients' rights in accordance with the principles of the Declaration of Helsinki (Emanuel, 2014). In the context of social media, where individual privacy can be compromised by the collection and use of personal data, informed consent emerges as an essential safeguard to protect users' rights and dignity.

1.2.6. Big Data

Originally used to refer to sciences such as astronomy or genetics, in 2000 the term big data was coined to describe massive sets of data, which today have been extended to all human areas (Cukier, 2017). When discussing big data, it is also important to understand the concept of open data, defined by the Open Knowledge Foundation (OKF, 2016), which describes all data that can be freely used, reused, and redistributed by anyone. These two terms go hand in hand, as having big data that is also open allows anyone to access large amounts of information (Ferrer Sapena & Sánchez Pérez, 2013). According to Gil (2016), big data refers to gigantic amounts of information controlled and filtered through the use of algorithms, generally used by companies and governments. Another factor is the amount of digitized information today; just two decades ago, less than 25% of information was digitized, while today more than 98% of information is digital (Mayor-Schonberger & Cukier, 1981).

1.3. State of the Art

1.3.1. Artificial Intelligence and Social Media: Transformation of the Digital Era

According to Bowser et al. (2017), AI has made a significant leap in data analysis and society. However, it also faces challenges such as algorithmic discrimination and threats to individuals' privacy. Algorithmic discrimination, as noted by Castillo Parrilla (2023), refers to the phenomenon where artificial intelligence algorithms perpetuate existing biases in training data or decision-making processes, which can result in unfair or discriminatory decisions toward certain groups. This issue poses significant ethical and social challenges, as it can have negative impacts on areas such as employment, justice, and healthcare (Carlos et al., 2023). Obermeyer et al. (2019) emphasize the need for careful attention in the design and regulation of artificial intelligence systems to address this issue and ensure fairness and justice. The use of advanced algorithms in these systems has led to the massive collection of user data, triggering significant concerns around online privacy, such as information leaks or misuse (Obermeyer et al., 2019).

AI's access to social media data is not subject to significant limitations. This omnipresence presents additional challenges for protecting user privacy, which is why organizations like the European Union (EU) have proposed regulatory measures. However, as highlighted by Suárez Xavier (2022), there is no specific legal framework. Consequently, there is a limitation on individuals' privacy rights concerning social media and AI. Regarding social media, it is important to maintain a balanced perspective due to the potential risks they pose to individual privacy. According to Morozov (2011), social media can be interpreted as spaces where information is collected from individuals who, in some way, have chosen to share part of their private lives publicly.

As noted by Van Dijck & Poell (2013), the digital environment of social media is shaped by algorithms invisible to the common user, which determine what content is shown and how it is distributed. However, the application of these algorithms can be perceived as intrusive, as they significantly influence the user experience, often without their full knowledge and bypassing informed consent. As a result, privacy on social media is regulated not only by individual preferences but also by the algorithmic decisions of the platforms. This interaction between AI and social media not only has implications for user privacy but also raises questions about fairness, transparency, and responsibility in the design and implementation of algorithms and the management of privacy rights. Therefore, Kubler (2016) argues that it is imperative to address these challenges comprehensively to ensure that the evolution of AI on social media benefits all users and respects their fundamental rights in the ever-changing digital environment. Additionally, Chander (2017) points out that algorithms can be unintentionally discriminatory and biased due to information obtained from the internet. This aspect presents a new challenge concerning the regulation and ethics of AI.

With the growth and popularity of social media, McNamee (2019) highlights the increasing concern about the access to personal information that these platforms possess, as well as the spread of false information and access to private data. According to Magaret Hu (2020), public information on social media can be used to feed algorithms that invade our privacy. For example, the company Cambridge Analytica used a Facebook app called "This Is Your Digital Life" to collect personal information from millions of users without their consent (Amnesty International, 2019). As Keltner et al. (2014) point out, this data was subsequently used to develop psychological profiles of users and to target them with personalized political advertisements. This scandal reached its peak when it was revealed that this data was used to influence undecided voters during the presidential elections in the United States, potentially affecting the electoral outcomes.

1.3.2. Turning Point in Digital Privacy: The Cambridge Analytica Scandal

The Cambridge Analytica scandal, which occurred in 2018, marked a significant turning point in the global public perception of digital privacy, highlighting the complex interactions between artificial intelligence and the protection of personal data on social media platforms. This incident exposed how large volumes of personal information could be manipulated without the explicit consent of users, triggering a critical debate on digital privacy and the ethical principles that should govern artificial intelligence (Vera, 2019).

Before this scandal, privacy was often perceived as a simple commercial exchange: users provided their personal information in exchange for access to personalized digital services at no cost. However, the revelation of economic surveillance practices by entities such as Cambridge Analytica and Facebook altered this perception. According to Afriat et al. (2020), after the scandal, a shift was noted in user attitudes, who began to question the idea of privacy as a conditional right and started to accept economic surveillance as an inevitable aspect of the digital world. This change underscores how privacy scandals can reshape public perception and promote critical dialogue about norms and practices in the handling of personal data.

The analysis of the relationship between Facebook and Cambridge Analytica revealed how the transfer of personal information has become a structured business model, involving an extensive ecosystem of data providers and consumers. Cruz & Dias (2022) highlight that this business model urgently requires a reconsideration of data protection strategies and propose the implementation of a comprehensive set of data protection recommendations to mitigate future risks.

Furthermore, Wagner (2021) examines how the Cambridge Analytica data breach not only demonstrated the capacity for global political influence through the misuse of personal information but also raised fundamental questions about ethical principles and responsibility in the management of personal data. This case emphasizes the need for stricter and more transparent regulations in the use of artificial intelligence and personal data management, showing how technology can radically transform the digital environment and profoundly impact both individual and collective privacy. This analysis highlights the importance of more rigorous and transparent regulation in the use of AI and personal data management on social media, demonstrating how technology can transform the digital environment and deeply affect individual and collective privacy.

1.3.3. Setting the Rules and Terms of Acceptance for the Most Used Platforms

Terms and conditions are fundamental legal documents that establish the relationship between social media companies and their users. These documents, which emerged in response to legislative data protection needs, detail the rights and obligations of both parties. The formal implementation of terms and conditions on digital platforms began to take shape with the evolution of the Internet and the first digital privacy regulations in the last decades of the 20th century. The EU Data Protection Directive in 1995 (European Union, 1995) and the Children's Online Privacy Protection Act (COPPA) in 1998 in the United States (United States, 1998) were pioneering regulations that required platforms to obtain explicit user consent for the processing of their data. These regulatory developments spurred the creation of the first terms and conditions on emerging platforms at that time.

With the advent of platforms such as Facebook (2004), Twitter (2006), Instagram (2010), and TikTok (2016), terms and conditions were established that were adapted not only to data protection laws but also to the commercial and technological needs of each platform. These terms and conditions were designed to facilitate the extensive use of data in marketing strategies and content personalization, significantly driven by advancements in artificial intelligence (AI). AI has enabled these platforms to optimize the user experience and precisely target content and advertising, thereby increasing their profitability and functionality.

However, the complexity and length of these documents have raised ethical and legal questions, particularly regarding their comprehensibility and the true voluntariness of consent. According to Schneble et al. (2021), the consent processes on many platforms are not taken as seriously as required, with terms and conditions that are often lengthy and difficult to understand, posing a significant challenge in terms of ethics and transparency. Moreover, the continuous evolution of privacy policies and terms of service reflects the need to adapt to an ever-changing digital environment, where AI plays an increasingly central role. Transparency and fairness in the use of AI are crucial to maintaining user trust and ensuring compliance with ethical and legal standards in the management of personal data.

1.3.4. Changes in Terms of Acceptance and How They Affect User Privacy

Terms and conditions are essential for the functioning of platforms like Facebook, Instagram, Twitter, and TikTok, playing a crucial role in controlling user privacy. Originally clear and straightforward, these terms have evolved significantly, adapting to new technologies and practices, particularly with the introduction of artificial intelligence. Accepting these terms means granting the platforms permission to access and manage a variety of personal data. The specific permissions and accesses granted by accepting the terms and conditions of each of these platforms are detailed in the following:

Founded in 2004, Facebook has adjusted its terms of service in response to its expansion and the integration of new technologies. Facebook collects information provided directly, such as name, email address, and content posted, as well as information about interactions, locations, and devices used. Additionally, the platform uses AI to personalize ads and content based on interests and activities. Facebook can share data with third parties, including companies within the Meta group, advertisers, and other business partners (Platforms, 2023). It also uses cookies and similar technologies to track behavior on and off the platform (Facebook, 2023). A clear example is the Cambridge Analytica scandal mentioned as a turning point. This case revealed how Facebook allowed this consultancy to access the personal data of millions of users without their explicit consent. This data was used to influence the 2016 US presidential elections by creating psychological profiles and targeting specific political ads (Amnesty International, 2019).

Instagram, acquired by Facebook in 2012, initially did not possess the data analysis complexity of its parent company. However, after the acquisition, Instagram's terms of service expanded to allow deeper analysis of images and videos. Instagram collects and analyzes the photos and videos uploaded, as well as interaction data (likes, comments). It can access precise and imprecise location data to personalize content. Additionally, it shares data with Meta group companies and other third parties to improve advertising and services. It collects device data, such as IP addresses, browser type, and operating system (Instagram, 2023). Instagram has been criticized for its exploration algorithm, which promotes content based on users' perceived interests. This has led to issues such as promoting content that can negatively affect adolescents' mental health, exposing them to unrealistic beauty standards and content that fosters social comparison (Pew Research Center, 2021).

Twitter, now known as X, was launched in 2006. This social network has seen significant changes in its terms of service, especially in how it manages and uses real-time data to personalize and moderate content. Twitter collects real-time data on tweets, retweets, likes, and other types of interaction. It uses the data to personalize ads and content suggestions. It collects information about the device used and the geographical location. It can also share data with business partners and advertisers (Twitter, 2023). During the 2020 US presidential elections, Twitter was criticized for its handling of misinformation. The platform used algorithms to identify and flag potentially misleading content but also faced challenges regarding the consistent application of these policies, leading to debates about freedom of speech and censorship (Frenkel & Alba, 2020).

TikTok, which emerged in 2016, quickly integrated AI technologies to analyze videos and user behaviors. Its ownership by ByteDance (2023) has raised international privacy concerns, especially related to data transfer and storage. TikTok analyzes uploaded videos and platform behavior (views, interactions) using AI. It collects personal data such as name, age, contact information, and biometric data. The data can be transferred and stored on servers outside the country of residence, including China. It uses the data to show ads and personalized content (TikTok, 2023). In 2020, it was revealed that TikTok was collecting biometric and location data from users, raising national security concerns in several countries. Additionally, TikTok's algorithm has been criticized for promoting specific content that can influence users' purchasing decisions and behaviors, especially among young people (Fowler, 2020).

1.3.5. Current Risks Related to AI in Social Media

Artificial intelligence (AI) has revolutionized the way we interact on social media, offering numerous advantages in terms of personalization and efficiency. However, it has also introduced significant risks affecting user privacy and security. This analysis explores some of these current risks, highlighting the need for adequate protective measures. One of the most prominent risks is the creation and proliferation of fake identities. Van der Walt et al. (2018) highlight how AI can be used to generate fake profiles that are indistinguishable from real ones. These profiles can be used to carry out malicious activities such as scams and opinion manipulation. Detecting these fake identities is a constant challenge due to the sophistication of the techniques employed.

Another major risk is account hacking, where attackers use AI techniques to crack passwords and bypass security measures. According to Khan (2017), the vulnerability of social platforms to these attacks has increased, and traditional protection methods are no longer sufficiently effective against advanced AI programs that learn and evolve. Data privacy is an ongoing concern on social media. Taddicken (2014) discusses how AI's data collection and analysis can lead to significant privacy violations, where sensitive personal information is compromised without the user's knowledge. The lack of transparency regarding what data is collected and how it is used is a central issue in the age of AI.

Social media users often become cyberstalkers, using publicly available information to track and collect data on others without their consent (Gil, 2016). Castillo Parrilla (2023) notes that AI can facilitate this behavior by automating and optimizing data collection, intensifying concerns about privacy and consent. A worrying aspect is the violation of the right to privacy, a fundamental principle of human rights. Vásquez & José Alberto (2021) argue that AI, by enabling intensive surveillance and monitoring, can infringe on this right without users having clear options to opt out or control the use of their data.

The role of AI in behavior manipulation is also significant. Through the analysis of large volumes of data, platforms can subtly influence users' decisions and opinions, a risk identified as one of the main ethical threats of AI on social platforms (Carlos et al., 2023). Finally, it is crucial to recognize the need to implement robust legal frameworks to regulate the use of AI on social media. The introduction of the General Data Protection Regulation (GDPR) in Europe and other similar legislations are steps towards protecting users against the potential abuses of AI, as suggested by Bosque & Villan (2018), who advocate for a multidisciplinary approach to addressing these challenges.

1.3.6. Regulatory Framework: General Data Protection Regulation (GDPR) and Ecuadorian Regulatory Framework

In the regulatory domain, the European Union's General Data Protection Regulation (GDPR) has established a comprehensive legal framework for the protection of personal data in the digital age (European Union, 2016). The GDPR highlights and underscores the importance of transparency in data handling and informed user consent. This regulation represents a significant regulatory effort to safeguard privacy in the context of AI and social media. While the GDPR is an important step in online privacy protection, it also poses additional challenges in the context of AI and social media. Alston & Gillespie (2012) argue that AI can play a crucial role in reducing the spread of misinformation online, potentially improving the accuracy and relevance of search results.

Although Ecuador does not directly implement the European Union's GDPR, Espinosa (2022) notes that it has served as a reference and foundation for the development of national data protection legislation. The Organic Law on Data Protection (LOPD) is the primary regulation in Ecuador to ensure the privacy and integrity of citizens' personal data. It came into force on May 27, 2021, and establishes fundamental principles for the transparent, fair, and secure handling of personal data, as well as the rights of individuals over their own data. Additionally, the LOPD introduces the figure of the Data Protection Officer (DPO), who acts as a privacy advocate and ensures legal and ethical compliance in the handling of personal data (Rodríguez Ayuso, 2020).

A concrete example of the application of the Organic Law on Data Protection (LOPD) in Ecuador is evident in the healthcare sector, where professionals and medical institutions must ensure the confidentiality and security of patients' medical information. Strict compliance with these provisions is essential to protect the fundamental rights of patients' privacy and confidentiality. Any violation of these regulations can result in not only legal sanctions but also severe consequences for the integrity and trust in the healthcare system.

In the Ecuadorian context, the starting point is the 2008 Constitution of Ecuador, which establishes the fundamental right to privacy and the protection of personal data, reflecting a robust legal framework aimed at safeguarding these rights nationally (National Assembly of Ecuador, 2008). Although Ecuadorian legislation does not specifically address artificial intelligence (AI), it can be inferred by analogy that the state has an obligation to protect the integrity and confidentiality of its citizens' data, as this is a fundamental right. The Organic Comprehensive Criminal Code of Ecuador (2021) (COIP) establishes in Articles 179 and 180 sanctions for individuals who violate the privacy of others by collecting, storing, or transmitting information without express authorization.

According to Article 66 of the 2008 Constitution of Ecuador, various fundamental rights related to privacy and data protection are recognized and guaranteed to individuals, including the right to privacy (Section 7), the inviolability of correspondence and communications (Section 11), the right to data protection (Section 18), the right to informational self-determination (Section 19), the privacy of personal life (Section 20), and the secrecy of banking and financial information (Section 21). These rights are an integral part of the Ecuadorian legal framework and reinforce the protection of privacy and data confidentiality nationally.

The analysis of Article 92 of the 2008 Constitution of Ecuador, which establishes the principle of habeas data, is fundamental for understanding personal data protection in the country. This article guarantees individuals the right to access, know, update, and rectify information collected about them in public or private databases and records of entities that process data. In other words, habeas data ensures that individuals have control over the information stored about them and allows them to correct any inaccuracies or incompleteness in their personal data. This constitutional provision further strengthens the Ecuadorian state's commitment to the protection of privacy and the integrity of personal data, establishing legal mechanisms to ensure the effective exercise of these rights.

Therefore, it can be inferred that any data violation in the Ecuadorian context not only constitutes a legal infraction but also a violation of fundamental human rights. The protection of privacy and the integrity of personal data is a central pillar in Ecuadorian legislation and jurisprudence, and its violation carries significant legal and ethical consequences. It is necessary to reinforce and enforce these legal provisions to ensure the effective protection of individual rights in the digital age.

1.3.7. The Right to Data Protection as a Fundamental Human Right

Fundamental rights, unlike human rights, are obligatorily protected by each state once they are enshrined in the constitution. Therefore, the protection of personal data is not merely a technical or administrative matter but a fundamental right that must be recognized and guaranteed as such (Martínez Martínez, 2007). In this sense, Cannataci et al. (2010), prominent Maltese scholars specializing in human rights and privacy in the digital age, argue that the right to data protection is crucial in an increasingly interconnected and technological world.

Based on the work "Global Privacy Protection: The First Generation," Rule & Greenleaf (2010) contend that the right to data protection is essential for preserving human dignity, autonomy, and individual freedom in contemporary society. They also warn of the challenges that arise regarding data protection in the context of artificial intelligence (AI). They recognize that AI can lead to greater collection and analysis of personal data, increasing the risk of privacy violations.

However, Rule and Greenleaf also emphasize the need to find a balance between technological innovation and privacy protection. They argue that robust regulations are fundamental to safeguarding the right to data protection in the context of AI. While acknowledging the potential benefits of AI in various fields, they warn of the dangers of irresponsible or malicious use of this technology that could undermine individuals' fundamental rights (Rule & Greenleaf, 2010).

The current access to data and the free flow of information is the greatest challenge faced by data protection policies. The GDPR itself asserts the need to unify the fundamental values of respecting private information and the free flow of information, as noted by Castillo Parrilla (2023). According to Gil (2016), the value of data increases with its interconnection. Data protection has traditionally been studied as part of the first generation of human rights, but according to Castillo Parrilla (2023), with the advent of AI and big data, a new dimension has been added to its analysis, placing it in the fourth wave of human rights, with a focus on the digital environment. Considering Gil's statements, data protection as a human right must be approached from a renewed perspective. This implies starting with the identification and analysis of what he calls "contaminating actions," such as excessive data collection, and then moving towards understanding a healthy digital environment that ensures individuals can operate with a minimum expectation of anonymity (Castillo Parrilla, 2023).

Currently, there is a trend to recognize data protection as a fundamental right, particularly in the European context, as data protection is mentioned in the Charter of Fundamental Rights of the European Union and was also included in the failed European constitution with a definition of a fundamental right (Martínez Martínez, 2007). In Chile, data protection has been enshrined in the constitution. As highlighted by Contreras (2020), with the latest reform of the Chilean constitution, data protection has found its place as a fundamental right. Personal data can be used as a tool for competitive advantage by predicting behaviors and generating trend lines. This has led many companies to push the boundaries of individual privacy, using these data to their advantage. This concern has driven the establishment of data protection as a fundamental right (Frigerio, 2018).

Additionally, Medina Guerrero (2022) argues that beyond data protection, individuals must be aware of the algorithms that use their data and the purposes of these algorithms, especially when their information is used in decision-making processes that affect them and in automated processes that impact their lives. Thus, data protection must be regulated and treated as a fundamental right in an era of digitalization that allows for excessive exposure of information, which must also guarantee its protection. Although data protection has been more developed in Europe, similar laws exist in South America, as shown in Table 1.

Table 1
Data Protection Laws

Country	Law	Year
Chile	Law No. 19628 on the Protection of Private Life	1999
Argentina	Personal Data Protection Law	2000
Paraguay	Law No. 1682 on Personal Data Protection	2001
Uruguay	Law No. 18.331 on Personal Data Protection and Habeas Data	2008
Venezuela	Organic Law on the Right to the Protection of Personal Data	2008
Bolivia	Law No. 1640 on Personal Data Protection	2011
Peru	Law No. 29733 on Personal Data Protection	2011
Colombia	Statutory Law No. 1581 of 2012 on Personal Data Protection	2012
Brazil	General Law on the Protection of Personal Data	2018
Ecuador	Organic Law on the Protection of Personal Data	2019

Note: All these laws were generated in a non-digitalized context but can be applied in this context.

1.3.8. Evolution of Regulations in Cases of Privacy Violations in Ecuador and Latin America

In Ecuador, the Constitution not only protects life but also guards against all types of invasions of the individual. “The right to data protection grants individuals the ability to control their personal data and, in turn, the capacity to manage and decide on its use” (Villalba, 2017). This constitutional principle aligns with habeas data, recognized as a mechanism guaranteeing the right to personal data protection in Ecuador. This right cannot be invoked as a means to request the physical delivery of the material or electronic support of documents containing personal information, but rather to know of its existence, access it, and exercise the actions provided for in Article 92 of the Constitution of the Republic, which establishes the legal framework of habeas data.

The legal scholar Puccinelli (1999) analyzes the Constitutional Court of Ecuador ruling 001-14-PJO-CC in reference to this right. In his analysis, he notes that the right to data protection, known as "informational self-determination," has an instrumental character. According to Puccinelli, this right is subject to the protection of other constitutional rights that could be affected when personal data is used, such as privacy and other fundamental rights.

It can be said that the right to data protection has evolved in the current digital context in which we live. In addition to the normative framework established in the Constitution and the Comprehensive Organic Criminal Code (COIP), Ecuadorian jurisprudence has played a crucial role in addressing privacy violations and the protection of personal data. According to studies by Durán Ramírez & Zamora Vázquez (2023), the Constitutional Court of Ecuador has issued rulings that have set important precedents in cases related to online privacy and the misuse of personal data.

Examples include ruling No. 2064-14-EP/21, which determined that the denial of a habeas data action violated the rights of a plaintiff whose intimate photos were disclosed without consent. The court recognized the violation of rights such as data protection, privacy, and good name. It ordered the removal of the images, prohibited their processing, and mandated training for judges on habeas data to safeguard privacy.

In ruling No. 032-17-EP/21, the court addressed a case where the unauthorized disclosure of personal information on social media constituted a violation of an individual's right to privacy. The court ordered measures to delete the disseminated information and protect the plaintiff's personal data on digital platforms, reaffirming the importance of safeguarding privacy in the digital environment.

In Argentina, the government has expressed its intention to present an artificial intelligence bill that includes provisions on ethics and human rights (Vercelli, 2023). This stems from growing concerns about data usage and the need to establish a regulatory framework governing AI, in the context of a fourth wave of human rights characterized by its focus on the digital and technological environment.

Brazil has enacted the General Data Protection Law (LGPD), particularly focusing on Law No. 13.709/2018. This law was developed to guarantee the freedom and privacy of Brazilian citizens (Torres et al., 2018). It provides legal security for all citizens in an increasingly digital economy; the LGPD defines personal data as "any information related to an identified or identifiable natural person" and establishes that data processing is any operation performed with an individual's data (LGPD, 2018).

In its recent constitutional reform, Chile has taken a significant step by establishing a solid regulatory framework for the protection of personal data, primarily referencing the GDPR. As noted by Contreras (2020), the adoption of principles and standards inspired by the GDPR reflects the Chilean authorities' recognition of the need to align with international best practices in data protection. These legislative efforts reflect the growing concern in the region to guarantee the protection of individual rights in an ever-evolving digital environment. These examples represent the influence of the GDPR in Latin America and how this European legal framework has driven the evolution of current legal norms.

1.3.9. The Use and Influence of GDPR in Some Andean Countries

As indicated in the book "The Latin American Vision on the General Data Protection Regulation" by Enríquez Álvarez (2020), since the GDPR came into effect, most Latin American countries, especially the

Andean ones, have started a process of data protection reforms to adapt to the mentioned legal framework. This phenomenon reflects a clear trend towards the new digital age and the pressing need for an adequate regulatory framework. Despite notable advancements in data protection driven by the GDPR, security professionals in Andean countries face a significant challenge as their training is primarily based on U.S. methodologies.

Bolivia has established data protection legislation, the Regulation to Law 163 on Telecommunications and Information and Communication Technologies (Bolivian ICT Regulation), which, according to Ildefonso & Aruquipa (2020), is inspired by the EU's GDPR. However, the Bolivian regulation differs in that it recognizes both natural and legal persons, whereas the GDPR focuses on natural persons. Its influence is evident, as shown in Table 2.

Table 2

Similarities between the GDPR and the Bolivian ICT Regulation

Topic	**GDPR**	**Bolivian ICT**
Lawfulness, fairness, and transparency	5.1a	4.IIc, 56. D
Purpose limitation	5.1b	4.II. a
Data minimization	5.1c	
Quality	5.1d	4.II. b
Storage limitation	5.1e	
Integrity and confidentiality	5.1f	4.II. d, 4. II. e
Proactive accountability	5.2	
Lawfulness of processing	6	
Conditions for consent	7	56.b
Consent for minors	8	
Sensitive data	9	
Personal data relating to criminal offenses	10	

Note: Own elaboration, adapted from Mapping of the Bolivian ICT Regulation, GDPR, and RIPD Standards in the field of Personal Data Protection, by Ildefonso and Aruquipa, 2020.

Although not all aspects covered by the GDPR are enshrined in the Bolivian ICT Regulation, the relationship between the two is clear, especially regarding general aspects. Peru, on the other hand, has Law No. 29733, the Personal Data Protection Law (LPDP), which was influenced by the European Union's General Data Protection Regulation (GDPR). The research by Vásquez Rodríguez (2022) exemplifies how Article 5 of the LPDP, concerning the principle of consent, is a clear reference to the GDPR. An essential part to consider about the LPDP is that this legal body and its regulation are infra-constitutional norms that develop individuals' rights through the derivation of the fundamental right to personal data protection (Vásquez Rodríguez, 2022).

According to Albornoz (2022), in Ecuador's Organic Law on Personal Data Protection of 2021, paragraphs 2, 3, and 4 of Article 3 contemplate criteria established by Article 3.1 of the GDPR. This is the clearest example of how the GDPR has influenced the regulations of the Andean countries. An additional example of this progress in data protection is the Ecuadorian Data Protection Agency (APD), which in 2022 helped a citizen recover data that had been used illegally after her ex-partner shared it without her authorization, ordering the deletion of the data and prohibiting further contact with this citizen.

The case of Colombia can be best exemplified by the recent sanction imposed by Colombia's Superintendence of Industry and Commerce on Claro for violating the Data Protection Regime, imposing the highest possible penalty; Claro failed to implement adequate and sufficient measures through one of its commercial campaigns (Superintendence of Industry and Commerce, 2023). This case reflects Colombian regulations, which, similar to Bolivian regulations, are infra-constitutional and influenced by the GDPR.

According to Bosque & Villan (2018), the impact of the GDPR on some Andean countries has driven laws and reforms by strengthening institutions and raising citizen awareness. Reforms that are enshrined in various legal bodies such as the COIP in the Ecuadorian case, the new Organic Law on Data Protection, Peru's LPDP, and Colombia's Data Protection Regime. Despite not directly applying the GDPR, its influence on the mentioned countries in establishing legal frameworks that protect individuals' data cannot be denied.

1.3.10. Data Privacy in the United States of America

According to Pérez (2022), the constitutional law of the United States generally does not enshrine individual rights but rather prohibits the denial of liberty, where privacy rights reside. This closely relates to the growing concern for data protection in the country, as privacy is closely linked to liberties. Barrio Andrés (2022) notes that this concern has led to the emergence of data protection proposals in the United States, which seek to address challenges and ensure the safeguarding of individual privacy in an ever-evolving digital environment.

To provide examples of the enshrinement of data protection laws, as of June 2022, California, Virginia, Colorado, Utah, and Connecticut have successfully enacted comprehensive state privacy laws regulating the protection of consumer data. A notable example is the California Consumer Privacy Act (CCPA), which came into effect in 2020 (CCPA, 2024). This law protects all natural persons within the state of California and grants consumers three main rights: to know the data companies have collected, to opt out of the sale of collected information, and to delete personal data collected under certain circumstances (Duties et al., 2024). These cases exemplify how concern for data protection has translated into data protection laws.

A case study on data protection is the Ashley Madison incident, a social network for extramarital affairs that was hacked in July 2015 (Platero Alcón, 2017). The exposure of user information raised concerns about data protection. According to Platero Alcón (2017), Ashley Madison's privacy statement authorizes the social network to share or sell all collected personal data, including significant information such as ethnic origin or sexual life, with third parties, as well as to reserve the right to share clients' financial information, given that the platform is fee-based. By highlighting the use of personal information in a big data environment, as in the case of the Ashley Madison social network, it reveals how this network exploits user data through terms and conditions that often go unnoticed by those sharing their information on these platforms.

Another prominent case is that of Cambridge Analytica. Following the data leak scandal, Facebook CEO Mark Zuckerberg was compelled to establish an independent privacy committee, stripped of his direct control, and to strengthen the oversight of third-party applications. According to Vera (2019), this case is perceived as an attack on democracy since the data obtained from Facebook was used to influence U.S. elections, resulting in Trump's victory. This incident not only violates individual privacy but also affects liberty, a fundamental human right protected by the United States for its citizens. The criticism focuses on the accusation against Zuckerberg of having shared data with Cambridge Analytica, which was then used in a campaign strategy to influence various political processes, such as the U.S. presidential elections and Brexit.

Considering that the misuse of data not only undermines individuals' privacy but can also affect democracy and international relations by influencing them through the use of big data, these cases exemplify the urgent need for specific data protection legislation with national scope, not limited to individual states but with a federal character.

2. Methodology

2.1 Systematic Review

The methodology selected for this research study is the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) declaration, recognized for its effectiveness in qualitative analysis in social fields, despite originally being designed for medical studies (Samala et al., 2023). Additionally, this methodology facilitates reverse verification, meaning that the obtained results can be corroborated.

2.2 PRISMA Application

To conduct this research, the following structured steps from Yepes-Nuñez et al. (2021) were followed according to the PRISMA methodology:

- Definition of questions and objectives: The main question established was: How does artificial intelligence violate the right to privacy on social media? This was subdivided into three sub-questions to facilitate the literature search and analysis: What techniques does artificial intelligence use to collect and analyze personal data on social media? How do these techniques contribute to privacy violations such as the creation of fake identities and hacking? What are the current regulatory measures aimed at protecting user privacy against these technologies?
- Selection of databases: Searches were conducted in highly relevant academic digital libraries: Scopus and Web of Science.
- Search string: Artificial AND intelligence AND human AND rights AND privacy
- Creation of an analysis matrix: An analysis matrix was created to classify and evaluate all collected articles according to their relevance and contribution to the research questions.
- Eligibility criteria: Inclusion and exclusion criteria were implemented to select pertinent and reliable studies as shown in Table 3.

Table 3
Inclusion and Exclusion Criteria for Article Selection

Criteria	Inclusion	Exclusion
Digital Libraries	Web of Science y Scopus	
Language	English and Spanish	Articles written in languages other than English and Spanish
Document Type		Editorial material, corrections, books, pages, magazines, opinions on literature reviews, early access, reports, conference proceedings, trade journals, letters, book series, notes
Years of Publication	2018-2024	
Countries/Regions	All countries	
Access Type	All types of articles, available for download	Specific cases that cannot be downloaded
Subject Area	Topics related to the research title	

2.3 Keywords

The search string strategy is: Artificial AND intelligence AND human AND rights AND privacy. Year filters will be applied to select studies from 2018 onwards, reflecting the impact of the Cambridge Analytica scandal as a turning point. This incident marked a significant shift in public perception of digital privacy and highlighted the complex interactions between artificial intelligence and the protection of personal data on social media, triggering a critical debate on digital privacy and ethical principles in artificial intelligence.

2.4 Application of the PRISMA methodology

The study selection process for this research was conducted in three phases, based on the PRISMA methodology, using a total of 90 selected articles, as seen in the appendices. The phases and criteria applied in each are described below:

Initial Screening:

- By entering the search string: Artificial AND intelligence AND human AND rights AND privacy in Web of Science, a total of 158 articles were obtained. In Scopus, 364 articles were retrieved.
- An initial filter based on the titles and abstracts of the articles was conducted to identify those potentially relevant to the research topic: “The interference of AI in the violation of the right to privacy on social media.”
- Articles published between 2018 and 2024 in English and Spanish, available in the Web of Science and Scopus databases, were included.

Full Review:

- The full texts of the articles selected in the screening phase were reviewed in detail to assess their compliance with the inclusion and exclusion criteria defined in Table 3.
- Articles that did not meet the criteria for thematic relevance, language, or document type were excluded.
- This review reduced the number of articles to 90, which met all the established criteria.

Metadata Download:

- The metadata of the 90 selected articles were downloaded in CSV format for subsequent systematic analysis.
- This data included relevant information such as title, author, year of publication, source database, and specific content related to the study topic.

2.5 Data Extraction

For the data extraction phase, the export options of the Web of Science and Scopus databases were used, allowing results to be downloaded in CSV and Excel formats, as detailed by the PRISMA methodology and according to a systematic review article respectively. These export tools facilitated the initial filtering of studies according to predefined criteria such as authors, year of publication, methodology employed, and main findings. Once the data extraction was completed, the information was organized into two Excel files. The first sheet of each file included the data downloaded in CSV format. On the second sheet, the information was written following the example of a literature review matrix provided by the UDA Library. This matrix allowed for the classification and synthesis of studies in a coherent and structured manner. Finally, the information organized in the Excel sheets was converted into a Word table, which is Appendix 1. This combination of automated processes and manual review ensured the relevance and quality of the extracted data.

3. Results

3.1 Data Analysis and Selection

The selection and analysis of data were carried out using a systematic literature review methodology. A total of 90 relevant articles addressing the interference of artificial intelligence in the violation of privacy on social media were identified (see Appendix 1). The results obtained are presented in the following.

3.2 Analysis of the Geographical Origin of the Publications

Table 4

Distribution of Publications by Regions

Region	Number of Articles
North America	40
Europe	25
Asia	15
Africa	5
Others	5

As shown in Table 4, the majority of publications come from North America and Europe, which makes sense due to the high concentration of studies on privacy violations and artificial intelligence in these regions. In the United States, concerns about data protection are closely related to constitutional liberties. This is why incidents like Cambridge Analytica, as highlighted by Vera (2019) in his article “Nothing is Private,” emphasize the severity of the misuse of personal data through Facebook, affecting millions of users and becoming one of the most notable examples of violations of informed consent. In 2023, approximately 81% of adults in the United States use YouTube and 69% use Facebook, indicating a high penetration of social media among the adult population. This widespread use of social media facilitates the massive collection of data, increasing the risk of privacy violations (Pew Center, 2024).

In Europe, with 25 publications, there has been a significant influence of the GDPR on data protection regulations in several European countries. This regulation has set a standard for personal data protection and has served as a model for other jurisdictions. Albornoz (2022) highlights how the GDPR has been fundamental in creating robust data protection policies in Europe. In Asia, with 15 publications, there is a growing focus on privacy regulation and data protection. In Japan, for example, human-centered data protection laws emphasize individual dignity and privacy. These laws reflect a commitment to protecting citizens' rights in an increasingly complex digital context (Miyashita, 2021).

In Africa, although there are only 5 publications, AI regulation must consider both the benefits and risks to human rights. Abe & Eurallyah (2022) highlight that the absence of robust human rights protections in some African countries increases vulnerability to privacy violations. However, there is also interest in using AI to improve regulations and protect the population, as noted by Brand (2022) in his article “Responsible Artificial Intelligence in Government: Development of a Legal Framework for South Africa,” which underscores both the lack of protection and the potential of AI to enhance human rights conditions in the region. In Latin America, the influence of the GDPR has been notable in the formulation of data protection laws (Enríquez Álvarez, 2020). This effort to align local regulations with international standards reflects a commitment to improving user privacy and better protecting their personal data in a global digital environment.

3.3 Analysis of Thematic Areas

The review of the 90 selected articles reveals a diversity of thematic approaches as shown in Table 5.

Tabla 5

Distribution of Publications by Thematic Areas

Thematic Area	Number of Articles
Computer Ethics	25
Data Regulation	20
Human Rights	18
Artificial Intelligence and Privacy	27

The studies in the area of Computer Ethics (25 articles) explore the ethical implications of using artificial intelligence, covering topics such as fairness, transparency, and responsibility in the design and implementation of AI systems. Regarding Data Regulation (20 articles), this area focuses on policies and laws related to data protection and privacy, evaluating the effectiveness of existing regulations and proposing new strategies to improve data security. The articles in the Human Rights category (18 articles) analyze how artificial intelligence can affect fundamental human rights, including the right to privacy and freedom of expression. Finally, the area of Artificial Intelligence and Privacy (27 articles) directly examines the relationship between AI and privacy, evaluating how AI technologies collect, process, and use personal data.

There is also a diversity of academic institutions from around the world, with a notable concentration in prestigious universities. These universities stand out not only for the quantity of their publications but also for the quality and impact of their research. Prestigious universities such as Harvard University, Stanford University, and the Massachusetts Institute of Technology (MIT) in the United States lead in terms of contributions. According to the QS World University Rankings, these institutions are among the best in the world due to their performance in key areas such as teaching, research, knowledge transfer, and international outlook (Universities, 2023). This recognition is based on rigorous indicators including academic reputation and the number of citations received, which underscores the relevance and academic rigor of their research.

These articles contribute significantly to this systematic literature review due to their advanced infrastructure, access to resources, and global collaboration networks. The participation of these institutions in research on artificial intelligence and privacy is important because it validates the selection of the reviewed articles, ensuring that the studies come from reliable and high-quality sources. The Times Higher Education World University Rankings 2023 highlights that U.S. universities are the most represented in the top 200, with 58 institutions, reflecting their leadership in research and higher education (Education, 2022).

3.4 Analysis of the Temporal Range

The review of articles published between 2018 and 2024, which aligns with the previously established inclusion criteria, shows a significant trend in the increase of publications starting in 2020, coinciding with the onset of the COVID-19 pandemic, as shown in Table 6.

Tabla 6
Number of Articles per Year

Year	Number of Articles
2018	2
2019	4
2020	8
2021	22
2022	21
2023	20
2024	13

The notable increase in the number of articles published from 2020 onwards can be attributed to the COVID-19 pandemic, which caused global lockdowns and a much greater reliance on social media and information technologies. During this period, people were more interconnected through digital platforms due to the confinement, leading to increased collection and use of personal data, along with heightened concerns about privacy and information security.

According to a study published by Bilisli & Tuzcu (2021), social media played a vital role in disseminating public health information during the pandemic but was also excessively used, which heightened mental health issues due to the spread of false news and social panic. This global context of increased interconnection and exposure to social media justifies the rise in research on privacy and artificial intelligence during these years.

3.5 Interpretation of the Results

After conducting a thorough analysis of the collected information sources, a regulatory framework was established to address the challenges of the current digital environment, particularly concerning artificial intelligence and privacy on social media. The results show a growing concern about privacy violations due to artificial intelligence on social media. Most of the reviewed studies emphasize the need to establish stricter and clearer regulatory frameworks to protect users' privacy rights. For example, Vásquez & José Alberto (2021) indicate that AI can violate fundamental rights and propose the need for human oversight to protect these rights. This perspective is shared by several authors who emphasize the importance of computer ethics and informed consent in the use of AI on social media. However, the reviewed articles address these issues from different angles. While some studies, such as Lane (2022), focus on the need for clarity in human rights standards, others, such as Miernicki & Ng (2021), explore moral rights in the context of AI.

The diversity in the thematic areas of the reviewed articles reflects the complexity of the topic and the need for a multidisciplinary approach to address the implications of AI on privacy. For instance, studies on data regulation and computer ethics highlight the importance of establishing policies and practices that adequately protect users' privacy in the digital environment. On the other hand, some studies, like Abe & Eurallyah (2022), approach AI from a more positive perspective, highlighting its potential benefits in regions like Africa, where technology could help overcome significant local challenges. However, these studies also acknowledge the risks and the need for appropriate regulation to protect human rights. In contrast, articles such as Villaronga et al. (2018) discuss the risks of AI in terms of privacy, noting that the technology can be used for mass surveillance and data collection without users' proper consent. This type of research emphasizes the importance of addressing the ethics and morals of both AI developers and users who accept terms and conditions without considering the long-term implications.

In the European context, data protection has been widely developed. For example, Castillo Parrilla (2023) highlights that this protection should be part of the fourth wave of human rights, focusing on how digitalization affects individual rights. In contrast, Martínez Martínez (2007) considers data protection a fundamental right, supported by national legislation, giving it binding force. This perspective is shared by Contreras (2020), who notes that the latest reform of the Chilean constitution recognizes data protection as a fundamental right. Bowser et al. (2017) argue that the use of data, artificial intelligence, algorithms, and neural networks presents significant ethical and social obstacles, as demonstrated by cases like Cambridge Analytica and Ashley Madison. Algorithmic discrimination is another problem identified by Castillo Parrilla (2023), who explains that algorithms can perpetuate biases, resulting in unfair or discriminatory decisions. This concern is shared by Obermeyer et al. (2019), who highlight the need for careful regulation to ensure fairness and justice.

The European Union's General Data Protection Regulation (GDPR) has had a significant impact on other countries. In Latin America, laws such as Peru's LPDP and Ecuador's Organic Law on Data Protection have been influenced by the GDPR. Vásquez Rodríguez (2022) exemplifies how Article 5 of the LPDP is a clear reference to the GDPR. Albornoz (2022) mentions that the Ecuadorian law incorporates GDPR criteria, demonstrating its influence in the region. In the United States, the adoption of regulatory measures in states like Utah, Virginia, Colorado, and Connecticut reflects the growing concern for personal data protection. Chander (2017) underscores the lack of ethics in artificial intelligence, highlighting the need for regulation that considers both technical and ethical aspects,

4. Discussion

The convergence between artificial intelligence (AI) and privacy protection on social media platforms emerges as a topic of paramount interest in academic, legislative, and social spheres. This study focuses on exploring this relationship and its implications, considering the exponential growth of AI in various aspects of contemporary life and the substantial challenges it poses for safeguarding users' personal information. The following section serves as a dialogue space among diverse researchers who have addressed this topic, examining the underlying mechanisms of privacy breaches and the regulatory measures designed to mitigate their effects.

This analysis helps to understand how the continuous expansion of AI in different areas of daily life, from online advertising to automated decision-making, creates a complex network of interactions that directly impact individuals' privacy. In this context, the present discussion aims to deepen the understanding of the dynamics underlying this intersection between AI and privacy, recognizing the imperative need to adopt comprehensive and effective approaches to protect personal information in the digital environment.

Through a systematic review of 90 selected studies, the main research question and its associated sub-questions were addressed. These questions are: How does artificial intelligence violate the right to privacy on social media? What techniques does artificial intelligence use to collect and analyze personal data on social media? How do these techniques contribute to privacy violations such as the creation of fake identities and hacking? What are the current regulatory measures aimed at protecting user privacy against these technologies?

In this regard, this contribution intersects theories and studies to generate existing knowledge about the intersection between AI and privacy on social media, offering a critical and contextualized view of the ethical, legal, and social implications of this emerging phenomenon. Through a rigorous evaluation of the relevant academic literature, it is hoped to contribute to the development of regulatory frameworks and public policies that ensure adequate protection of individual rights in the constantly evolving digital environment. This discussion starts from answering the questions posed in the study in line with the different voices of the authors of the texts recovered in the process of searching, filtering, and selecting the study texts.

Question 1: How does artificial intelligence violate the right to privacy on social media?

The issue of how artificial intelligence (AI) violates the right to privacy on social media is a complex and multifaceted topic, as demonstrated by various recent studies that, although addressing different aspects, converge on the need for a holistic approach to tackle these challenges. Villaronga et al. (2018) highlight that data deletion in database-driven environments presents significant challenges, particularly in terms of the quality of the results obtained. In their study, the deletion of individual data points did not show a considerable impact on a large scale; however, they point out that the random deletion used in the experiments does not adequately reflect real cases, where individuals requesting deletion may share common characteristics that, when removed, could differently affect the data set. This finding suggests that data deletion is not only a technical issue but also an ethical and practical challenge in privacy protection.

In parallel, Vásquez & José Alberto (2021) address the importance of human control as an emerging right in the context of AI. They highlight that artificial intelligence can significantly impact fundamental rights such as equality, privacy, due process, and freedom of expression. According to their study, protecting personal data in the use of AI is crucial, and they express concern about potential privacy violations due to the mass collection of data by AI systems. This study underscores the need for stricter regulations and user training to understand the algorithms that impact their daily lives. These results complement Villaronga et al.'s findings, showing that concerns about privacy and data integrity are not only technical issues but also widely recognized social demands. Both studies agree on the urgency of protecting privacy, though they differ in focus: one centers on technical challenges and the other on the need for human control and regulations.

On the other hand, the study by Biesaga et al. (2023) offers a perspective on how the pandemic has influenced European narratives about smart cities and surveillance, using a quantitative analysis of 184 press articles. They identified dominant narratives including AI regulation and facial recognition, technological combat against climate emergencies, contact-tracing applications, and the potential of 5G technology to drive digitalization processes. The study highlights that privacy and surveillance concerns are central in two of the four narratives discovered, and that privacy and surveillance are often considered a "necessary evil" to maintain the EU's competitiveness in the global technological rivalry. However, narratives related to social welfare and the transparency of new policies are almost non-existent. This analysis reveals a polarization in perceptions of surveillance, indicating that the debate on privacy and AI is both media-driven and social. Biesaga's findings complement previous studies by adding a media and social dimension, showing how privacy and surveillance are perceived and discussed in the public sphere.

However, Raab (2020) and Kosta (2022) accentuate in their studies that the problem lies in the misuse of this technological tool by society, which puts the security and integrity of users at risk. They also point out that stricter regulations are necessary to protect online privacy and prevent potential abuses by tech companies. This aligns with Vera (2019) and Hueso & Valencia (2020), who state that social media, especially Facebook, misuses users' personal data and, along with the use of AI in social media and advanced data processing techniques, poses serious privacy challenges. According to the cited authors, it is essential to conduct an ethical and legal review of the use of algorithms, data analysis, and the treatment of social media users' databases without their explicit consent (Kosta, 2022). Companies must obtain clear and informed consent from users, ensuring the confidentiality and security of information. Additionally, Pew Center (2024) indicates that it is crucial to implement transparency and accountability mechanisms, allowing users to understand and question algorithmic decisions. Promoting ethical awareness through education and the development of clear policies is also essential to address issues such as algorithmic bias and social responsibility.

Finally, Hoxhaj (2023) focuses on the legal framework of the General Data Protection Regulation (GDPR) in the European Union, highlighting the need for a responsible and GDPR-compliant approach to AI development. He emphasizes that the principles of legality, fairness, transparency, and data minimization are fundamental to ensuring that AI applications respect individual privacy and data protection rights. This study stresses the urgency of adopting ethical guidelines and regulatory measures, advocating for the safeguarding of human rights and dignity in an AI-driven world. Thus, AI poses significant challenges to the right to privacy on social media, extending beyond technical aspects to include ethical, social, and legal dimensions. While technical issues of data deletion are highlighted, the need for human control and data protection is also emphasized, revealing the complexity of social narratives about privacy and surveillance. Ultimately, there is a need for a clear legal and ethical framework to address this issue.

Question 2: What techniques does artificial intelligence use to collect and analyze personal data on social media?

According to the findings of Zhang et al. (2021), who analyzed a vast corpus of literature on AI ethics and privacy, multiple techniques and ethical concerns were identified. Their study highlighted 27 AI techniques and the interconnection between techniques, ethical concerns, and social issues in the medical and health fields. This approach aligns with the study by Goncalves et al. (2024), which also emphasizes the use of machine learning algorithms in neuromarketing, a field that significantly benefits from AI for consumer preference segmentation and targeting. Both studies underscore the importance and positive impact of AI in optimizing processes and making data-driven decisions.

On the other hand, Kosta (2022), and Kim & Routledge (2022), address the ethical and privacy challenges posed by machine learning algorithms. Kosta highlights the limitations of traditional safeguards against algorithmic surveillance and the biases embedded in algorithms, which aligns with Kim and Routledge's concern about the need for ex post explanations and transparency in data use. Both studies suggest that although AI techniques offer significant advantages, their application in the collection and analysis of personal data must be carefully managed to protect individual rights and ensure fairness in algorithmic outcomes.

Conversely, Devia (2019) provides an overview of how AI and Big Data have transformed large-scale data analysis, highlighting AI's predictive capabilities in areas such as content personalization and automated decision-making. This viewpoint complements the findings of Zhang et al. and Goncalves et al., as all recognize AI's potential to improve accuracy and effectiveness in various applications through advanced data analysis. However, Devia also emphasizes the need for ethical and responsible use, a concern shared by Kosta and Kim & Routledge.

Additionally, Shaik et al. (2022) introduce the concept of federated learning, an advanced technique that allows for the collection and analysis of personal data without centralizing it. This methodology offers an innovative solution to the privacy concerns highlighted by Kosta and Kim & Routledge. By decentralizing data analysis, federated learning can mitigate some of the risks associated with state surveillance and data manipulation by companies, providing an additional layer of protection for individual privacy.

Economic transactions involve the sale of personal data to third parties who use it for various commercial purposes. These transactions can range from selling information to marketing companies to sharing data with financial entities to assess individuals' creditworthiness. This economic use of data poses serious privacy risks, as it often occurs without the users' knowledge or explicit consent (Van Bekkum & Borgesius, 2021).

Moreover, Lamchek (2023) indicates how the monetization of personal data can lead to significant abuses without an adequate regulatory framework to protect individuals. Van Bekkum & Borgesius (2021) add that fraud detection systems, though well-intentioned, often compromise privacy by processing data indiscriminately. These systems can analyze large volumes of personal data to identify suspicious patterns, resulting in excessive surveillance and automated decision-making that negatively affects users without allowing them to intervene or correct errors.

The implementation of AI systems in fraud detection, such as the SyRI case in the Netherlands analyzed by Van Bekkum & Borgesius (2021), shows how these technologies can violate privacy if not implemented with adequate safeguards. The court determined that the SyRI system was illegal because it did not respect the right to privacy under the European Convention on Human Rights. Aloisi & De Stefano (2023) del ve into how the lack of transparency in AI algorithms can result in detailed user profiling, sometimes leading to discrimination and manipulation. Finally, Miyashita (2020) emphasizes that current regulations, although progressive, do not always keep pace with AI's emerging capabilities, leaving significant gaps in privacy protection.

Thus, the growing integration of artificial intelligence in various social media applications and fraud detection systems highlights the urgent need for robust regulatory frameworks to address the ethical and legal challenges associated with these technologies. The lack of transparency and indiscriminate use of personal data without adequate consent undermine user trust and can lead to significant abuses. It is imperative that legislation evolves alongside technological developments to ensure that privacy rights are respected and effectively protected.

In this context, several techniques are used by AI to collect and analyze personal data on social media. Machine learning and natural language processing are widely employed by AI to collect and analyze large volumes of data on social media. Kim & Routledge (2022) examine how these methods can compromise privacy by monitoring and predicting behaviors without the user's explicit knowledge. Kosta (2022) adds that data collection through AI often lacks the necessary safeguards to protect against the misuse of information. Additionally, Raab (2020) and Lamchek (2023) discuss how the lack of clear regulations allows entities to exploit these data without adequate ethical constraints.

Question 3: How do these techniques contribute to privacy violations such as the creation of fake identities and hacking?

The evolution of artificial intelligence (AI) techniques and their increasing adoption in various fields have generated significant concerns regarding the privacy and security of personal data. Various studies and authors have explored how these technologies can contribute to privacy violations, such as the creation of fake identities and hacking.

According to Vásquez & José Alberto (2021), designing AI systems that comply with existing laws and protect user privacy is crucial. They highlight the importance of clearly understanding the processes used in building AI systems to ensure transparency and respect for human rights. This aligns with Villaronga et al. (2018), who analyze the effectiveness of the right to be forgotten in an environment where AI plays a crucial role. Despite efforts to process data deletion requests using AI algorithms, significant privacy concerns persist. This study emphasizes that while AI technologies can comply with certain privacy regulations, concerns remain about their ability to truly protect personal data in a context of continuous surveillance and potential abuse. This emphasis on transparency and legality highlights a growing concern for the ethical and legal implications of AI, particularly in terms of data privacy and security. Transparency is a recurring factor in how AI techniques can lead to the creation of fake identities and hacking, as a lack of clarity in AI processes can facilitate the misuse of personal data. Both Vásquez & José Alberto and Villaronga et al. agree on the need for transparency and regulatory compliance to ensure privacy, though Villaronga et al. additionally highlight the perceived effectiveness of AI in data protection.

Milossi et al. (2021) address the importance of explainability and transparency in AI systems, especially in automated decision-making. The ability of AI to make autonomous decisions requires a transparent process that allows individuals to understand and potentially challenge these decisions. Similarly, Raab (2020) emphasizes the importance of privacy and ethical impact assessments for emerging technologies. His study reviews how documents in this field incorporate ethical and normative principles, focusing on transparency and accountability. This ethical approach is essential to mitigate privacy violation risks, as it promotes responsibility and oversight in AI development and application. The insistence on ethics and norms by Raab aligns with the findings of Milossi and colleagues in "I Ethics: Algorithmic Determinism or Self-Determination? The GDPR Approach" and Vásquez and Toro in "The Right to Human Control: A Legal Response to Artificial Intelligence," consolidating the idea that transparency and adherence to ethical principles are fundamental for privacy in AI. This transparency is crucial to avoid abuses such as the creation of fake identities and hacking, which can occur when AI systems operate without adequate oversight and clear explainability. This point also resonates with Vásquez and Toro's observations on the need for users to have a clear understanding of AI processes, strengthening the relationship between transparency and data security.

Devia (2019) demonstrates how the collection and abusive use of personal data can lead to privacy violations. A test completed by 265,000 users allowed the extraction of sensitive data without their knowledge, showing how AI and Big Data can be exploited to create user profiles and misuse data. This example underscores the need for effective regulation to protect individuals from invasive and potentially harmful practices. The evidence presented by Devia contrasts with the aspirations of transparency and normative protection mentioned by authors like Vásquez & José Alberto (2021) and Milossi et al. (2021), highlighting the practical gaps that still exist in the implementation and oversight of these norms.

Kosta (2022) addresses the challenges that machine learning algorithms pose to the protection of individual rights. Traditional safeguards are insufficient to face the complexities of algorithmic surveillance, which can include biases and a lack of transparency. These issues can facilitate the creation of fake identities and hacking, as biased algorithms can misinterpret or manipulate data in ways that compromise users' privacy and security. This analysis aligns with the ethical and transparency concerns highlighted by Raab, as well as the need for explainability mentioned by Milossi and colleagues, underscoring those traditional solutions may be insufficient for the new challenges posed by AI.

A practical case is the judicial ruling on the SyRI legislation in the Netherlands, analyzed by Van Bekkum & Borgesius (2021), which reveals how a lack of transparency in technology can lead to privacy violations. The legislation was declared illegal due to its opacity and invasion of citizens' private lives, highlighting the high risk of privacy violations associated with the use of deep learning and data mining technologies. This practical case concretely illustrates the theoretical risks mentioned by other authors, consolidating the shared concern about the lack of transparency and its direct impact on privacy. Finally, Cardiell (2021) discusses the impact of humanoid robots on human privacy, highlighting how interaction with these technologies can expose personal information. Humanoid robots, equipped with multiple functionalities, increase the exposure of personal data, raising concerns about information control and privacy. This analysis complements previous studies by introducing a more tangible dimension of human-technology interaction and its implications for privacy.

This analysis demonstrates a consensus on the need for transparency and effective regulation to protect privacy in the use of AI techniques. Although these technologies can comply with certain regulations and offer significant benefits, a lack of adequate oversight and transparency can facilitate privacy violations, such as the creation of fake identities and hacking. Integrating ethical principles and adopting robust safeguards are essential to mitigate these risks and protect individuals' rights in an increasingly complex digital environment. The agreements among authors highlight the importance of transparency and ethics, while discrepancies point out the practical gaps that still need to be addressed to achieve effective privacy protection in the realm of AI.

Question 4: What are the current regulatory measures aimed at protecting user privacy against these technologies?

The protection of user privacy against artificial intelligence (AI) technologies is a critical issue in the digital age. Various studies have explored existing regulatory measures and user perceptions of privacy, revealing both challenges and significant advancements in this area. For example, Moratinos & Parrilla (2020) address the importance of transparency and adherence to ethical principles in the use of AI systems, highlighting the need to provide comprehensible information about the functioning of these systems to ensure privacy protection. This need for transparency is also reflected in the findings of Adams et al. (2023), who note that many users are unaware of how their personal data is used on online platforms. Both studies emphasize the importance of transparency and human oversight in the development and use of AI technologies, suggesting that regulatory measures should include clear requirements for disclosing information about the functioning of these systems and the use of personal data.

Additionally, Niklas (2021) reinforces the need to implement clear regulations and ethical safeguards to protect users and ensure that AI is used responsibly and equitably. This call to action is based on the growing concern about privacy and potential abuses in data collection. The findings of Miyashita (2021) on the risks associated with the exploitation of personal data underscore the importance of such regulations. Furthermore, Devia (2019) argues that without proper informed consent, data collection practices can be seen as invasive and ethically questionable.

In this context, the importance of informed consent is another recurring theme. Miyashita (2021) highlights that privacy policies are so lengthy and complex that a person would need to spend 244 hours a year reading them, making it difficult to effectively control their consent. This challenge is complemented by the findings of Adams et al. (2023), where many users provide personal information without fully understanding their rights. Both studies suggest that regulatory measures should simplify and make privacy policies more accessible to facilitate real informed consent. This could include the development of standardized formats and executive summaries that allow users to quickly understand how their data will be used. Additionally, companies should implement clear and transparent measures to protect user privacy, such as data encryption and limiting access to personal information. This would promote a culture of respect for privacy and ensure that users can make informed decisions about the use of their personal data.

On the other hand, Haitsma and Miyashita address the risk of algorithmic discrimination. Haitsma (2023) points out the challenges in excluding sensitive data in profiling based on PNR data and the difficulty in ensuring the accuracy and non-discrimination of the collected data. Miyashita (2021) also mentions the risk of unintentional discrimination due to biases embedded in AI systems. Both studies suggest that regulatory measures should include requirements for statistical analysis and regular audits of AI systems to identify and mitigate potential discrimination. Implementing bias analysis techniques and including impact assessments on privacy and discrimination in the development of these systems are crucial to addressing these challenges.

Additionally, studies by Villaronga et al. (2018) explore the technical challenges of complying with the requirements of the right to be forgotten in AI environments, highlighting that technology companies face technical difficulties and consider it impossible to fully meet these legal objectives. These technical and legal challenges underscore the need for an interdisciplinary approach to develop effective solutions. Regulatory measures could include the development of new technologies that facilitate data deletion and the creation of legal frameworks that consider current technical limitations.

Regarding the social and economic impact of AI, Abe & Eurallyah (2022) focus on the impact of AI on the labor market and human rights in Africa, noting that surveillance systems limit privacy and that automation could result in significant job losses. These findings suggest that regulations should consider not only the protection of privacy but also the social and economic impact of AI. It is necessary to develop policies that balance technological innovation with the protection of fundamental rights and the promotion of job opportunities. Additionally, Brand (2022) notes that many ethical AI documents highlight transparency and privacy as key principles. Several documents also emphasize responsibility, fairness, and non-harm. These results indicate that most ethical AI documents focus on the impact on human rights. This study applied internationally, specifically in South Africa, covers various regulatory and ethical initiatives in the use of AI in governments of different countries on this continent, highlighting the global relevance of addressing ethical and legal challenges in this area.

Finally, studies such as those by Gorbalinskiy et al. (2023) and Autili et al. (2019) suggest the importance of a robust legal framework and the development of ethical technological solutions. Gorbalinskiy proposes developing legal aspects of human rights protection in the context of AI, while Autili and colleagues demonstrate the effectiveness of tools like EXOSOUL in improving personal data protection and ethical awareness. EXOSOUL, also known as EXOALMA in Spanish, is a tool that creates a software exoskeleton designed to manage users' ethical and privacy preferences in the digital world. This exoskeleton encapsulates personal data with rules governing its creation, use, and destruction according to the owner's preferences, thus promoting transparency and control over personal data. These proactive approaches, which empower individuals to make informed decisions and protect their digital rights, should be integrated into regulatory measures.

There are various regulatory measures in place to protect user privacy against these technologies. Although there are regulatory frameworks like the GDPR in Europe, these often fall short of addressing the complexities introduced by AI. Villaronga et al. (2018) argue that existing regulations do not adequately address the complexities introduced by AI, suggesting the need for further updates and adaptations of current laws to effectively protect user privacy in a world increasingly dominated by artificial intelligence. Furthermore, it is essential for governments and organizations to work together to develop more specific and effective regulations that address the ethical and legal challenges posed by the growing use of AI. In this regard, it is crucial to establish clear standards and oversight mechanisms to ensure that AI is used ethically and responsibly across all sectors. Otherwise, there is a risk of privacy violations and other ethical issues that could undermine trust in this emerging technology.

In Ecuador, the Organic Law on the Protection of Personal Data (LOPD) is the main regulation to ensure the privacy and integrity of citizens' personal data. This law, inspired by the GDPR, establishes fundamental principles for the transparent, fair, and secure processing of personal data and introduces the figure of the Data Protection Officer (DPO) (Rodríguez Ayuso, 2020). The 2008 Constitution of Ecuador also guarantees various fundamental rights related to privacy and data protection, reinforcing the state's commitment to protecting the privacy of its citizens.

In other Latin American countries, such as Brazil and Chile, similar laws inspired by the GDPR have been enacted to protect personal data privacy. Brazil's General Data Protection Law (LGPD) and the recent reforms regarding the ethical use of artificial intelligence in the Chilean constitution reflect a continuous effort to adapt international best practices in data protection (Contreras, 2020). Despite these advances, it is evident that regulations must continue to evolve to address the new challenges posed by AI. In this interpretation, AI undoubtedly violates the right to privacy on social networks, and current regulatory measures, while necessary, must be continually reinforced and adapted to effectively protect users' rights in the digital environment. Although addressing different aspects of this problem, all agree on the urgent need for more effective regulation adapted to emerging technological capabilities. The comparison between the studies highlights a common concern: AI, without adequate safeguards, can facilitate privacy violations on an unprecedented scale.

The analyzed studies agree on the need to ensure transparency, informed consent, and protection against algorithmic discrimination. Existing regulatory measures must evolve to address these challenges and ensure a balance between technological innovation and the protection of fundamental individual rights. Implementing ethical and privacy-focused technological solutions, such as EXOSOUL software, demonstrates the effectiveness of proactive approaches to empower individuals in protecting their digital rights. The evolution of privacy policies and the inclusion of ethical impact assessments in AI development are essential steps toward more effective and fair regulation.

Violations of privacy, such as the creation of false identities and hacks due to the sophistication of AI algorithms and the lack of adequate regulations, are critical concerns. The capability of AI to generate fake profiles and perform hacks with high precision has grown exponentially, facilitated by the fact that social media platforms' terms and conditions are often not fully understood by users. This situation puts users in a vulnerable position, where they must accept terms that allow extensive use of their personal data without the option to decline. The evolution of social media has shown that, in the past, information and informed consent were not as violated as they are today. Previously, users could more easily understand and consent to the use of their data. Today, social media platforms do not allow users to decline consent terms without losing full functionality, exacerbating the situation. It is crucial for platforms to improve the transparency and understanding of these terms to effectively protect user privacy. As technology advances, regulations must adapt to address these ethical challenges and ensure that user rights are respected.

The results of the reviewed articles highlight a universal concern about the ethical and legal implications of AI on privacy. Raab (2020) and Lamchek (2023) illustrate how current guidelines still struggle to keep pace with emerging technologies operating through social networks. Kosta (2022) points out that the challenges posed by algorithmic surveillance and data accumulation require a renewed normative approach. These studies emphasize the need for dynamic policies that can quickly adapt to technological changes. A lack of consistency in the application of existing regulations is also highlighted. Van Bekkum & Borgesius (2021) discuss that, despite legislative efforts like the GDPR, these measures are insufficient to address all the ways AI can exploit personal data. Miyashita (2021) reinforces this point by analyzing the Japanese case, showing that even in contexts with strong traditions in data protection, significant gaps exist. These findings indicate that current regulations are not robust enough to face the challenges presented by AI.

The issue of privacy on social networks and artificial intelligence (AI) is undoubtedly complex. The terms and conditions of use of these platforms are extensive and often invasive, allowing companies to collect, analyze, and use personal data in ways that many users might consider intrusive. However, it should be noted that the acceptance of these terms is voluntary. Users choose to accept these conditions by deciding to use the platforms, whether they are fully aware of the implications or not.

Most users do not take the time to read these terms and conditions. This omission is partly due to the length and complexity of the documents but also reflects a lack of ethical and moral responsibility. Many users prefer to enjoy the benefits of social media without interruptions, overlooking the potential consequences for their privacy. However, it is important to remember that by accepting these terms and conditions, users are granting certain rights to the platforms to collect and use personal data. Users should be informed about how to protect their privacy online and make conscious decisions regarding what information they share on the internet. This includes regularly reviewing privacy settings on social networks and limiting the amount of personal information shared. Ultimately, the responsibility falls on each individual to protect their privacy online and take proactive steps to ensure their digital security.

Privacy on social networks and AI is not only a technological or corporate policy issue but also reflects users' decisions and priorities. Users often complain about privacy invasions, but it is they who accept the terms without reading them and decide that the advantages of being on social networks outweigh the risks. This attitude reveals a disconnect between users' desire for privacy and their willingness to take measures that protect it. It is important to reflect on one's actions and habits online to protect privacy more effectively. Likewise, educating oneself about the implications of sharing personal information on social networks can help users make more informed and conscious decisions. Some measures to take include reviewing and adjusting privacy settings on accounts, limiting the amount of personal information shared, and being aware of who has access to the information. It is also crucial to remember that once something is shared online, it can be difficult or impossible to remove completely.

The issue of privacy in the era of AI and social networks is multifaceted. While platform policies may seem invasive, it is also true that users have the responsibility to inform themselves and make conscious decisions. Ethics and morality play a crucial role in this balance, and it is the duty of each individual to find a balance between the desire to stay connected and the need to protect their privacy. Users should reflect on how they use social networks and what information they share, always considering the potential risks and consequences. Moreover, advocating for stricter regulations that protect user privacy in an increasingly digital world is essential. Being proactive in protecting online privacy and advocating for laws that ensure data security is crucial. At the same time, educating others about the risks and benefits of sharing information on digital platforms can foster a culture of responsibility and awareness online.

5. Recommendations and Limitations for Future Research

Limitations

The present research encountered several limitations that were taken into account. Firstly, limited financial resources restricted access to certain databases, such as Web of Science and Scopus, which require a paid subscription. This meant that access to some articles was restricted unless paid for. The time available to complete the systematic literature review was another limiting factor. The research was conducted over a period of 4 months, which constrained the data collection and analysis to a relatively short time frame.

Recommendations

While the focus of this systematic literature review was on the violation of privacy by artificial intelligence on social media, other relevant topics emerged during the literature review. For instance, individual privacy and informed consent in medical areas were recurring themes that deserve further investigation. Additionally, the Cambridge Analytica case (2018) represents a significant turning point. This case highlighted not only privacy violations on social media but also the use of AI to spread false information for political purposes, affecting the right to a fair vote by manipulating the information sent to users. Although this review focused on social media, future researchers could continue exploring this case, relating it to the distortion of electoral processes and the ethical and legal implications of such practices.

6. Conclusion

The present research has addressed the interference of AI in violating individuals' privacy and social networks, a topic of growing relevance in the contemporary digital context related to the fourth wave of human rights (HR). Through a systematic review of the literature in response to the overall objective of this study, the influence of AI on social networks and its impact on individual rights were identified and analyzed. The consequences of using AI on privacy were delineated, detailing the characteristics of the data used by this technology and exploring the social, legal, and ethical aspects involved. It was found that the misuse and lack of understanding of user terms and conditions lead to these issues. The methodology implemented allowed for answering the research questions, exposing the techniques employed by AI to collect and analyze personal data, and the ways these techniques contribute to privacy violations, such as creating false identities and hacks; these are the main means by which users' information and privacy are violated. The current regulatory measures aimed at protecting user privacy are based on the GDPR, but regions like South America remain a challenge.

Additionally, the ethical implications of these practices were discussed, emphasizing the responsibility of digital platforms in ensuring the protection of their users' data. The existing regulatory measures aimed at protecting user privacy are based on the European Union's General Data Protection Regulation (GDPR), which establishes a rigorous legal framework for handling personal data. However, it was highlighted that regions such as South America still face significant challenges in implementing and complying with robust privacy regulations. The lack of equivalent regulations in these regions exposes users to greater risks of exploitation and privacy violations.

Furthermore, there is a need to strengthen privacy policies and user education on the importance of terms and conditions. Solutions should include not only technological improvements for data protection, such as implementing more secure algorithms and advanced encryption techniques, but also legislative and educational efforts to promote greater awareness and understanding among users about how their data is used. It is crucial for digital platforms to provide clear and understandable terms and conditions, avoiding technical and legal jargon that complicates understanding for the average user. In this regard, legislative efforts should focus on creating and enforcing regulations that compel companies to be transparent in their data collection and usage practices. This includes implementing regular audits and imposing significant penalties on organizations that violate privacy regulations. On the educational level, it is essential to integrate digital literacy into school curricula and conduct awareness campaigns for all ages, teaching individuals how to protect their personal information online and what practices to follow to maintain their privacy.

This holistic approach is essential to mitigate the risks associated with AI in social networks and effectively protect privacy rights in the digital age. By combining advanced technological solutions with robust regulatory frameworks and an informed citizenry, a safer and more ethical digital environment can be created. Technological solutions should include developing transparent and explainable AI systems, allowing users to understand how their data is processed and how automated decisions that affect them are made. Additionally, it is crucial to implement data protection technologies such as end-to-end encryption, anonymization techniques, and consent management tools. Solid regulatory frameworks must ensure that data protection laws and policies are up-to-date and adequate to address the emerging challenges of AI. This includes creating specific regulations for AI that address issues such as algorithmic responsibility, transparency, and accountability. Regulators must work closely with technology and ethics experts to develop guidelines that ensure the responsible and safe use of AI.

In this context, user education is equally crucial. An informed citizenry about their privacy rights and data protection practices can make more conscious and proactive decisions. It is necessary to promote digital literacy and privacy awareness from an early age, incorporating these topics into school curricula and providing accessible educational resources for all ages. Public awareness campaigns can help increase understanding of how personal data is used and how to protect it.

The contribution of this research lies in its comprehensive and up-to-date approach to the use of AI, social networks, and their consequences on privacy. Through the analysis of 90 selected articles, a detailed view of current practices and emerging challenges in this field has been provided. Furthermore, the importance of establishing robust and transparent regulatory frameworks, such as the General Data Protection Regulation in Europe and the Organic Law on Personal Data Protection in Ecuador, among others, has been emphasized to protect privacy rights in an increasingly complex digital environment.

This study has also highlighted the need for strong computer ethics and informed consent as pillars to protect individual autonomy and integrity in the use of social networks. Robust computer ethics must be comprehensive, encompassing the design and development stages of AI technologies to their implementation and use. Developers and tech companies must adhere to ethical principles that prioritize privacy, security, and user well-being. This includes creating algorithms that are not only efficient but also fair and transparent, avoiding any form of discrimination or bias.

Informed consent is equally crucial. Users must be fully aware of how their data is collected, used, and stored, and must have the ability to give or withdraw their consent clearly and easily. Social media platforms must strive to present their privacy policies and terms of service in an accessible and understandable manner, eliminating complicated technical and legal language that often confuses users. Informed consent should not be a bureaucratic formality but a continuous and meaningful process that empowers users to make informed decisions about their personal information.

The ethical and social implications of AI on individual privacy require continuous attention and a multidisciplinary approach to ensure that technological evolution benefits society without compromising fundamental rights. This implies collaboration between technologists, legislators, academics, privacy advocates, and other relevant actors to address ethical challenges comprehensively. Ethics committees and external audits can play an important role in overseeing AI practices, ensuring that ethical standards are respected and individuals' rights are protected.

It is also essential to consider the diverse perspectives and cultural contexts in the discussion about AI privacy and ethics. What may be considered acceptable in one culture or region may not be in another, so it is vital to adopt an inclusive and respectful approach to cultural differences. The participation of various stakeholders in the development and regulation of AI technologies can help ensure these variations are considered and respected. Public education and awareness also play a crucial role in this context. Increasing digital literacy and understanding privacy rights can enable individuals to participate more actively and critically in the digital ecosystem. Educational programs, workshops, and awareness campaigns can help equip users with the tools and knowledge necessary to protect their privacy and exercise their rights.

By integrating advanced technological solutions, robust regulatory frameworks, and an informed citizenry, a safer and more ethical digital environment can be achieved. This holistic approach is essential to address the complex challenges posed by AI in social networks and protect privacy rights effectively in the digital age.

7. References

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. https://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 Dartmouth 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

8. Appendices

Appendix 1 *Results matrix*

Title	Author	Coding of Sources	Year of Publication	Specific Content	Database
The right to human control: A legal response to artificial intelligence	Vásquez, CS; Toro-Valend, JA	A1	2021	Artificial Intelligence and Human Rights Violations: Supervision and Protection	Web of Science
Clarifying human rights standards through artificial intelligence initiatives	Lane, L	A2	2022	AI violates fundamental rights; human control is needed to supervise and protect these rights.	Web of Science
Artificial intelligence and moral rights	Miernicki, M; Ng, I	A3	2021	AI increases legal certainty in human rights; more clarity is needed.	Web of Science
Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten	Villaronga, EF; Kieseberg, P; Li, T	A4	2018	Artificial intelligence and moral rights.	Web of Science
Regulating Artificial Intelligence through a Human Rights-Based Approach in Africa	Abe, O; Eurallyah, AJ	A5	2022	Artificial intelligence and the right to be forgotten.	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	AI in Africa: benefits and risks for human rights.	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	AI violates rights; human control is needed to protect them.	Web of Science
AI Ethics: Algorithmic Determinism or Self-	Milossi, M; Alexandropoulou-Egyptiadou, E; Psannis, KE	A8	2021	The benefits and problems of AI require ethical guidance based on human rights.	Web of Science

Determination? The GPDR Approach					
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	The ethics of AI according to GDPR: algorithmic determinism or self-determination.	Web of Science
Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholder Guidelines	Fukuda-Parr, S; Gibbons, E	A10	2021	Algorithmic evaluation and human rights: the SyRI and GDPR case.	Web of Science
Ethics and privacy of artificial intelligence: Understandings from bibliometrics	Zhang, Y; Wu, MJ; Tian, GY; Zhang, GQ; Lu, J	A11	2021	Consensus on ethical AI: human rights critique of voluntary guidelines.	Web of Science
ALGORITHMIC INEQUALITIES: HIGH-RISK PRACTICES TO HUMAN RIGHTS	Roig, MJA	A12	2022	Ethics and privacy of AI: perspectives from bibliometrics.	Web of Science
Regulating Artificial Intelligence in International Investment Law	McLaughlin, M	A13	2023	Algorithmic inequalities: high-risk practices for human rights.	Web of Science
Information privacy, impact assessment, and the place of ethics	Raab, CD	A14	2020	Regulation of artificial intelligence in international investment law.	Web of Science
ARTIFICIAL INTELLIGENCE BIG DATA, AND DIGITAL ERA: A THREAT TO PERSONAL DATA?	Devia, AM	A15	2019	Information privacy, impact assessment, and ethics.	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	AI and big data threaten personal data; ethical regulation is needed.	Web of Science
Digital welfare fraud detection and the Dutch SyRI judgment	van Bekkum, M; Borgesius, FZ	A17	2021	Right to explain algorithmic decisions: a trust-based approach.	Web of Science
Responsible innovation ecosystems: Ethical implications of the application of the ecosystem concept to artificial intelligence	Stahl, BC	A18	2022	Digital fraud detection and the SyRI case ruling in the Netherlands.	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	Responsible innovation ecosystems: ethical implications in AI.	Web of Science
Ensuring Data Science and Its Applications Benefit Humanity: Data Monetization and the Right to Science	Lamchek, JS	A20	2023	Social rights are marginal in the EU's AI policy debate.	Web of Science
Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks	Beduschi, A	A21	2022	The right to science requires balancing data monetization and human benefits.	Web of Science
Human-centric data protection laws and policies: A lesson from Japan	Miyashita, H	A22	2021	AI can transform humanitarian action but carries significant risks.	Web of Science
Algorithmic state surveillance: Challenging the notion of agency in human rights	Kosta, E	A23	2022	Human-centric data protection in Japan emphasizes dignity.	Web of Science
From human resources to human rights: Impact assessments for hiring algorithms	Yam, J; Skorburg, JA	A24	2021	State algorithmic surveillance challenges the notion of agency in human rights.	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	Impact assessments for hiring algorithms protect human rights.	Web of Science
FREEDOM OF THOUGHT: LEGAL PROTECTION FROM MANIPULATION	Harutyunyan, D; Yeremyan, L	A26	2020	Review of tools for ethical AI system development.	Web of Science
Neuromarketing algorithms' consumer privacy and ethical considerations: challenges and opportunities	Goncalves, M; Hu, YW; Aliagas, I; Cerdá, LM	A27	2024	Freedom of thought: legal protection against manipulation.	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	Privacy and ethics in neuromarketing: challenges and opportunities with AI.	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	FedStack: Personalized activity monitoring using federated learning.	Web of Science
Future Smart Connected Communities to Fight COVID-19 Outbreak	Gupta, D; Bhatt, S; Gupta, M; Tosun, AS	A30	2021	Software exoskeleton to protect digital ethics and privacy for citizens.	Web of Science
Why converging technologies need converging international regulation	Helbing, D; Ienca, M	A31	2024	Smart communities connected to combat COVID-19 outbreaks.	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	Converging technologies require unified international regulation for ethical challenges.	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	AI disclosures under GDPR are inadequate and non-transparent.	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	Design of a card to assess AI risks in workplace health in Australia.	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	Comparative evaluation of AI regulation in the EU and North America.	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	Creating sustainable smart cities: ethics, trust, and transparency.	Web of Science
Utilizing Bio Metric System for Enhancing Cyber Security in	Khan, HU; Malik, MZ; Nazir, S; Khan, F	A37	2023	Regulation of algorithmic discrimination: the CJEU and PNR data profiling.	Web of Science

Banking Sector: A Systematic Analysis					
An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems	Mantelero A.	A38	2021	Use of biometric systems to improve cybersecurity in the banking sector: systematic analysis.	Scopus
Legal aspects of artificial intelligence in the employment process	Špadina H.	A39	2023	Evidence-based methodology for assessing human rights impact in the development of data-intensive AI systems.	Scopus
Responsible Artificial Intelligence in Government: Development of a Legal Framework for South Africa	Brand D.J.	A40	2022	Legal aspects of AI in the employment process.	Scopus
Ensuring Data Science and Its Applications Benefit Humanity: Data Monetization and the Right to Science	Lamchek J.S.	A41	2023	Responsible AI in government: developing a legal framework for South Africa.	Scopus
Personal Identity in the Metaverse: Challenges and Risks	Mitrushchenkova A.N.	A42	2022	Ensuring data science benefits humanity: data monetization and the right to science.	Scopus
What rights matter? Examining the place of social rights in the EU's artificial intelligence policy debate	Niklas J.	A43	2021	Personal identity in the metaverse: challenges and risks.	Scopus
Social and Legal Risks of Artificial Intelligence: An Analytical Stu	Al-Tkhayneh K.M.	A44	2023	What rights matter? Assessment of social rights in the EU's AI policy.	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	Social and legal risks of AI: an analytical study.	Scopus
"Humanity's new frontier": Human rights implications of artificial intelligence and new technologies	Nagy N.	A46	2024	Mitigating risks and labor rights: transatlantic AI regulation.	Scopus

Artificial intelligence: a claim for strict liability for human rights violations*	Fernandes Barbosa L.V.	A47	2023	"New frontier of humanity": human rights implications of AI and new technologies.	Scopus
From human resources to human rights: Impact assessments for hiring algorithms	Yam J.	A48	2021	AI: demand for strict liability for human rights violations.	Scopus
Exploring the impacts of artificial intelligence on freedom of religion or belief online	Ashraf C.	A49	2022	From human resources to human rights: impact assessments for hiring algorithms.	Scopus
A Framework for Systematically Applying Humanistic Ethics when Using AI as a Design Material	Dent K.	A50	2019	AI impacts on freedom of religion or belief online.	Scopus
The Bayes model for the protection of human interest	Zharova A.	A51	2023	Framework for systematically applying humanist ethics in AI design.	Scopus
Contesting border artificial intelligence: Applying the guidance-ethics approach as a responsible design lens	La Fors K.	A52	2022	The Bayesian model for protecting human interests.	Scopus
Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten	Villaronga E.F.	A53	2018	Questioning frontier artificial intelligence: applying the ethics guide approach as a lens for responsible design.	Scopus
Applying the ethics of AI: a systematic review of tools for developing and accessing AI-based systems	Ortega-Bolaños R.	A54	2024	Artificial intelligence and the right to be forgotten.	Scopus
Towards Industrial Revolution 5.0 and Explainable Artificial Intelligence: Challenges and Opportunities	Taj I.	A55	2022	Review of ethical tools for developing and evaluating AI systems.	Scopus
Human Rights Dilemma and International Rule of Law in the Age of Digital Intelligence	Xing A.	A56	2024	Towards Industrial Revolution 5.0 and explainable artificial intelligence: challenges and opportunities.	Scopus
Generative AI and deepfakes: a human rights approach to tackling harmful content	Romero Moreno F.	A57	2024	Human rights dilemma and the rule of international law in the digital intelligence era.	Scopus

Regulating around freedom in the “forum Internum”	Alegre S.	A58	2021	Generative AI and deepfakes: a human rights approach to addressing harmful content.	Scopus
Information privacy, impact assessment, and the place of ethics *	Raab C.D.	A59	2020	Regulation around freedom in the "forum internum."	Scopus
REPLIKA AND THE EMOTIONAL ARTIFICIAL INTELLIGENCE COMPANY: The ethical and social challenges of company chatbots	Gutiérrez J.L.M.	A60	2022	Information privacy, impact assessment, and the place of ethics.	Scopus
Why converging technologies need converging international regulation	Helbing D.	A61	2024	REPLIKA and the emotional AI company: the ethical and social challenges of the company's chatbots.	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	Why converging technologies need convergent international regulation.	Scopus
Platform Law and Platform Solutions in the Fight against the Pandemic	Altoukhov A.V.	A63	2021	Automated decision-making in EU member states: the right to explanation and other "appropriate safeguards" in national legislation.	Scopus
FREEDOM AS AN ISSUE IN THE CONTEXT OF TRANSHUMANISM AND ARTIFICIAL INTELLIGENCE, DIGITALIZATION, AND ROBOTICS (AIDR)	Dağ A.	A64	2023	Platform Law and Platform Solutions in the Fight Against the Pandemic.	Scopus
Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective	Deeb-Swihart J.	A65	2022	Freedom as an issue in the context of transhumanism and artificial intelligence, digitization, and robotics (AIDR).	Scopus
Applying ethics to AI in the workplace: the design of a scorecard for Australian workplace health and safety	Cebulla A.	A66	2023	Ethical tensions in AI applications to address human trafficking: a human rights perspective.	Scopus

The right to the privacy of personal data in the digital age	Díaz M.F.S.	A67	2023	Applying ethics to AI in the workplace: designing a dashboard for occupational health and safety in Australia.	Scopus
Artificial intelligence, big data and applications against Covid-19, and privacy and data protection	Hueso L.C.	A68	2020	The right to privacy of personal data in the digital age.	Scopus
Artificial intelligence in healthcare: Threats to the fundamental values of our society	Zikmundová K.	A69	2022	Artificial intelligence, big data, and COVID-19 applications, and privacy and data protection.	Scopus
The emergence of “truth machines”? Artificial intelligence approaches to lie detection	Oravec J.A.	A70	2022	Artificial intelligence in healthcare: threats to the fundamental values of our society.	Scopus
Algorithmic valuation before human rights and the European Convention on Human Rights and the General Data Protection Regulation: The SyRI case	Moratinos G.L.	A71	2020	The emergence of "truth machines": AI approaches to lie detection.	Scopus
Ensuring Human Rights in the Era of Artificial Intelligence: Ukraine and Practice of ECHR	Gorbalinskiy V.	A72	2023	Algorithmic evaluation of human rights and the European Convention on Human Rights and GDPR: the SyRI case.	Scopus
The right to human control: A legal response to artificial intelligence	Vásquez C.S.	A73	2021	Ensuring human rights in the era of artificial intelligence: Ukraine and the ECHR practice.	Scopus
“A robot is watching you”: Humanoid robots and the different impacts on human privacy	Cardiell L.	A74	2021	The right to human control: a legal response to artificial intelligence.	Scopus
Ethical principles for artificial intelligence in K-12 education	Adams C.	A75	2023	A robot is watching you: humanoid robots and the different impacts on human privacy.	Scopus
AI in education: learner choice and fundamental rights	Berendt B.	A76	2020	Ethical principles for artificial intelligence in K-12 education.	Scopus
Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks	Beduschi A.	A77	2022	AI in education: student choice and fundamental rights.	Scopus

Regulating Artificial Intelligence through a Human Rights-Based Approach in Africa	Abe O.	A78	2021	Leveraging AI potential for humanitarian action: opportunities and risks.	Scopus
The effect of the pandemic on European narratives on smart cities and surveillance	Biesaga M.	A79	2023	Regulation of artificial intelligence through a human rights-based approach in Africa.	Scopus
Research design for an integrated Artificial Intelligence ethical framework	Karatzogianni A.	A80	2021	The effect of the pandemic on European narratives on smart cities and surveillance.	Scopus
Digital welfare fraud detection and the Dutch SyRI judgment	van Bekkum M.	A81	2021	Research design for an integrated ethical framework for artificial intelligence.	Scopus
ETHICAL IMPLICATIONS AND HUMAN RIGHTS VIOLATIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE	Hoxhaj O.	A82	2023	Digital welfare fraud detection and the SyRI ruling in the Netherlands.	Scopus
Responsible living labs: what can go wrong?	Habibipour A.	A83	2024	Ethical implications and human rights violations in the era of artificial intelligence.	Scopus
Emerging Consensus on ‘Ethical AI’: Human Rights Critique of Stakeholder Guidelines	Fukuda-Parr S.	A84	2021	Responsible living labs: what can go wrong?	Scopus
CLARIFYING HUMAN RIGHTS STANDARDS THROUGH ARTIFICIAL INTELLIGENCE INITIATIVES	Lane L.	A85	2022	Emerging consensus on 'ethical AI': human rights critique of stakeholder guidelines.	Scopus
Delineating privacy aspects of COVID tracing applications embedded with proximity measurement technologies & digital technologies	Saheb T.	A86	2022	Clarifying human rights standards through AI initiatives.	Scopus
Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach	Kim T.W.	A87	2022	Delimiting privacy aspects of COVID-19 tracking applications integrated with proximity measurement and digital technologies.	Scopus

How to Create and Foster Sustainable Smart Cities? Insights on Ethics, Trust, Privacy, Transparency, Incentives, and Success	Riedmann-Streitz C.	A88	2024	Why there should be a right to an explanation of algorithmic decision-making: a trust-based approach.	Scopus
Video Surveillance and Privacy: A Solvable Paradox?	Cucchiara R.	A89	2024	How to create and foster sustainable smart cities: insights on ethics, trust, privacy, transparency, incentives, and success.	Scopus
Collaboration among recruiters and artificial intelligence: removing human prejudices in employment	Chen Z.	A90	2023	Video surveillance and privacy: a solvable paradox?	Scopus