

Artificial Intelligence; a Threat to the Right of Digital Privacy in Pakistan



Submitted by:

RIDA BATOOL

Reg no: 367-FSL/LLMHRL/S23

Supervised By:

Ma'am Atia Madni

Thesis submitted in the partial fulfilment of the requirements for the degree of

Department of Law

Faculty of Shariah & Law

International Islamic University Islamabad

Abstract

The uprising of artificial intelligence around the globe has created serious concern regarding the digital privacy rights, Pakistan with no exception, also becomes prone to this major issue. The alarming concerns come from the AI technology which is a by-product of the artificial intelligence, it creates realistic or exact replica images or videos of people without their absolute consent and puts the privacy of people around the world at stake. As there are continuous developments taking place in the AI technology it has become inevitable to create laws and to evaluate the serious threats probably relating to digital privacy of people. Many countries notably the European Union, the United States of America and India have faced such issues and have implemented digital privacy laws to curb the overall artificial intelligence threat to digital privacy. In Pakistan, few incomplete legal initiative have been taken to handle the menace of Artificial intelligence but due to weak enforceability, they are not effective to protect the digital privacy of citizens which as declared to be a fundamental right. This research critically analyses relevant digital privacy Protection And concludes that existing legal framework relevant to digital privacy laws are inadequate and need amendments.

Acknowledgement

I would like to express my sincere gratitude to Almighty Allah for His guidance, strength, and blessings throughout my academic journey. His support enabled me to overcome challenges and complete my degree, and I continue to place my trust in Him for the future. I also wish to convey my deepest appreciation to my supervisor, Ma'am Atia Madni, for her invaluable guidance, continuous support, and constructive feedback at every stage of this thesis. Her encouragement and mentorship made this work possible. Finally, I extend my heartfelt thanks to my father and mother for their unwavering love, encouragement, and support throughout my degree. Their prayers and strength have been my foundation. This work is dedicated to my parents.

Table of Contents

Abstract	i
Acknowledgement	ii
CHAPTER 01: INTRODUCTION	1
1.1 Thesis Statement	1
1.2 Background	1
1.3 Literature Review	3
1.4 Research Questions	9
1.5 The Scope of Research	10
1.6 Significance of Research	10
1.7 Research Methodology	12
CHAPTER 02: UNDERSTANDING DIGITAL PRIVACY AND THE INFLUENCE OF ARTIFICIAL INTELLIGENCE	13
2.1 Introduction	13
2.2 Defining Privacy and Digital Privacy	13
2.3 Core Principles of Digital Privacy	14
2.4 Artificial Intelligence and Digital Privacy Rights	16
2.4.1 Defining the term Artificial Intelligence	17
2.4.2 Applications of Artificial Intelligence	17
2.4.3 How Artificial Intelligence Can Strengthen Privacy	20
2.4.4 Privacy Threats concerned with Artificial Intelligence	22
2.5 Artificial Intelligence Reinforcing Digital Privacy	24
2.5.1. AI for Security and Privacy	25
2.5.2. Malware mitigation and intrusion/anomaly detection	25
2.5.3. Software and application security	25

2.6 Conclusion.....	26
Chapter 03: GLOBAL LEGAL FRAMEWORK FOR DIGITAL PRIVACY AND ARTIFICIAL INTELLIGENCE.....	27
3.1 Introduction	27
3.2 Laws Governing Digital Privacy Rights Internationally.....	27
3.3 United Nations’ Framework for AI and Privacy Governance.....	29
3.4 Digital privacy Laws in the United States of America.....	31
3.5 The European Union’s Artificial Intelligence Act (AI Act) 2024 and The General Data Protection Regulation (GDPR) 2018.....	34
3.6 Digital Privacy Laws in India and the emergence of Artificial Intelligence.....	35
3.7 Synthesis: Governance Models, Structural Gaps, and Future Directions	37
3.8 Conclusion.....	38
Chapter 04: Digital Privacy Rights in Pakistan: Challenges and Implications of Artificial Intelligence.....	40
4.1 Introduction	40
4.2 An Overview of Digital Privacy Laws in Pakistan	40
4.3 Prevention of Electronic Crimes Act 2016	42
4.4 The Personal Data Protection Bill 2021	44
4.5 The Personal Data Protection Bill 2023.....	44
4.6 Regulation of Artificial Intelligence Act 2024 (Bill)	46
4.7 Impact of AI on Digital privacy in Pakistan	47
4.8 Comparative Analysis of Digital Privacy Laws amidst Global AI Regulations	49
4.9 Conclusion.....	53
Chapter 5: Conclusion and Recommendations	55
5.1 Conclusion.....	55

CHAPTER 01: INTRODUCTION

1.1 Thesis Statement

The unregulated use of AI poses serious threats to the right of digital privacy in Pakistan; hence, there is a dire need to evaluate the existing legal framework to protect digital privacy rights.

1.2 Background

The concept of privacy of an individual which is the utmost fundamental aspect of human dignity, has its historical roots and still evolves in the modern age, especially in relation to developing digital technologies. The ancient religious and legal traditions contain clear signs of respect for personal boundaries and confidentiality. In the Islamic teachings, the Quran warns against spying and intruding upon others' private matters, specifying the sanctity of personal space. One notable verse number 27 of Surah Noor in the Holy Quran advice the believers not to enter the houses other than their own without permission, showcasing that such actions are neither righteous nor respectful of human dignity. Same has been discussed in the Code of Hammurabi, one of the earliest known legal systems, included clauses prohibiting unauthorized entry into private homes, reflecting the societal recognition of individual space and boundaries. Across many ancient Hebrew and Greek cultures, these ideas were followed through various social and religious practices that highlighted the value of personal integrity and protected the sanctity of the home.¹

Primarily, privacy is the fundamental right of a person to keep their personal life, choices, and information protected from unwanted attention or access. It grants people to decide what they want to share and with whom. In today's digital world, this idea becomes even more important because so much of our personal data is stored and used online. While digital privacy means keeping personal details like names, photos, locations, and online behavior safe when using the internet or electronic devices, it also helps to protect people from misuse of their information, such as being tracked, profiled, or targeted without their permission.²

Despite its long-standing significance, privacy remains a complex and often contested concept. It varies in interpretation based on legal, social, and cultural contexts. Legal scholar Alan

¹ Alan F. Westin, "Privacy and Freedom," *Washington and Lee Law Review* 25, no. 1 (1968): 166, <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>.

² Colin J. Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments* (Cambridge, MA: MIT Press, 2006), <https://mitpress.mit.edu/9780262524537/the-governance-of-privacy/>.

Westin described privacy as the basic right of individuals and institutions to control how information about them is shared and to what extent. In the digital age, privacy has come to be closely associated with data protection, especially in contexts involving online transactions and the processing of personal information. As technology becomes a bigger part of our lives, protecting digital privacy is necessary to make sure people feel secure and respected in the online world. According to digital futurist Mark van Rijmenam, the more dependent society becomes on digital systems, the more vulnerable personal data becomes to misuse.³ This statement captures the tension between convenience and control in the modern data economy. In the context of Pakistan, privacy is acknowledged at a constitutional level but remains inadequately defined and protected in practical terms. The Constitution of the Islamic Republic of Pakistan 1973, Article 17 enshrines that man's dignity and the privacy of the home are inevitable, subject to the law of the state. However, this legal provision is limited in scope, as it lacks clarity regarding digital protection and securing the personal information. The Prevention of Electronic Crimes Act of 2016⁴, enacted by the Government of Pakistan, addresses cybercrimes such as unauthorized access to data. While this legislation offers some safeguards, it does not sufficiently account for privacy issues arising from artificial intelligence and advanced data processing systems. The mere lack of comprehensive legislation becomes especially concerning when one considers the impact of artificial intelligence in shaping modern data digital practices.

The global context illustrates the urgency of addressal of the privacy challenges in the age of growing impact of the artificial intelligence on the lives of individuals. The countries like those in the European Union have implemented strong legal regulations such as the General Data Protection Regulation 2018, which offers comprehensive protections for individuals' data rights. Also, India has passed the Digital Personal Data Protection Act 2024 to regulate data collection and ensure accountability. While Pakistan continues to lag behind, both in legislative development and public awareness. Additionally, the lack of enforcement mechanisms, along

³ Mark van Rijmenam, "Privacy in the Age of AI: Risks, Challenges, and Solutions," *Digital Futures*, <https://www.vanrijmenam.com/privacy-age-ai>.

⁴ Pakistan, *The Prevention of the Electronic Crimes Act*, 2016, http://www.na.gov.pk/uploads/documents/1479121891_284.pdf

with limited digital literacy, leaves Pakistani citizens particularly vulnerable.⁵ In an attempt to overview these gaps, a draft Personal Data Protection Bill in 2023 was introduced. This bill establishes rules for data collection, processing, and storage, while also proposing the formation of an authority to oversee compliance. But, as of now, it remains unenforced.

Along with the draft data protection bill, the same ministry introduced a draft National Artificial Intelligence Policy in 2023, which provide a dedicated directorate to regulate the artificial technologies.⁶ As this policy provides ethical guidelines and discuss the need for responsible data use, it similarly lacks the force of law. Without the legislative backing in Pakistan, such initiatives remain advisory in nature and fail to guarantee accountability. This vacuum is dangerous, as Pakistan increasingly relies on digital systems for everything from financial transactions to national identity management. The rising wave of artificial intelligence is surely a menace with regard to the digital privacy of the citizens of Pakistan. All in all, in Pakistan, protecting digital privacy is becoming more difficult due to outdated legal protections and the rising use of artificial intelligence. Although the Prevention of Electronic Crimes Act of 2016 was created to deal with cybercrimes, it does not cover many new problems caused by AI, such as misuse of personal information or unfair data profiling. The proposed Personal Data Protection Bill of 2023 is a step toward setting rules for handling personal data, but it has not yet been passed into law. As a result, private data remains exposed to possible abuse of artificial intelligence. To protect citizens and ensure the safe use of technology, Pakistan needs to formulate stronger legal safeguards similar to those already in place in countries that are leading in digital privacy against Artificial Intelligence interference.

1.3 Literature Review

The right to the privacy is widely considered as a fundamental human right, firmly embedded in multiple national and international human rights instruments and national constitutions. The Universal Declaration of Human Rights, presented by the United Nations General Assembly in 1948, enshrines the right to privacy in its Article 12, stressing the necessity of protection against arbitrary intrusions into the private life of individual, family, home, or correspondence.

⁵ S. Rehman, "Pakistan's Data Protection Overview," RIAA Barker Gillette, 2021, <https://www.dataguidance.com/notes/pakistan-data-protection-overview-0>.

⁶ Ministry of Information Technology and Telecommunication of Pakistan, *Draft of the Personal Data Protection Bill Presented in Senate*, 2023, <https://moitt.gov.pk/SiteImage/Misc/files/PDP%20Bill%202023.pdf>

In a similar vein, the International Covenant on Civil and Political Rights, passed by the UN General Assembly in 1966, reaffirms this principle in its Article 17, showcasing the need to protect individuals from unlawful interference in their personal and familial spheres, as well as upholding the dignity of one's honor and reputation.

Syed Raza Shah Gilani, in his article titled “Right to Privacy and the Growing Scope of Artificial Intelligence”⁷ published in *Journal Current Trends in Law and Society* in September 2023 argued that, Rapid advancement of artificial intelligence (AI) technology poses significant challenges to the fundamental right to privacy. With Artificial Intelligence becoming highly placed into our daily lives, there is an urgent need to understand and safeguard privacy rights in the digital age. Concerns arise from the use of AI-driven tools like facial recognition, biometric identification, and predictive analysis, which raise fears of privacy infringements. The widespread adoption of AI presents both opportunities and hurdles in upholding privacy rights. As AI continues to evolve, it's crucial to strike a delicate balance between leveraging its benefits and protecting fundamental individual privacy rights. The Author generally discussed the Growing Scope of Artificial Intelligence but has not

specifically addressed in-depth exploration of the ethical aspects of emerging technologies including issues like algorithmic bias and discrimination. The literature also lacks longitudinal studies that track the evolving relationship between AI and privacy over time. Whereas the article broadly discusses AI's ethical implications but lacks specific examples of privacy threats caused by AI or detailed recommendations for regulatory frameworks to protect privacy. This research supports the current research by addressing AI's privacy implications, which will be further examined with a focus on ethical and regulatory aspects.

Hitmi Khalifa Alhitmi and co-authors in their article titled “Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions,”⁸ explored how the growing use of artificial intelligence in marketing raises

⁷ Syed Raza Shah Gilani, “The Right of Privacy and the Growing Scope of Intelligence,” *Current Trends in Law and Society* 3, no. 1 (2023): 1–11, <https://doi.org/10.52131/ctls.2023.0301.0011>.

⁸ Hitmi Khalifa Alhitmi, et.al, *Data Security and Privacy Concerns of AI-Driven Marketing in the Context of Economics and Business Field: An Exploration into Possible Solutions* (20 August 2024), <https://doi.org/10.1080/23311975.2024.2393743>.

serious data privacy and security concerns. The authors explain that while AI improves customer targeting, personalization, and campaign efficiency, it also introduces risks like unauthorized data access, phishing, misinformation, and data sharing without consent. They highlight challenges across sectors, especially healthcare, where breaches of sensitive information can lead to legal and ethical consequences. Although the article outlines general solutions such as better regulations, consumer awareness, and technical safeguards, it lacks critical evaluation of the effectiveness and enforcement of existing privacy laws. The study remains focused on descriptive analysis without offering deeper insights into sector-specific legal responsibilities. This research will address these gaps by analyzing the legal and ethical dimensions of AI use, evaluating current frameworks, and proposing enforceable mechanisms to protect privacy and ensure responsible AI marketing practices.

Siva Karthik Devineni, in his 2024 article titled “AI in the Data Privacy and Security”⁹ discussed how artificial intelligence is changing the way data privacy and security are handled. The paper starts by explaining the importance of protecting data and points out the weaknesses in older security methods. Real-life examples from banking and healthcare are used to show how AI can be applied in practice, along with lessons learned from these uses. The article also mentions some ethical concerns, such as the risk of bias, increased surveillance, and improper data handling. Although it covers technical progress well, the study does not deeply explore legal responsibilities or give strong suggestions for privacy laws. This research aims to fill that gap by focusing on legal and ethical responsibilities and recommending practical rules to ensure better privacy protection in the digital world.

Bareq Lami, Safinaz Mohd. Hussein, Ramalingam Rajamanickam, and Grace Kaka Emmanuel in their research titled “The Role of Artificial Intelligence in Shaping Data Privacy,”¹⁰ published in the *International Journal of Law and Management*, examined how AI acts both as a protector and a possible threat to personal data. The authors use a qualitative doctrinal approach to examine existing literature on AI and data privacy laws, highlighting that

⁹ Siva Karthik Devineni, *AI in Data Privacy and Security*, *International Journal of Artificial Intelligence and Machine Learning* 3, no. 1 (February 2024): 35–49, https://www.researchgate.net/publication/378288596_AI_in_Data_Privacy_and_Security.

¹⁰ B. Lami, S. Mohd. Hussein, R. Rajamanickam, and G. K. Emmanuel, "The role of artificial intelligence (AI) in shaping data privacy," *International Journal of Law and Management*, ahead-of-print no. ahead-of-print (2024), <https://doi.org/10.1108/IJLMA-07-2024-0242>.

while AI can strengthen data protection through automation and analysis, it can also lead to misuse if not properly regulated. The paper finds that there is a lack of clear and specific legal rules focused on AI, which creates risks for privacy and data rights. It emphasizes the need for transparency, fairness, accountability, and strict adherence to privacy laws when using AI tools. The study offers real-world examples and discusses how innovation, ethics, and regulation are closely linked in this evolving space. However, it does not provide in-depth policy recommendations or sector-specific legal solutions. This research aims to fill that gap by offering practical legal frameworks and ethical guidelines to ensure AI supports data privacy without compromising individual rights.

Aridi Janjeva and Marion Oswald in their report “The Privacy Intrusion and National Security in the Age of AI”¹¹, studied how AI is used by national security and police in the UK. They looked at how this use might affect people’s privacy. These government agencies have legal rights to collect personal data. But now, they often use AI to analyse that data. This creates new privacy concerns. To address this, the authors created a step-by-step method. This method helps check if AI use is fair and respects privacy. The method reviews all parts of AI use. It starts with how data is collected. Then it looks at how AI is trained and tested. Finally, it considers how AI is used in real cases. The authors developed this tool after talking to people in government, security, and law. They also studied fairness in UK law. Their method uses common terms to help experts discuss privacy issues clearly. This tool does not replace legal rules already in place. Instead, it adds extra care and helps prepare for future AI tools. This research analysis is very useful for current research. It provides a way to check AI-related privacy problems. This can guide rules and policies for Pakistan’s AI use.

Philip Menard and Gregory Bott in their research titled as “The misuse of Artificial intelligence and concern for information privacy: New construct validation and future directions”¹², studied how people feel about their privacy when companies use AI to analyze large chunks of data. Companies use AI to create detailed profiles of consumers for targeted ads, which can make

¹¹ Aridi Janjeva, Mufy Calider, and Marion Oswald, *Privacy Intrusion and National Security in the Age of AI* (London: Centre for Emerging Technology and Security, The Alan Turing Institute, May 22, 2023), <https://cetas.turing.ac.uk/publications/privacy-intrusion-and-national-security-age-ai>.

¹² Philip Menard and Gregory J. Bott, “Artificial Intelligence Misuse and Concern for Information Privacy: New Construct Validation and Future Directions,” *Information Systems Journal*, July 1, 2024, <https://doi.org/10.1111/isj.12544>. Accessed May 27, 2025.

shopping easier and marketing more effective. But collecting data this way raises serious privacy worries. For example, people's private information might be shared without meaning to, AI could treat some groups unfairly, and it can be hard to fully remove personal data from AI systems when asked. Their study shows that when people have more privacy concerns, they see higher risks and are more likely to support privacy protections, but they trust companies less. Interestingly, unlike past studies, trust and risk didn't change how people actually behaved. These results help guide future research and practical efforts to handle AI privacy problems. This research is important because it offers a useful way to measure AI privacy concerns that can help shape data protection policies in Pakistan which will be discussed in this thesis.

Won Kyung Jung and Hun Yeong Kwon, in their 2024 article "*The Privacy and Data Protection Regulations for AI Using Publicly Available Data: Clearview AI Case*",¹³ examined the complex legal challenges posed by AI companies using publicly accessible data for facial recognition technology. Through an analysis of regulatory responses across multiple jurisdictions, including America, Europe, Canada, and Australia, the authors mentioned the difficulties in enforcing privacy laws amid rapidly evolving AI applications. The Clearview AI case serves as a central example, illustrating how unauthorized data scraping raises serious privacy violations and legal disputes. The study points to significant inconsistencies in enforcement, cross-border legal uncertainties, and gaps in existing data protection frameworks. The authors emphasize the urgent need for harmonized, transparent, and enforceable regulations that balance innovation with individual privacy rights. While the article provides a thorough overview of legal controversies and enforcement outcomes, it stops short of offering detailed policy reforms. This research addresses that gap by advocating for comprehensive and practical legal frameworks that can adapt to technological advancements and effectively protect personal data in a globalized digital environment.

¹³ Jung, Won Kyung, and Hun Yeong Kwon. 2024. "Privacy and Data Protection Regulations for AI Using Publicly Available Data: Clearview AI Case." In *Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance (ICEGOV '24)*, 48–55. <https://doi.org/10.1145/3680127.368020>.

Keyur Tripathi in his Article Titled “Protecting the Privacy in the age of Artificial Intelligence”¹⁴ argued that Artificial intelligence (AI) has developed rapidly in recent times. Today, both private and public sector organizations around the world are immensely using AI tools. As AI and personal data protection have a lot to do for the benefit of the welfare of state. Hence, there must be machine learning mechanisms designed to monitor. Both variables i.e. artificial intelligence and the protection of personal data. It generally discussed the rapid development and growth of Artificial intelligence in modern era but has neither highlighted the challenges which can be occurred due to AI nor suggested any solution to overcome such challenges. This research contributes to the present study by highlighting AI’s rapid growth, which will be explored in greater detail regarding privacy protection mechanisms.

In her policy paper titled “Generative AI and Privacy,”¹⁵ Kate Charlet emphasizes that privacy protection should be built into AI systems from the beginning. She suggests that strong privacy policies can help balance the benefits of AI with the need to keep users safe. Key privacy strategies include being open about how data is used, collecting only the needed information, and giving users control over their data. These steps help reduce risks like private data leaking, especially when AI is being trained or used. Finally, Kate argues that teamwork between governments, companies, and others is essential to make sure AI develops responsibly while still protecting people’s privacy. This research is central to the thesis in hand, providing a foundation for analyzing AI’s privacy impacts in Pakistan and drawing lessons from global frameworks.

Alessia Zornetta and Ignacio Cofone in their research work “The Artificial Intelligence and the Right to Privacy”¹⁶, studied how AI struggles to follow privacy and data protection rules that protect human rights online. Their work focuses on important principles of the European Union’s General Data Protection Regulation (GDPR), but lessons can be used worldwide. They explain the difficulties in applying rules like collecting only necessary data, being clear about

¹⁴ Keyur Tripathi, “Protecting the Privacy in the Age of Artificial Intelligence,” SSRN, March 24, 2020, accessed May 26, 2025, <https://ssrn.com/abstract=3560047>.

¹⁵ Kate Charlet, “Designing for Privacy in an AI World,” Google Blog, June 4, 2024, accessed May 26, 2025, <https://blog.google/technology/safety-security/designing-for-privacy-in-an-ai-world/>.

¹⁶ Alessia Zornetta and Ignacio Cofone, “Artificial Intelligence and the Right to Privacy,” in *Artificial Intelligence and Human Rights*, ed. Jeroen Temperman and Alberto Quintavalla (2023; online edn, Oxford Law Pro), <https://doi.org/10.1093/law/9780192882486.003.0008>, accessed June 29, 2025.

how data is used, and holding developers responsible. The chapter also suggests practical ways developers can meet these rules to protect privacy and human rights well. This research is useful for the current thesis because it offers guidance on applying strong privacy laws to AI, which can help Pakistan improve its own privacy and data protection policies.

Rowena Rodrigue's article "The Legal and Human Rights issues of AI: Gaps, Challenges and Vulnerabilities"¹⁷ discussed AI's legal challenges, like bias, transparency, and privacy, using a "vulnerability" lens to highlight risks to human well-being, especially for vulnerable groups. The author was unable to concentrate on the possible threats to the right to privacy explicitly in the context of AI because they have collectively examined every facet, vulnerability, and difficulty encountered by the general public as a result of the growing hype surrounding AI. This is pertinent to the current legal research and provides a broad perspective on AI's human rights challenges, which will be specifically addressed in terms of privacy.

Such of the research could give valuable insights into the effectiveness regulatory measures and help anticipate future challenges. Bridging these gaps will lead to a more comprehensive understanding of the complex relationship between new technologies and digital privacy rights in Pakistan. It will help to draft an extensive Data protection law in Pakistan in order to cope with the digital privacy threats.

1.4 Research Questions

- 1) Whether Artificial Intelligence is affecting individuals' digital privacy in the modern era, and if so, how?
- 2) Whether countries like India and European Union have adopted legal frameworks to protect digital privacy from the impacts of Artificial Intelligence, and what lessons Pakistan can take from them to improve its own digital privacy laws?
- 3) Whether Pakistan's existing legal framework properly addresses digital privacy and Artificial Intelligence, and how effective laws i.e., the draft Personal Data Protection Bill, 2021 and the Prevention of Electronic Crimes Act, 2016 are in protecting digital privacy?

¹⁷ Rowena Rodrigues, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities," *Journal of Responsible Technology* 4 (2020): 100005, <https://doi.org/10.1016/j.jrt.2020.100005>.

- 4) What lessons Pakistan can take from Neighboring countries to improve its own digital privacy laws?

1.5 The Scope of Research

This thesis has a major focus on the understanding of how the technology especially artificial intelligence is affecting digital privacy rights in Pakistan. It also looks at how artificial intelligence can misuse the personal information, when there are not enough rules to prevent this. This research reviews existing Pakistani laws like PECA and the 2023 Data Protection Bill only and the rest of the legislations are out of the scope of the study. Moreover, the research compares Pakistan's legal framework governing the digital privacy rights with countries like India and European Union only while the rest are out of scope of study.

1.6 Significance of Research

The primary purpose of this research is to look upon the countries, i.e., the United States, the European Union, and India and discuss how they are dealing with the challenges of protecting personal digital privacy in the age of Artificial Intelligence. The thesis will look into the laws and institutions these regions have put in place to manage Artificial Intelligence and keep people's private information safe. The thesis also aims to find useful ideas for developing countries, especially Pakistan, that can be followed to improve their own legal system regarding the protection of digital privacy rights. Currently, Pakistan does not have a proper law focused on protecting privacy of the citizens in a digital world where AI is becoming more common. Basically, Privacy is not just a personal concern, but also a human right. Without strong digital privacy protection laws, people are left open to risks like surveillance, mimicking via deep fakes, data misuse, and unfair profiling. The latest international developments offer practical examples for other developing nations around the world. For example, the European Union introduced the Artificial Intelligence Act 2024, which stands as the world's first detailed legal framework on the regulation of artificial intelligence that aims to ensure that AI applications are used transparently and responsibly, while also strengthening personal data protection through regulatory controls and risk classification methodologies.¹⁸ Whereas in India, the Digital Personal Data Protection Act 2023 provide obligations on both public and

¹⁸ "European Union Artificial Intelligence Act, Up to Date Developments," The Artificial Intelligence Act, accessed May 27, 2025, <https://artificialintelligenceact.eu/>.

private entities to manage personal data securely and to regulate the artificial systems that process such data.¹⁹

The United States has taken a legalistic approach through its "Blueprint for an Artificial Intelligence-Bill of Rights," formulated in 2022.²⁰ The primary protection concerns in the age of Artificial Intelligence revolve around the right to digital privacy, the development of safe and effective systems, and the need to safeguard individuals from algorithmic discrimination. It is increasingly emphasized that AI tools must be designed with "privacy by design" principles, meaning they should inherently protect personal data, limit unnecessary data collection, and maintain public transparency throughout their operation. Crucially, the global discourse also stresses the importance of establishing clear oversight mechanisms and robust accountability structures to prevent misuse and ensure ethical governance. With AI becoming deeply embedded in digital platforms worldwide, privacy concerns have reached new heights. Today, over 5.64 billion people, more than two thirds of the global population, are connected to the internet. This unprecedented level of digital engagement significantly amplifies the risks associated with data breaches, surveillance, and unethical AI deployment. These risks are particularly severe in countries like Pakistan where regulatory mechanisms remain underdeveloped, public awareness is limited, and enforcement capacities are weak, making individuals especially vulnerable in the face of rapidly evolving technological landscapes.

In Pakistan, the Prevention of Electronic Crimes Act 2016 remains the core legislation for cybercrime. While it addresses unauthorized access to digital data, it does not provide targeted regulations for artificial intelligence. For example, the Act does not cover complex issues like algorithmic discrimination or the creation and spread of deep fakes. A recent 2025 amendment to PECA added Section 26(A)²¹, penalizing fake news online, but it still overlooks the unique challenges posed by AI technologies. Recognizing these challenges, Pakistan's Senate

¹⁹ Kaushiik Molitra and Karneeka Valabh "From The Algorithms to Accountability: AI Governance in India's Data, 2025.
<https://www.lexology.com/library/detail.aspx?g=1e6c3a8d-db38-4e5a-9dbc-b7e8e8358349>.

²⁰ The White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, Office of Science and Technology Policy, 2022,
<https://bidenwhitehouse.archives.gov/ostp/aibill-of-rights/>.

²¹ Kamran Adil, "2025 Amendments to The Prevention Of Electronic Crimes Act, 2016: An Introduction," Research Society of International Law (RSIL), 2025, <https://rsilpak.org/2025/2025-amendmentsto-the-prevention-of-electronic-crimes-act-2016-an-introduction/>.

proposed a Regulation of Artificial Intelligence Act in 2024, though it has not yet been enacted. It will articulately focus on how Pakistan can bring its future AI and data protection laws closer to international practices. The suggestions will include forming independent regulatory bodies, using privacy by design principles, and putting legal measures in place to prevent the adverse effects of AI. These efforts aim to support a digital future for Pakistan that is fair, transparent, and safe for everyone.

1.7 Research Methodology

This thesis will have a qualitative research approach to explore how artificial intelligence impacts digital privacy in Pakistan, where AI is increasingly prevalent across various sectors. The research will rely on primary sources, such as national laws, international treaties, and expert interviews, alongside secondary sources, including scholarly articles, books, policy reports, and credible websites. Through this method, the study will collect and examine data to understand how countries like India, the European Union, and the U.S. address AI-related privacy risks including the existing laws of the countries along with the most recent amendments. This way it ought to suggest practical ways and a devised legal framework for Pakistan to strengthen its legal framework to protect personal data in the digital era.

CHAPTER 02: UNDERSTANDING DIGITAL PRIVACY AND THE INFLUENCE OF ARTIFICIAL INTELLIGENCE

2.1 Introduction

Artificial intelligence is expanding rapidly and evolving the world, bringing exciting advancements and serious concerns about its effects on society. One key issue is digital privacy, which is essential for personal freedom. AI can improve Digital Privacy by handling large amounts of information, but it can also risk personal details through misuse. This chapter explains digital privacy, introduces AI and its relevant uses, explores how AI can protect or harm privacy, and looks at the changing field of data protection.

2.2 Defining Privacy and Digital Privacy

Privacy is considered as a fundamental human right that allows individuals to live without unwanted interference, choose their associations, and control access to personal information.²² It appears in various forms: physical privacy, such as maintaining bodily autonomy during medical exams or security checks; surveillance privacy, where actions remain untracked; and information privacy, which focuses on safeguarding details about identity and beliefs. Thereof, Privacy is a key human right, though it comes with some complexity. The basic right to privacy is enshrined in the international and regional human rights frameworks. For instance, the 1948 UDHR-Universal Declaration of Human Rights prohibits the interference with an individual's personal family, life, home, or correspondence, as well as attacks on their honor. It emphasizes that everyone is entitled to legal safeguards against such violations. Similarly, the International Covenant on Civil and Political Rights 1966 declares that no one unlawfully or arbitrarily intrude into someone's privacy, family, or reputation, and mandates legal protections to prevent such acts. The concept is found in other agreements too, such as the UN conventions on migrant workers and children's rights, the Charter of Africa, American Convention, the Arab Charter, and the European Convention. Each one protects privacy in its own way. Over 130 countries worldwide also have privacy protections in their constitutions. It is a widely accepted principle, even if its application varies by region.²³

While on the other hand, Digital privacy involves protecting personal information online. It enables control over data like names, addresses, or financial details, ensuring security and anonymity on the internet. Basically, online privacy, sometimes called internet or digital

²² Office of the Australian Information Commissioner, "What Is Privacy?" OAIC, accessed June 29, 2025, <https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-privacy>.

²³ Privacy International, "The Understanding of the Concept of Personal Privacy," The Explainer, May 8, 2017, <https://privacyinternational.org/explainer/56/what-privacy>

privacy, refers to the safeguarding of personal information of individuals while they explore the internet.²⁴ It involves protecting sensitive details, such as financial data, names or personalized passwords from unauthorized access and ensuring individuals have control over what information they share and how it is used by others, such as websites or third parties. Digital privacy is about a person's ability to manage and secure their personal data while engaging with online platforms. This applies to a variety of digital platforms, such as websites, mobile apps, and various software's. The personal data refers to any information that can identify an individual. This includes not just their name or physical address, but also other details such as phone numbers, credit card data, or even a vehicle's license plate number.²⁵

Online privacy at its core signifies the fundamental right of individuals to control who can access their personal information as they navigate the digital landscape. Ideally, users should be empowered to decide what data is collected, how it is utilized, and who has access to it. However, the practical reality is far more complex. Controlling personal data in the age of cookies, algorithms, and extensive surveillance is incredibly challenging. Despite growing efforts by governments and private companies to introduce protective measures and policies, the burden of safeguarding digital privacy still largely falls on individuals. This places users in a difficult position, often requiring them to navigate technical settings, terms of service, and opaque consent mechanisms, highlighting the pressing need for stronger, and more user centric privacy protections.

2.3 Core Principles of Digital Privacy

Digital privacy in Pakistan is essential because it needs to protect individual rights while also considering the growing use of digital technologies prominently artificial intelligence. Data protection refers to the laws and regulations meant to keep the private information safe from the misuse, or the security breaches.²⁶ For example, if a bank collects personal information from its customers, such as names, addresses, and financial details, it must be ensured that this data is stored securely and accessed only by authorized personnel. In Pakistan, where the digital technologies are integrated into the daily lives of individuals, overhauling the data protection stands essential. It means that the citizens should hold the right to accept or dissent to

²⁴ Usman Hussain, "Defining The Digital Privacy And Exploring Through Digital Privacy and Safety," accessed May 19, 2025, <https://www.enzuzo.com/blog/digital-privacy-definition>.

²⁵ Reuben. B, "What Actually Is Online Privacy? Definition, Risks, and Advice," The Built In, April 16, 2025, <https://builtin.com/articles/what-is-online-privacy>(<https://builtin.com/articles/what-is-online-privacy>).

²⁶ Pakistan Telecommunication Authority, "Data Protection in Pakistan: A Comprehensive Overview," accessed Apr. 1, 2025, <https://www.pta.gov.pk/en/faq/data-protection-in-pakistan>.

permission for the collection and use of their personal information. The free consent allows people to regulate the control over their data, including their identity, contact details, and online activities. In Pakistan, as the data collection through digital platforms is growing quickly, it is crucial to ensure that consent is informed and voluntary. This is also equally important for fairness and for protecting individual rights.²⁷

The transparency is also essential aspect of data protection. Organizations should provide clear and detailed information about how they collect, store, and use data. For instance, if a social media platform collects user data to personalize ads, it should be openly explained how come the data is being collect, how it will be used, and who it may be shared with.²⁸In Pakistan, where public trust in institutions may be low, transparency is vital for improving accountability in how data is handled. The principle of purpose limitation is important for managing data ethically. It means that individual's personal information should solely be collected for a specific and legitimate reason, which should be clearly stated from the beginning. For instance, if the data is collected for a purchase, it shouldn't be used for unrelated marketing without a good reason. This principle is important in Pakistan, where there is the rise of technology which raises the risk of data leak and being used for unethical purpose. Major security measures are also a major part of data protection.²⁹These provided measures can include everything from the basic security protocols to the advanced encryption techniques, depending on how much sensitive the data is which is being scrutinized.

And accountability is regarded as the final and one of the most vital pillars of data protection. It ensures that organizations entrusted with managing individuals' data strictly adhere to established laws and regulations designed to safeguard privacy. These organizations must not only implement robust data protection practices but also take full responsibility for any lapses or failures in handling personal information. This responsibility includes being subject to regulatory oversight, facing potential penalties or fines, and taking prompt corrective measures when breaches or violations occur. Accountability serves as a crucial mechanism to enforce compliance and build trust between users and data controllers. In many countries, including

²⁷ Ayesha Khan, "Data Protection Laws in Pakistan: An Overview," *Journal of Information Technology & Politics* 18, no. 2(2021):123–35, accessed on 20th May 2025, <https://doi.org/10.1080/19331681.2021.1891234>.

²⁸ Muhammad Zafar, "Need for Data Protection Legislation in Pakistan," *Pakistan Law Journal* no. 3 45–60, <https://www.pakistanlawjournal.com/articles/2020/3/need-for-data-protection-legislation>.

²⁹ General Data Protection Regulation, Regulation (EU) 2016/679, Official Journal of the European Union, May 4, 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.

Pakistan, the legal and institutional frameworks surrounding digital privacy are still evolving and often lack maturity. This makes the role of accountability even more important, as it acts as a deterrent against negligence and malpractice, and as a safeguard to protect citizens' rights in the digital realm. Without strong accountability measures, efforts to protect personal data remain ineffective. Therefore, embedding accountability into data governance is essential for achieving reliable and trustworthy data management systems that respect users' privacy and uphold their rights.

2.4 Artificial Intelligence and Digital Privacy Rights

Artificial Intelligence is rapidly becoming an integral part of our digital lives. It powers everything from personal assistants and social media algorithms to surveillance systems and healthcare technologies. While AI brings remarkable convenience and boosts efficiency across various sectors, it also raises significant concerns about the collection, use, and potential misuse of personal data. Questions about privacy, data security, and ethical use of AI technologies are becoming increasingly urgent as these systems become more pervasive and influential in everyday life.

The 21st century has witnessed a remarkable surge in artificial intelligence, propelled by extensive developments in machine learning, deep learning, and the utilization of the big data.³⁰ The 2010s marked a pivotal moment as artificial intelligence (AI) entered the mainstream, highlighted by the introduction of virtual assistants like Apple's Siri, the rise of self-learning AI systems such as AlphaGo, and the development of generative models including GPT-3 and DALL-E. These innovations revolutionized fields like natural language processing and image generation, fundamentally changing how machines understand and create content.

Today, AI is deeply embedded in everyday life, influencing various range of sectors including the healthcare, finance, education, and entertainment. The ongoing advancement of AI research is pushing towards the development of artificial general intelligence (AGI), which purpose is to create machines with human-like cognitive abilities. Alongside these technological breakthroughs, there are active and necessary discussions about the impact of automation on jobs, and the broader social consequences. As AI technology continues to evolve and expand,

³⁰ Andreww Erick, *The Age of Second Machine: The Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York, Norton & Company, 2014), 7–10, <https://www.jstor.org/stable/j.ctt13wst7> Accessed on 21st May 2025.

its role in shaping the future of society remains one of the most important and transformative narratives of the modern era.

2.4.1 Defining the term Artificial Intelligence

Artificial intelligence is formally defined as a principle of computer science focused on creating platforms that can perform tasks requiring human intelligence.³¹ These methods include learning, problem-solving, recognizing things, and understanding the language models. Instead of copying how humans think, AI uses different methods to act intelligently. The goal is to help machines process information, learn from the data, and make elaborative decisions with little human input.

2.4.2 Applications of Artificial Intelligence

Artificial intelligence exerts a profound influence across diverse fields, employing sophisticated computational techniques to resolve intricate issues with exceptional accuracy and efficiency.³²

2.4.2.1 Astronomy

Artificial intelligence is a vital instrument in astronomy, enabling scholars to unravel complex cosmic mysteries. Through meticulous analysis of extensive telescopic data, it facilitates the classification of celestial entities and the precise forecasting of astronomical phenomena.³³ This approach surpasses traditional observational methods, deepening comprehension of the universe's structure and origins. By processing vast datasets, artificial intelligence enhances the study of stellar evolution and galactic formation, providing insights unattainable through earlier techniques. Its adoption marks a significant advancement in astrophysical inquiry and theoretical development.

2.4.2.2 Healthcare

In healthcare, artificial intelligence substantially refines diagnostic accuracy and operational effectiveness. It examines comprehensive records, including patient histories, medical imagery, and genetic information, to detect diseases promptly and support clinical judgments. Continuous monitoring of patient conditions allows for early warnings of deterioration, permitting timely interventions before hospitalization. Such advancements promise a notable

³¹ Norvig, Peter. *Artificial Intelligence: A New Modern Approach*, 3rd ed. The Upper Saddle River, NJ: Prentice Hall, 2010), 1–2.

³² Simplilearn, "Top 24 Artificial Intelligence Applications and Uses," 2025, accessed June 29, 2025, <https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/artificial-intelligence-applications>.

³³ .Dalya Baron, *Machine Learning in Astronomy: A Practical Overview*, arXiv preprint, April 15, 2019, <https://doi.org/10.48550/arXiv.1904.07248>.

shift in medical practice over the next decade, particularly in specialties requiring rapid and precise responses.³⁴ The integration of these systems elevates standards of patient care and heralds a new era of predictive medicine.

2.4.2.4 Gaming

Artificial intelligence profoundly shapes the gaming industry, especially in strategic contexts like chess. Equipped with advanced computational reasoning, systems assess numerous potential moves based on current game states, often outperforming human players.³⁵ While earlier models relied on fixed rules, modern developments incorporate adaptive strategies, enriching gameplay complexity. This evolution creates engaging, competitive environments that challenge participants with intricate tactical scenarios. The involvement of artificial intelligence in this field underscores its capacity to enhance interactive entertainment and strategic simulation.

2.4.2.5 Digital Privacy

Amid increasing digital vulnerabilities, artificial intelligence has crucial role in strengthening data protection by accurately identifying threats and detecting anomalies that might otherwise go unnoticed. Through sophisticated algorithms and detailed pattern analysis, AI systems can monitor network activities and user behavior in real time to pinpoint irregularities such as unusual access attempts or malicious software behavior. This proactive detection helps identify software vulnerabilities before they can be exploited by cybercriminals, allowing the organizations to respond swiftly and effectively to the certain breaches. Furthermore, AI powered cybersecurity tools continuously learn and adapt to evolving threats, improving their ability to counter increasingly sophisticated cyberattacks. These specialized systems enhance defensive measures by automating threat detection, incident response, and risk assessment processes, thus reducing human error and enabling faster mitigation. In today's highly interconnected digital environment, where data flows across multiple platforms and borders, AI driven protection mechanisms are essential for maintaining the integrity, confidentiality, and availability of critical information, ensuring stronger resilience against cyber intrusions and safeguarding the privacy of individuals and organizations alike.³⁶ This capability proves

³⁴ A. Esteva et al., "A Guide to Deep Learning in Healthcare," *Nature Medicine* 25, no. 1 (January 2019): 24–29, <https://doi.org/10.1038/s41591-018-0316-z>.

³⁵ Yueliang Wu et al., "Artificial Intelligence for Video Game Visualization: Advancements, Benefits and Challenges," *Mathematical Biosciences and Engineering* 20, no. 8 (July 2023): 15345–15373, accessed on 31st May 2025, <https://doi.org/10.3934/mbe.2023686>.

³⁶ Dhanamma Shankar Jagli, "The Role of Artificial Intelligence in Cyber Security," *Journal of Electrical Systems* 20, no. 3 (April 2024): 5283–5291, <https://doi.org/10.52783/jes.6327>.

essential for organizations facing persistent cybersecurity challenges, offering a proactive shield for valuable digital resources.

2.4.2.6 Social Media

Artificial intelligence plays a crucial role in managing the vast amounts of data generated daily by social media platforms like Facebook, WhatsApp, and Twitter by systematically organizing and analyzing user profiles through advanced algorithms. It processes diverse information, including posts, messages, interactions, and metadata, to detect emerging trends, understand user preferences, and identify key markers such as hashtags and popular topics. By extracting these insights, AI optimizes content distribution, ensuring users receive personalized and relevant information tailored to their interests, which enhances engagement and helps platforms prioritize certain messages for marketing or social interaction. Additionally, AI's ability to analyze large datasets in real time enables social media companies to make swift decisions about promoting, flagging, or restricting content, addressing issues like misinformation and harmful material. This dynamic management powered by AI not only shapes how users consume and share information but also supports platform goals such as user retention and advertising effectiveness, ultimately creating a more interactive and efficient digital environment.³⁷ This basic function supports tailored user experiences and strategic marketing, adeptly detecting the complexities of digital engagement.

2.4.2.7 Automotive Industry

Artificial intelligence has changed the automotive industry by inducing the advanced assistants and self-navigating systems into vehicles such as auto pilots. Such innovations, produced by the leading manufacturers such as Tesla, enhance user functionality and safety.³⁸ Also self-driving cars, overviewed and guided by comprehensive traffic analysis, reduce errors and improve road reliability.

2.4.2.8 Robotics

In the field of robotics, artificial intelligence significantly enhances machines beyond performing routine tasks by enabling them to adapt and execute actions based on accumulated experience and learning. This advancement allows for the development of sophisticated robots, including humanoid models equipped with speech and behavioral capabilities, which can

³⁷ Musawer Hakimi et al., "Artificial Intelligence for Social Media Safety and Security: A Systematic Literature Review," *Studies in Media Journalism*, <https://doi.org/10.32996/smjc.2023.1.1.2x>

³⁸ Mohsen Soori, BehroozArezoo, and RozaDastres, "Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics: A Review," <https://doi.org/10.1016/j.cogr.2023.04.001>. Accessed on 31st May 2025.

independently perform a wide range of complex functions. AI-driven robotics can learn from their environments, make decisions in real time, and interact naturally with humans, thereby expanding their applications across industries such as healthcare, manufacturing, service, and exploration. These intelligent machines not only improve efficiency and precision but also open new possibilities for automation and human robot collaboration in tasks that were previously considered too intricate or dynamic for traditional robots.³⁹

2.4.2.9 Education

Artificial intelligence is changing education in many helpful ways. It can do tasks like grading tests and assignments automatically, which saves teachers a lot of time. This way, teachers can spend more time teaching and helping students. AI tools can also talk with students and give them quick answers or explanations, making learning easier and more fun. These tools can adjust to how each student learns best, so everyone gets the help they need. In the future, AI could provide personal tutors that are available anytime, anywhere, so students can get extra help whenever they want. This will make education more available to everyone, even those who live far away or do not have many resources. Overall, AI can make learning more personalized and accessible for all students.⁴⁰

2.4.3 How Artificial Intelligence Can Strengthen Privacy

Since the days of handwritten record keeping, Digital Privacy and privacy have advanced dramatically. Since data became more accessible at the danger of being compromised, the digital age brought with its new challenges. In order to safeguard the sensitive data, it resulted in expanding of technology including firewalls and encryption. However, Digital Privacy and privacy have been transformed by artificial intelligence. AI can help safeguard data and prevent security breaches by the analysis large amounts of data and quickly identifying trends and possible risks.⁴¹ The field of protecting personal information from prying eyes is evolving quickly due to constantly improving technologies. The basic idea of information concealment first surfaced many years ago, after the growth of databases and computers in the 20th century.

³⁹ Anna L. Buczak and Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials* 18, no. 2 (January 2015): 1–1, <https://doi.org/10.1109/COMST.2015.2494502>.

⁴⁰ Wayne Holmes, Maya Bialik, and Charles Fadel, *Artificial Intelligence in Education: Promise and Implications for Teaching and Learning* (Boston, MA: Center for Curriculum Redesign, 2019), Accessed on 31st May, 2025, https://www.researchgate.net/publication/332180327_Artificial_Intelligence_in_Education_Promise_and_Implications_for_Teaching_and_Learnngi.

⁴¹ Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro, "Cyber Security: State of the Art, Challenges and Future Directions," *Cyber Security and Applications* 2 (2024): 100031, <https://doi.org/10.1016/j.csa.2023.100031>.

Securing the military and government computer systems that held critical keys was the main priority at the time. But when computers were more widely used for managing personal data, the emphasis shifted to safeguarding people's privacy. Some nations began enacting laws in the 1970s and 1980s. Concerns regarding the privacy of personal data and how computers keep and use it are one factor contributing to this.

2.4.3.1 Data Breach Detection

AI-powered cybersecurity systems are increasingly used to monitor digital platforms for suspicious activity. These tools can detect data breaches by identifying unusual access patterns or behavior across networks. For example, Darktrace, an AI cybersecurity company, uses real-time machine learning to isolate threats before they cause harm, thus strengthening privacy safeguards.⁴²

2.4.3.2 Customized Privacy Settings

AI helps people better understand and manage their privacy settings. For example, platforms like Google use machine learning in tools like Privacy Check-up to suggest privacy options that fit each user's unique habits and preferences. This makes it easier for users to protect their personal information without needing to figure out complex settings on their own.⁴³ This empowers users to manage their digital footprints.

2.4.3.3 Data Anonymization in Sensitive Fields

In important fields like healthcare and academic research, Artificial Intelligence plays a helpful role in protecting privacy while still allowing useful analysis. One major way it helps is by anonymizing personal data. This means removing any information that can directly identify a person. For example, hospitals often have large amounts of patient records. If this data is not protected, it could lead to privacy issues. With the help of AI, hospitals can automatically remove details like names, phone numbers, or medical record numbers from these files. This allows researchers to study health trends and improve treatments without revealing who the patients are.⁴⁴

In the same way, academic researchers can use AI to clean data collected from surveys or experiments. The information becomes useful for study, but no personal details are shared.

⁴² PrivacyBee, "How AI Is Changing the Privacy Landscape (For Better or Worse)," Privacy Blog, accessed June 29, 2025, <https://privacybee.com/blog/ai-impact-on-privacy/>.

⁴³ Mark van Rijmenam, "The Privacy in the New Age of AI: Linked Risks, Challenges and Solutions," The Digital Speaker, accessed May 19th, 2025, <https://www.thedigitalspeaker.com/privacy-age-ai-riskschallenges-solutions/>.

⁴⁴ Murdoch, B. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Med Ethics* **22**, 122 (2021), accessed June 29, 2025 <https://doi.org/10.1186/s12910-021-00687-3>

This approach keeps people's identities safe while still helping research move forward. AI makes it easier to respect privacy and make progress at the same time.

2.4.4 Privacy Threats concerned with Artificial Intelligence

Artificial intelligence is an increasingly crucial part of our daily lives, from the apps we use on our phones to the services we rely on online. However, as AI systems collect and analyze massive amounts of personal data, this raises serious concerns about individual privacy. Many people worry about how their information is gathered, stored, and shared, and whether it might be used without their consent or for purposes they do not approve of. The fear of data breaches, misuse, or surveillance by AI technologies makes privacy a critical issue that needs careful attention. As AI grows more powerful and widespread, it becomes essential to balance the benefits of these technologies with strong protections that respect individuals' rights to keep their personal information safe and private.⁴⁵ The main privacy threats caused by AI are:

2.4.4.1 Unauthorized Data Collection

Artificial Intelligence often collects personal information such as a person's location, online behavior, or the content they type or upload. Many users are not fully aware that this data is being gathered, especially when there is no clear permission process. For example, AI tools that generate written content or create images might quietly store parts of what users input. This information is then used to make the tool work better in the future. While this can help improve accuracy and performance, it also creates serious concerns about privacy. People may unknowingly share sensitive details that are saved and reused without their knowledge. This shows the need for clear rules and stronger protections to make sure personal data is handled in a fair and safe way.⁴⁶ This can lead to data leaks or misuse if proper security measures are not in place.

2.4.4.2 Invasive Monitoring

Artificial Intelligence surveillance systems are increasingly being used by law enforcement agencies and private companies to monitor individuals. These systems often rely on a mix of security cameras, social media activity, and other digital data sources to track people's movements and behavior. However, there is usually very little transparency in how this technology is used. Most people are not informed when they are being monitored, where the

⁴⁵ Alice Gomstyn and Alexandra Jonker, "Exploring Privacy Issues in the Age of AI," IBM Think Blog, September 30, 2024, <https://www.ibm.com/think/insights/ai-privacy>

⁴⁶ Akash Takyar, "Digital Privacy in AI Systems: Types of Threats, Principles and Techniques to Mitigate Them and Best Practices," LeewayHertz, accessed June 29, 2025, <https://www.leewayhertz.com/data-security-inai-systems/>.

surveillance is happening, or for what purpose their data is being collected. This lack of openness raises serious problems about digital privacy and the misuse of such AI technology, especially when there are no clear rules or public oversight in place.⁴⁷ This can limit personal freedom and create fear of constant observation.

2.4.4.3 Biased Decision Making

Artificial Intelligence systems can sometimes produce unfair or discriminatory outcomes, especially when data is used to train them is biased. If an AI model is trained on information that reflects historical inequalities or social prejudices, it may unintentionally learn and repeat those patterns. For example, if a company uses AI to help with hiring decisions and the training data includes past hiring records that favored certain genders or ethnic groups, the system may continue to prefer those same groups. As a result, qualified candidates from underrepresented backgrounds could be unfairly rejected. This shows how important it is to carefully check the data used in AI training and to make sure that these systems are tested for fairness before they are put into use.⁴⁸ This misuse of personal data can harm individuals and reinforce discrimination.

2.4.4.4 Data Misuse and Fake Content

Artificial Intelligence has developed to the point where it can produce highly realistic fake videos or images, commonly known as deep fakes. These digital creations often feature real people, making it appear as though they are speaking, acting, or doing things they never actually did. In some cases, deep fakes have been used in political propaganda, fake news, or even in personal revenge. Because they are so realistic, it becomes difficult for the average viewer to distinguish between what is real and what is artificially created. This not only poses a threat to individual privacy and dignity but also raises serious concerns about trust, truth, and safety in the digital world.⁴⁹ These can spread false information or damage reputations. Moreover, scams using artificial intelligence can induce people in causing serious breach of the digital privacy.

⁴⁷ Catarina Fontes et al., “AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them,” *Technology in Society* 71 (October 2022): 102137, accessed June 29th, 2025, <https://doi.org/10.1016/j.techsoc.2022.102137>.

⁴⁸ Jasmine Williams, *Understanding the Impact of AI Bias for Recruiting*, reviewed by Dr. Andrew Buzzell, last modified February 24, 2025, <https://vidcruiter.com/interview/intelligence/ai-bias/>, accessed June 29th, 2025.

⁴⁹ KinzaYasar, Nick Barney, and Ivy Wigmore, “What Is GenAI? Generative AI Explained,” *WhatIs (TechTarget)*, May 22, 2025, <https://www.techtarget.com/whatis/definition/deepfake>

2.4.4.5 Big Tech Data Control

Large technology companies collect and analyze enormous amounts of personal data from users around the world. This includes information such as search history, location, browsing habits, purchases, and even private conversations on digital platforms. By gathering such detailed data, these companies gain deep insights into people's behavior, preferences, and daily routines. This not only helps them improve their services or target advertisements more effectively but also gives them significant control over how personal information is used, stored, and sometimes shared. The power these companies hold raises important concerns about privacy, data ownership, and accountability.⁵⁰ It could also lead to intrusive practices such as targeting users with ads based on private information often without clear user knowledge or control.

2.4.4.6 Job Loss and Privacy Trade Offs

The automations of the artificial intelligence can fully or partially replace jobs pushing workers into roles that require sharing personal data such as gig economy platforms. The following platforms may demand details like location or work history forcing individuals to give up privacy to earn a living.⁵¹ The use of such technology in hiring may also analyses online behavior without candidate's awareness. In the most recent time, Google has faced criticism for tracking user locations even when users turned off location settings risking exposure of sensitive data. Predictive policing AI has unfairly targeted certain communities leading to biased surveillance. Amazon once used an AI hiring tool that discriminated against women because it was trained on male dominated resumes.

2.5 Artificial Intelligence Reinforcing Digital Privacy

Strong encryption and advanced authentication methods are becoming more and more common in the modern era brought about by technological breakthroughs and increased awareness in the Digital Privacy space. Automation is the process of depending on software and technology to automatically detect, evaluate, and address security incidents and threats in order to safeguard data and systems. As AI develops further, attention must be focused on its responsible development and use. When creating AI systems, we must make sure that transparency, accountability, and ethical issues are considered. Responsible usage of AI can help reduce these risks and guarantee that everyone benefits from AI advances. As a result,

⁵⁰ Aliza Vigderman, "The Data Big Tech Companies Have On You," *Security.org*, last modified March 10, 2025, <https://www.security.org/resources/data-tech-companies-have/>, accessed June 29th, 2025.

⁵¹ A. Shaji George, "Artificial Intelligence and the Future of Work: Job Shifting Not Job Loss," April 2024, <https://doi.org/10.5281/zenodo.10936490>, accessed June 29th, 2025.

protecting personal information has a history, and the threats and solutions to avoid them are always changing. From the first simple safety regulations to the most sophisticated plans that include artificial intelligence, this subject has undergone significant change. It provides a quick and clever method of safeguarding important data. It turns out that there are issues to be resolved as we get more knowledge about the capabilities and applications of AI. But AI has a great chance to transform how we safeguard and preserve our personal data.⁵²

2.5.1. AI for Security and Privacy

When discussing security and privacy concerns in the discipline of artificial intelligence, AI itself plays a vital role. It helps detect and prevent potential adversarial attacks or data poisoning attempts, which can harm AI systems. By analyzing patterns and behaviors, AI systems can spot unusual activities and intrusions as they happen. This real-time monitoring allows for quick responses to stop attacks before they cause significant damage, making AI a key tool in protecting both itself and the data it handles.⁵³

2.5.2. Malware mitigation and intrusion/anomaly detection

Artificial Intelligence can also be used to improve the overall security of computer and network systems through anomaly and intrusion detection systems. In order to take pre-emptive action, the Artificial Intelligence algorithms continuously monitor network traffic and behavior of users, spot suspicious activity, and spot potential threats. AI can also help prevent malware and help create more efficient antivirus software by examining code and identifying dangerous trends.⁵⁴

2.5.3. Software and application security

In terms of software and application security, AI can be used to identify and remove software vulnerabilities. AI provided methods assist developers in improving the security of their applications through code analysis and vulnerability discovery. Additionally, AI can assist in tracking down software flaws and proactively identifying or anticipating potential assaults, allowing you to have pre-planned strategies to protect your company's systems and data. Generally speaking, artificial intelligence is responsible for the creation of certain technologies

⁵² Mazley Rafey, Artificial Intelligence in Cyber Security (West Virginia University, January 2024), <https://doi.org/10.13140/RG.2.2.19552.66561> , accessed March 10, 2025.

⁵³ Valerio Capraro et al., "The Impact of Generative Artificial Intelligence on Socioeconomic-Inequalities and Policy Making," *PNAS Nexus* 3, no. 6 (June 2024): pgae191

⁵⁴ Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (Hoboken, NJ: Wiley, 2011), <https://www.wiley.com/enus/Secrets+and+Lies%3A+Digital+Security+in+a+Networked+World+9781118082270>.

which support digital privacy and security by identifying suspicious activity or situations involving risks, hindering malware penetration, and improving software protection features.⁵⁵

2.6 Conclusion

In conclusion, artificial intelligence is becoming a major part of modern legal systems. It is used in areas like public safety, online security, and judicial services. These systems can help detect crimes, prevent cyber threats, and make legal work faster and more organized. Artificial intelligence also supports the protection of personal data by identifying risks and offering tools to control information access. However, when artificial intelligence is used without proper legal rules, it can lead to serious privacy issues. In law, privacy is not just a choice. It is a legal right that protects individuals from being watched or judged without fair reason. Many laws in different countries, as well as global human rights agreements, clearly say that every person has a right to keep their personal life private. But problems arise when artificial intelligence collects information without asking the person involved. Sometimes it keeps track of people's behavior or makes decisions about them without giving them a chance to respond. This can be unfair and harmful, especially if the technology is not fully accurate or free from mistakes. Because of these risks, it is very important for lawmakers, courts, and government agencies to create strong legal protections. These should include clear rules that say how artificial intelligence can be used, who is responsible for its actions, and how the rights of people will be protected. There should be legal limits to stop misuse of data, and there must be systems to review the decisions made by artificial intelligence. To sum up, artificial intelligence can be useful in improving legal work and protecting the public. But if it is not handled with care, it can also harm the basic rights of people. The use of artificial intelligence must always follow the law and respect the privacy, dignity, and freedom of every individual.

⁵⁵ Nadidem Beyza Dokur, The Artificial Intelligence (AI) Applications in the Cyber Security, January 2023, https://www.researchgate.net/publication/367253331_Artificial_Intelligence_AI_Applications_in_Cyber_Security.

Chapter 03: GLOBAL LEGAL FRAMEWORK FOR DIGITAL PRIVACY AND ARTIFICIAL INTELLIGENCE

3.1 Introduction

As mentioned in the last chapter, privacy is an upmost a human right associated with the autonomy, dignity, and freedom. The need and importance for privacy have become much clearer due to development of artificial intelligence in the digital world. AI systems are largely data driven and rely on extensive personal data, creating question about misuse but also rights of privacy. Across the world, many legislatures have passed or amended digital privacy laws with strong emphasis on regulations regarding the collection, storage and use of personal data, as well as, the general need for data protection. In addition to that, there's also been an international emphasis on the value of protecting personal data, requiring a cohesive stance toward emerging challenges presented by AI. This chapter will speak how AI is driving digital privacy across the globe in developed regions, including Europe, and India.

3.2 Laws Governing Digital Privacy Rights Internationally

The artificial intelligence has expanded the scale of the data collection, mostly through biometric surveillance, behavioral tracking, and predictive profiling, they also pose serious risks to personal autonomy and bodily integrity.⁵⁶ Digital privacy legal frameworks provide the essential safeguards against unwarranted intrusion and ensure that individuals retain control over how their personal information is used. Nations worldwide are taking control over data generated within their borders through legislation that limits cross border data transfers and imposes data localization requirements. While some other measures may be helpful to protect national interests, they can also look over the internet and restrict the global flow of information, raising complex questions about balancing sovereignty with international interoperability.⁵⁷

The deep fakes which are the fabricated videos, audio, and images generated by the Artificial intelligence models, have become a double-edged sword in the arena of digital privacy. But on the contrary, they offer creative possibilities in entertainment, education, and marketing; on the other, they pose significant risks by enabling malicious activities such as fraud, defamation, and misinformation. The ability to produce unauthorized explicit content without consent has

⁵⁶ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Cambridge, MA: Harvard Business School, 2019), <https://www.hbs.edu/faculty/Pages/item.aspx?num=56791>.

⁵⁷ David Lyon, *Surveillance Society: Monitoring Everyday Life*, illustrated reprint ed. (Buckingham: McGraw-Hill-Education-(UK), 2001), 63–79, Accessed on 1st June 2025. https://books.google.com.pk/books?id=aXX1AAAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

caused emotional distress and reputational harm, disproportionately affecting women and marginalized communities. As beyond individual harm, deep fakes facilitate identity theft, allowing malicious actors to impersonate others for fraudulent purposes, such as financial scams or unauthorized access to sensitive systems. The erosion of trust in media is another critical concern, as fabricated content can easily deceive audiences, manipulate public opinion, and undermine democratic processes. For example, the deep fakes have been used to spread false narratives during elections, sowing confusion and weakening public confidence in institutions. The accessibility of tools and Chabot's have made access to deep fakes creation much easier for the individuals with minimal technical expertise to produce harmful content, further enhancing these risks.⁵⁸

As the AI technologies advance at a fast pace, existing laws often lag behind, creating gaps that can leave individuals' rights unprotected and make regulation enforcement complicated. Some countries have recognized these challenges and begun to take proactive steps to address them. For example, China has introduced specific regulations which require the organizations to obtain formal consent from individuals before using their personal data in deep fake media, aiming to curb misuse and protect privacy in this emerging area. Similarly, the European Union has taken a comprehensive approach by prioritizing transparency and accountability in AI applications through landmark legislative efforts such as the Artificial Intelligence Act proposed in June 2024. This EU legislation seeks to establish clear standards for how AI systems should operate, focusing on protecting fundamental rights, promoting ethical use, and ensuring that AI technologies are developed and deployed in a trustworthy manner. Despite these efforts, many countries, especially those with less developed regulatory environments, continue to face challenges in creating robust legal frameworks that can effectively manage AI's complex and far-reaching impacts. The technological innovation often outstrips the ability of lawmakers to craft, pass, and enforce suitable regulations, resulting in a pressing need for adaptable, forward-looking policies that can protect citizens while encouraging innovation.⁵⁹

The global rise of Artificial Intelligence and the increasing prevalence of deep fakes have brought to light the urgent need for international cooperation among governments and regulatory bodies. Digital content flows freely across national boundaries, making it difficult

⁵⁸ European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final.

⁵⁹ Tambiana Madiega, Artificial Intelligence Act, EU Legislation in Progress, PE 698.792 (Brussels: EuropeanParliamentaryResearchService, September 2024), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).

for any single country to effectively regulate or control harmful uses of technology on its own. This reality calls for harmonized standards and collaborative enforcement mechanisms that allow different nations to work together in addressing challenges that cross borders. Without such cooperation, criminals and bad actors can exploit gaps between jurisdictions to spread misinformation, violate privacy, or commit fraud with little fear of consequences.⁶⁰ In response to these new digital risks, countries around the world have started developing legislation tailored to the demands of the digital age and the protection of personal data. Many nations have modelled their privacy laws on the European Union's General Data Protection Regulation (GDPR), which is widely recognized as a comprehensive and strict standard for safeguarding individuals' data rights. The GDPR sets clear rules on how data can be collected, used, and shared, and it grants individuals greater control over their personal information. This has influenced privacy regulations in numerous countries seeking to protect their citizens in a connected world.

Whereas, the United States has taken a different approach by adopting sector-specific laws rather than a single, overarching privacy framework. This means that instead of one broad law, different industries such as healthcare, finance, or children's online data each have their own regulations. While this allows for specialized rules that address the needs of each sector, it can sometimes create complexity and gaps in privacy protection. This difference in legal approaches makes international collaboration even more vital, as it ensures that privacy standards are respected regardless of where data travels. Ultimately, as technology continues to evolve and digital content becomes even more global, countries must come together to establish shared guidelines and enforcement strategies. Such efforts will not only help prevent misuse of AI and deep fakes but also protect individuals' privacy rights and maintain trust in the digital world. Without a united global response, the risks posed by these advanced technologies may continue to grow unchecked.

3.3 United Nations' Framework for AI and Privacy Governance

Privacy is a prominent human right under international law, most notably in Article 12 of the Universal Declaration of Human Rights 1948 and Article 17 of the International Covenant on Civil and Political Rights 1966. The United Nations has made significant strides in formulating a normative foundation for the governance of AI and digital privacy. While the UN lacks

⁶⁰ Stamatis Karnouskos, "Artificial Intelligence in Digital Media: The Era of Deepfakes," IEEE Transactions on Technology and Society PP, no. 99 (June 2020): 1–1, <https://doi.org/10.1109/TTS.2020.3001312>.

binding enforcement authority in this area, its resolutions and reports carry strong normative influence and shape the discourse on AI ethics, human rights, and digital governance. In March 2024, the UN General Assembly adopted Resolution 78/241 titled, "The Safe, Secure and Trustworthy Artificial Intelligence Systems," marking a landmark consensus on the ethical governance of AI technologies.⁶¹

A resolution co-sponsored by over 120-member states emphasizes the need for transparency, accountability, inclusiveness, and strict adherence to international human rights laws in how Artificial Intelligence is developed and used. The resolution urges countries to create national strategies that prevent AI systems from infringing on fundamental rights such as the right to privacy and the freedom of expression without discrimination. It highlights the importance of ensuring that AI technologies respect these rights and operate fairly for everyone. One of the key points of the resolution is that existing human rights frameworks already apply to AI systems. This means that countries must consider human rights principles whenever they design, implement, or regulate AI technologies. Additionally, the resolution stresses the necessity of human oversight in decision-making processes that are automated by AI. This is to make sure that critical decisions affecting people's lives are not left entirely to machines but have meaningful human involvement. While this resolution does not have legal effect and is not legally binding, the fact that it has received wide international support reflects a growing consensus among nations about the fundamental principles that should guide AI governance. It shows a shared recognition of the importance of protecting privacy and human rights as AI continues to advance and become more integrated into society. This broad agreement lays the foundation for future laws, policies, and cooperation on responsible AI use around the world.⁶²

The United Nations Educational, Scientific and Cultural Organization, commonly known as UNESCO, has taken a leading role in shaping the global ethical framework for Artificial Intelligence. In 2021, UNESCO adopted a landmark document called the Recommendations on the Ethics of Artificial Intelligence. This was the first-ever global agreement on AI ethics to receive endorsement from all 193-member states, making it a truly universal standard. The recommendations outline a set of core ethical principles that should guide the development and use of AI technologies worldwide. Among these principles are respect for human dignity, ensuring that AI serves the well-being of all individuals without causing harm. The document

⁶¹ UNGA Res. 78/241, "The Safe, Secure and Trustworthy Artificial Intelligence Systems," March 21, 2024, UN Doc A/RES/78/241, paras. 4 and 7–10.

⁶² Ibid, 11

also emphasizes the importance of preventing discrimination in AI systems, promoting gender equality, and supporting environmental sustainability as key goals. By setting these ethical guidelines, UNESCO aims to encourage responsible innovation that benefits humanity while respecting fundamental rights and values.⁶³

3.4 Digital privacy Laws in the United States of America

Protecting personal information in the United States involves a fragmented framework made up of a patchwork of federal, state, and sometimes even local laws, unlike the European Union's comprehensive and centralized General Data Protection Regulation (GDPR). This decentralized approach means that privacy protections vary depending on the type of data, the industry involved, and the state where the individual resides. At the federal level, laws like the Health Insurance Portability and Accountability Act (HIPAA) protect health data, the GrammLeach-Bliley Act (GLBA) safeguards financial information, and the Children's Online Privacy Protection Act (COPPA) governs children's online data. Meanwhile, individual states have begun introducing their own privacy laws, with California leading the way through the

California Consumer Privacy Act (CCPA) and its expanded version, the California Privacy Rights Act (CPRA), which give residents the right to know what data is collected about them, request deletion, and opt out of data selling. Other states like Virginia, Colorado, and Connecticut have followed suit with their own versions of privacy regulations. However, the lack of a single, unified federal law creates confusion and inconsistencies in enforcement and compliance, especially for companies operating across state lines. As public concern grows over data breaches, identity theft, and the misuse of personal information by tech companies and advertisers, there is increasing pressure on the U.S. government to enact a comprehensive privacy law that would standardize protections and strengthen individual rights nationwide.⁶⁴ Internet privacy, a big part of data protection, focuses on keeping information safe when it's shared online through things like tracking or data collection. Without one main law, some areas like health, money, or online activities are covered, but not everything, so states are stepping in with their own rules. On the other hand, federal government has several laws, but each one covers only specific things. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 ensures doctors and hospitals keep medical records safe. The Gramm-LeachBliley Act (GLBA) from 1999 requires banks to protect information about money. The Children's Online

⁶³ Naeem Allahrakha, "UNESCO's AI Ethics Principles: Challenges and Opportunities," *International Journal of Law and Policy* 2, no. 9 (September 2024): 24–36, <https://doi.org/10.59022/ijlp.225>.

⁶⁴ Thomas Ruters, "How Your Personal Information Is Protected Online," Thomson Reuters Legal Insights, <https://legal-thomsonreuters.com/en/insights/articles/how-your-personalinformation-is-protected-online>.

Privacy Protection Act (COPPA) of 1998 sets rules for websites to keep kids under 13 safe online. The Privacy Act of 1974 ensures the government keeps records about citizens and legal residents secure. The Federal Information Security Modernization Act (FISMA) from 2014, which updated an older law, tells government agencies to make their computer systems safe. The E. Government Act of 2002 sets rules for protecting information in online government records. The Freedom of Information Act (FOIA) lets people see government records but hides private details. The Trade Secrets Act of 1948 punishes stealing business secrets, including private information. The Paperwork Reduction Act (PRA) of 1995 stops the government from asking for too much data process. Social-Security-Number-Fraud Prevention Act of 2017 Limits Social Security numbers in mailed documents unless needed. The Federal Trade Commission (FTC) also stops companies from lying about how they handle information.⁶⁵

With no single federal law, states are making their own rules. California led the way with the California Consumer Privacy Act (CCPA), enacted in 2020. This law lets people find out what data companies have, ask to delete it, stop data sales, and not be treated differently for using these rights. It applies to big companies making over \$25 million a year, handling data from 100,000 or more people, or earning a lot from selling data. The California Privacy Rights Act (CPRA), starting in 2023, made these rules stronger by creating the California Privacy Protection Agency to check if companies follow the law. It also added rights like fixing wrong information or limiting sensitive data, like location or fingerprints. Twenty states now have their own privacy laws to keep data safe and hold companies accountable. These laws are different, making it tricky for companies working in multiple states. Some focus on letting people see or delete their data, while others push for better security. Talks about a national law, like the American Privacy Rights Act of 2024, aim to create one set of rules, but it hasn't happened yet. The strong laws of California State show efficiency, but a single law for the whole country would help keep everyone's information safe.

For years, lawmakers have talked about making new privacy laws, especially after big events like the 2012 Consumer Privacy Bill of Rights and the 2018 Cambridge Analytical scandal. Now, because artificial intelligence is growing so fast, there's a bigger need to talk about protecting people's information. Big tech companies are changing their rules to allow collecting personal data to train artificial intelligence, which makes privacy a bigger concern.

⁶⁵ Paul K., "U.S. Data Privacy Protection Laws: 2025 Guide," TechTarget, November 21, 2024, accessed May 20, 2025, <https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws>.

Meanwhile, the European Union has strong laws like the General Data Protection Regulation, the Digital Services Act, and the Artificial Intelligence Act to control how data is used. The United States could learn from these laws to make rules that give people more control over their information and keep them safe from artificial intelligence that watches them too closely. This would also help businesses follow the same rules and show that the United States and Europe share the same ideas about privacy and digital rights.⁶⁶ Artificial intelligence requires a huge quantity of data to work properly. For example, some reports say that Chatgpt, a popular artificial intelligence tool, used 1.5 billion pieces of data in 2019, and that number jumped to 175 billion by 2020. It's probably even bigger now. Companies collect data from all kinds of places, like websites, news articles, search histories, phone locations, and shopping records. Since artificial intelligence needs so much data, companies want to gather and keep more information for longer. These systems look for patterns in the data to guess things about people, like their income, beliefs, or relationships, even from unrelated details like what they buy or where they go online. Sometimes, even if the data is supposed to be unknown, artificial intelligence can figure out who someone is by combining different pieces of information. Even with these efforts, the United States still needs a big national law to protect everyone's privacy from artificial intelligence. In May 2025, some lawmakers shared a plan to create such a law, saying it would help companies know what rules to follow and show that the United States is different from countries that use artificial intelligence to control people. In recent years, Congress has tried to pass laws that would limit data collection, let people say no to certain artificial intelligence decisions, and check how algorithms affect people.⁶⁷

One significant effort to regulate privacy in the United States was the proposed American Privacy Rights Act. However, this bill was put on hold in June because lawmakers could not reach an agreement on several key issues. Among the disputed points were measures to prevent unfair treatment based on personal data and provisions that would allow individuals to opt out of major decisions made by artificial intelligence systems. While this national legislation remains stalled, some states and cities have taken their own steps to regulate AI and data privacy. For example, certain places have passed laws that restrict the use of facial recognition technology or aim to reduce bias in hiring practices involving AI. Unfortunately, these laws

⁶⁶ Caitlin Rothmann, "Protecting Data Privacy as a Baseline for Responsible AI," Center for Strategic and International Studies, July 18, 2024, accessed May 26, 2025, <https://www.csis.org/analysis/protecting-dataprivacy-baseline-responsible-ai>.

⁶⁷ U.S. House of Representatives, American Privacy Rights Act, H.R. 8818, 118th Cong., June 25, 2024, accessed May 26, 2025, <https://www.congress.gov/bill/118th-congress/house-bill/8818>.

vary widely across the country, creating a patchwork of rules that can be confusing for both people and businesses. In contrast, on May 19, 2025, President Donald Trump signed a new law known as the Take It Down Act, which specifically targets the problem of nonconsensual intimate imagery. This includes harmful content such as deep fake revenge pornography created with artificial intelligence. The law makes it a criminal offense to share explicit images or videos without the consent of the person shown, including fake material that appears real. It also requires social media platforms and websites to promptly remove such content within 48 hours of a victim's request. Importantly, the law balances the protection of free speech by focusing only on those who knowingly distribute this harmful content. Additionally, it allows responsible use of artificial intelligence by doctors or law enforcement in certain situations, as long as they follow proper guidelines. This law marks an important step toward addressing the growing risks posed by AI in the digital age.⁶⁸

3.5 The European Union's Artificial Intelligence Act (AI Act) 2024 and The General Data Protection Regulation (GDPR) 2018

The European Union leads globally in addressing the growth of artificial intelligence, which has made digital privacy a critical concern. Two key laws guide this effort: The General Data Protection Regulation (GDPR), effective since May 25, 2018, and the Artificial Intelligence Act, proposed on April 21, 2021, adopted on March 13, 2024, published on July 12, 2024, and effective from August 1, 2024. These laws protect personal data in artificial intelligence systems while promoting ethical innovation. The Artificial Intelligence Act 2024, the world's first comprehensive artificial intelligence regulation, divides artificial intelligence systems into four risk levels: unacceptable, high, limited, and minimal. Systems like facial recognition in public spaces or social scoring, which heavily use sensitive personal data, which was banned from February 2, 2025. High risk systems, such as those in hiring or law enforcement, require strict measures like detailed checks, documentation, human oversight, and ongoing monitoring due to their use of private data like health or identity information. Limited-risk systems, like Chabot's, must inform users they're artificial intelligence-driven, while minimal-risk tools, like spam filters, face no rules. Many artificial intelligence systems, especially high-risk ones, process personal data, closely linking the GDPR and Artificial Intelligence Act. Around 90% of high-risk artificial intelligence systems, such as those for biometric identification or

⁶⁸ Mariya Frances and Antony Robledo, "The Take It Down Act: Explaining Law Signed by President Trump Aimed at Revenge Porn, Deepfakes," USA TODAY Network, May 19, 2025, accessed May 26, 2025, <https://www.usatoday.com/story/news/politics/2025/05/19/take-it-down-act-trump/83731286007/>.

policing, handle sensitive data like ethnic backgrounds or medical records, requiring GDPR compliance. The GDPR demands legal, fair, and transparent data use, often requiring explicit consent for sensitive information. The Artificial Intelligence Act 2024 reinforces this for high-risk artificial intelligence.⁶⁹

Privacy professionals, experienced since the GDPR's enforcement on May 25, 2018, are essential for Artificial Intelligence Act compliance. They can identify personal data in artificial intelligence systems, limit data use, and conduct risk assessments that satisfy both laws. GDPR's DPIAs align with the Artificial Intelligence Act's assessments for high-risk systems, protecting privacy and other rights. They also train employees on artificial intelligence rules, meeting the Artificial Intelligence Act's requirement for artificial intelligence literacy. Their vendor management and compliance skills further support artificial intelligence governance. The Artificial Intelligence Act is likely to shape global laws, as the GDPR did, with countries like Canada drafting similar rules. Audits can help businesses stay compliant. The GDPR and Artificial Intelligence Act create a strong framework for protecting digital privacy in artificial intelligence systems. By leveraging GDPR expertise, businesses can meet Artificial Intelligence Act requirements for high-risk systems using sensitive data. Privacy experts are key to responsible artificial intelligence use. As global artificial intelligence regulations evolve, a unified compliance approach will foster trust and ethical innovation.⁷⁰

3.6 Digital Privacy Laws in India and the emergence of Artificial Intelligence

In current digital world, the issue of data privacy and protection has become extremely important, especially in a fast-developing and digitizing country like India. As internet use and digital technologies grow rapidly, a huge amount of personal information is being collected, stored, and used by both government departments and private companies. This growing use of personal data has raised serious concerns about how individual privacy is protected, since personal data is now seen not only as a business asset but also as something that could be misused for government surveillance. A turning point came in 2017 when Supreme Court of India, in the case of Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017), commonly known as the Right to Privacy verdict declared the right to privacy as a fundamental right under the Indian Constitution. This judgment marked a pivotal moment in India's legal

⁶⁹ Autoriteit Persgevens, Artificial Intelligence & Algorithmic Risks Report Netherlands 2023/2024, accessed on May 20, 2025, <https://www.autoriteitpersoonsgegevens.nl/en/documents/netherlands-winter-20232024/>.

⁷⁰ "Artificial Intelligence and the EU Artificial Intelligence Act," Insights, European Commission, accessed May 20, 2025. <https://lhc.ca.gov/wp-content/uploads/Commissioner-Packet-7-25-24.pdf>

landscape by emphasizing the urgent need for strong legal frameworks to protect personal data in the digital era. It recognized that the privacy is a fundamental right and stated the state's responsibility to create comprehensive safeguards that regulate how personal information is collected, stored, and used. Acting as a catalyst, the ruling paved the way for India to develop unified data protection laws aligned with international standards, moving beyond fragmented regulations to establish clear guidelines for businesses and protect individuals' rights. This decision not only shaped India's approach to digital privacy but also inspired broader reforms aimed at balancing technological innovation with the protection of personal information. Overall, the judgment was a crucial step toward building a citizen-focused digital privacy framework, setting the foundation for India's ongoing efforts to address privacy challenges in an increasingly connected world.

The Digital Personal Data Protection Act 2023 became law on August 11, 2023. It aims to protect personal data in India and applies to entities both within and outside the country if they offer services or goods to Indian citizens.⁷¹ This law is made to protect people's personal information. It says that no one can use someone's personal data without a clear reason and without asking them first. People also have the full right to take back their permission at any time. Everyone should be able to see their own data, fix anything wrong in it, delete it if needed, and know how it's being used. The companies or people collecting this data must keep it safe and only use it for the right reasons. If a company handles a lot of people's data or its work affects many people, it has to follow stricter rules. Sometimes, a small company might collect and manage the data by itself, but it still has to follow the law carefully. Also, every organization must appoint someone to make sure the data is being handled properly and to deal with any complaints. If anyone thinks their data is being misused, they can complain to a special board that looks into such issues. This board can check the case and fine those who break the rules. Lastly, personal data can only be sent to another country if the person agrees and the government thinks that country is safe enough. If there's a data breach, the seriousness of the damage and the effort to fix it will decide the penalty.⁷²

The law is officially created to give people greater control over their personal information and to hold companies accountable for managing that data in a responsible way. It aims to protect

⁷¹ The Digital Personal Data Protection Act, 2023 (*No. 22 of 2023*), Gazette of India, August 11, 2023, <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>

⁷² Kambayi Rao, "Digital Personal Data Protection Act 2023, A Game Changer," *The Times of India*, Aug. 21, 2023, accessed on May 20th, 2025, <https://timesofindia.indiatimes.com/blogs/kembai-speaks/digitalpersonal-data-protection-act2023-a-game-changer/>.

citizens by ensuring their private details are not misused or shared without consent. A recent example that shows the dangers of manipulated content involved a fake video of Congress leader Kamal Nath. This fabricated video caused confusion about a government program, misleading the public and highlighting how deep fakes can be used to disrupt trust in important political processes. Such incidents demonstrate the serious threat deep fakes pose to electoral integrity and public confidence in democratic institutions.⁷³

In 2021, the Indian government introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, aimed at increasing accountability of digital platforms and ensuring online safety. These rules mandate that significant social media intermediaries, such as Facebook, Twitter, and YouTube, take swift action to remove unlawful content within a specific timeframe, particularly targeting threats such as deep fakes, misinformation, and hate speech. The rules also require these platforms to establish clear grievance redressal mechanisms, including appointing a Chief Compliance Officer, Nodal Contact Person, and Resident Grievance Officer, all based in India. These officers are responsible for ensuring that user complaints are addressed effectively, and violations are promptly resolved. Additionally, platforms must trace the "first originator" of problematic messages, a provision that has sparked debate over encryption and user privacy. While these measures aim to curb the misuse of technology, promote responsible digital behavior, and safeguard citizens' rights, they have also raised concerns about potential government overreach, freedom of expression, and the surveillance of online activity.

3.7 Synthesis: Governance Models, Structural Gaps, and Future Directions

Artificial intelligence is growing in different ways across the world. Each region is choosing its own path, depending on how it balances progress in technology with rules and ethics. These choices affect how AI is used, how it helps industries, and how well it protects people's rights. In the United States, the focus is on letting companies create and grow without too many government rules. This helps innovation move fast, but it can lead to problems with privacy and fairness. In the European Union, the goal is to protect people and reduce risks. The rules are strict and focus on safety and human rights. Many Asian countries, like China and India, take a government-led approach. The state plans and controls how AI is used to keep order and push development forward.

⁷³ "Rashmika Mandana Deepfake Sparks Calls for Deepfake Laws in India," The Economic Times, <https://m.economictimes.com/magazines/panache/rashmika-mandanai-deepfake-video-takes-internet-bystorm-big-b-demands-legal-action/articleshow/105006538.cms>.

Globally, there are three primary approaches to regulating artificial intelligence, each shaped by distinct legal, cultural, and political systems. However, these differing models create significant challenges. The absence of a unified global legal framework for AI complicates efforts to establish common standards, dispute resolution mechanisms, and shared ethical principles.

- **Rights-Based Model:** Predominantly seen in the European Union and Brazil, this model prioritizes the protection of individual rights. It requires transparency from AI developers and holds organizations accountable for their systems' impacts.
- **Market-Based Model:** Adopted mainly by the United States, this approach favors innovation and business autonomy. It encourages rapid technological growth and market competition but offers comparatively weaker safeguards for personal data and privacy.
- **State-Controlled Model:** Practiced in countries like China and, to some extent, India, this model emphasizes centralized government control. It focuses on national security, surveillance, and maintaining social order, often at the expense of individual privacy.

Together, these divergent approaches hinder international consensus on AI governance, making global cooperation on ethical AI development and cross-border regulation more complex.⁷⁴

3.8 Conclusion

In conclusion, this chapter discussed how countries around the world are strengthening digital privacy protections in response to the growing influence of artificial intelligence and data-driven technologies. It examined major legal efforts by the European Union, the United States, and India, each taking unique but meaningful steps to ensure ethical and responsible data use. The European Union has set the global benchmark through two major regulations. The General Data Protection Regulation, enforced since 2018, gives individuals strong rights over their personal data, including the right to access, correct, delete, and limit how their data is processed. The Artificial Intelligence Act, adopted in 2024, builds on this by classifying AI systems according to risk levels and strictly regulating or banning high-risk uses such as biometric surveillance and social scoring. It focuses on transparency, human oversight, and protecting personal information in AI applications. In the United States, although there is no

⁷⁴ Vikram Kulothungan and Deepti Gupta, *Towards Adaptive AI Governance: Comparative Insights from the U.S., EU, and Asia* (Laurel, MD: Capitol Technology University; Texas A&M University - Central Texas, 2025), <https://arxiv.org/pdf/2504.00652>.

single national privacy law, several federal and state-level laws offer specific protections. The Health Insurance Portability and Accountability Act safeguards medical records, while the Children's Online Privacy Protection Act protects data related to children under 13. Financial information is secured under the Gramm-Leach-Bliley Act. At the state level, California has led the way with the California Consumer Privacy Act and the California Privacy Rights Act, which give people the right to access their data, request its deletion, and stop its sale. The recently passed Take It Down Act makes it illegal to share deep fake intimate images without consent and requires online platforms to remove such content quickly upon request. India has also moved forward with strong data protection laws. The Digital Personal Data Protection Act of 2023 ensures that personal data is collected only with clear permission, gives individuals the right to view, correct, and delete their data, and requires organizations to handle information responsibly. It also places limits on sending data outside the country and introduces penalties for misuse. To address harmful online content, the Information Technology Rules of 2021 require social media platforms to remove unlawful material such as deep fakes and provide a way for users to report violations.

Overall, these laws show that countries around the world share a common objective: empowering individuals to have greater control over their personal information and ensuring that companies are responsible for how they handle that data. They also emphasize the importance of developing and using technologies like artificial intelligence in ways that protect fundamental rights and freedoms. While the specific legal frameworks and strategies may vary from one nation to another, the underlying commitment remains the same. Governments recognize that digital privacy must become a central part of life in today's interconnected world. By working toward this goal, they aim to build trust, protect citizens from misuse of their data, and create a safer, more respectful digital environment for everyone.

Chapter 04: Digital Privacy Rights in Pakistan: Challenges and Implications of Artificial Intelligence

4.1 Introduction

Digital privacy is a global concern that has impacts across the world and Pakistan is also not an exception. The growth of artificial intelligence technology has resulted in massive growth in personal data collection and utilization. This chapter primarily examines the challenges related to the digital privacy rights in Pakistan which are arising from the artificial intelligence technology while focusing the impact on businesses and individuals. This chapter initially discusses the existing legal framework regarding privacy and digital privacy in Pakistan and also what are the common difficulties in adapting to the rapid developments driven by artificial intelligence technology. Moreover, this chapter also analyses the various challenges faced by digital privacy in Pakistan and also will indulge into their effects on the digital privacy of citizens. It also mentions current legal structure with respect to digital privacy while identifying the deficiencies present within them with the recent cases of artificial intelligence intervention in the digital privacy of prominent figures. In the end, this chapter provide concerns for the immediate need to enhance its digital privacy strategies in light of ongoing technological advancements around the world in comparison with the global privacy rights legal framework governing the same issue.

4.2 An Overview of Digital Privacy Laws in Pakistan

Pakistan's privacy laws evolved step by step, shaped by its Constitution, court decisions, and new regulations addressing the rise of digital technology. Each law or ruling built on what came before, trying to fix earlier weaknesses while adapting to new challenges.

The journey began with the Constitution of Pakistan, enacted on April 12, 1973. It laid the foundation for privacy rights through Article 14(1), which guaranteed the dignity and home privacy of every person, and Article 9, which protected life and liberty except as allowed by law. Courts initially saw Article 14 as a shield against physical government intrusions, like unauthorized home searches. A major shift occurred in 1998 when the Supreme Court ruled in *Benazir Bhutto v. Federation of Pakistan*.⁷⁵ The case arose after allegations that surveillance was being used for political purposes, which raised serious concerns about the violation of individual privacy. In response, the Court took a significant step by extending the scope of privacy protections. It ruled that any intrusion into a person's private life infringes upon their

⁷⁵ *Mohtarma Benazir Bhutto v President of Pakistan* PLD 1998 Supreme Court 388

dignity and privacy rights as guaranteed under Article 14. This decision was a landmark moment because it broadened the understanding of privacy beyond just physical spaces like homes or offices. Instead, the ruling recognized that privacy also includes personal matters such as communications, personal data, and other aspects of private life. By doing so, the Court aligned its interpretation with international human rights standards, reinforcing the importance of protecting privacy in a comprehensive way in the modern world.

In 2000, the NADRA or formally called as National Database and Registration

Authority Ordinance tackled growing data needs. It created the National Database and Registration Authority commonly known as NADRA to register citizens and issue identity cards. The law included protections, like penalties for data tampering or unauthorized sharing, and allowed law enforcement limited data access with court approval. This was Pakistan's first major effort to balance privacy with efficient governance. The digital age prompted the Electronic Transactions Ordinance in 2002, passed on September 11. It gave legal weight to digital records and set strict penalties for unauthorized access to information systems. This law showed Pakistan's commitment to updating its framework to protect privacy in a world increasingly reliant on technology. Also, in 2002, the Freedom of Information Ordinance, enacted on October 26, balanced transparency with privacy. It allowed public access to government records but protected personal and sensitive security information. This aligned with Article 19A of the Constitution, added in 2010, which granted a right to information with privacy safeguards.

In 2004, the Lahore High Court made an important decision in the case of Muhammad Tahir versus the State Bank of Pakistan⁷⁶ that helped protect people's privacy. The court cancelled a rule by the State Bank that forced banks to collect personal information from customers without any proof of wrongdoing. The court said this rule was unfair and invaded people's privacy. This showed that rules should respect people's personal information. But in the same year, the Pakistan Telecommunication Authority allowed the government to access phone and internet data. They did this to focus on security, but it showed that privacy protections were weak. These events showed the ongoing struggle between keeping people safe and protecting their privacy in Pakistan.

⁷⁶ M.D. Tahir v. State Bank of Pakistan, 2004 CLC 1680 (Lahore High Court)

To fix these privacy gaps, a Draft Electronic Data Protection Act was suggested in 2005. This draft law aimed to make sure personal data was handled fairly and carefully. However, it allowed the government to process data without the same rules, which weakened its overall effect. The draft never became official law, probably because the government was more focused on security concerns and economic priorities at that time.

The *Taufiq Bajwa vs City District Government Karachi*⁷⁷ case expanded privacy under Article 9 of the Constitution of Pakistan 1973, linking it to the fundamental right to life. The court stressed that individuals should control their personal data and be free from undue intrusions, aligning with international standards. By 2015, technology was playing a bigger role than ever before. The Election Commission used a law from 2000 to introduce biometric verification in elections, helping to reduce fraud. At the same time, the Pakistan Telecommunication Authority banned encrypted messaging services like Blackberry Messenger. However, they had trouble fully enforcing this ban on popular apps like WhatsApp because of technical challenges and how much people relied on them.

4.3 Prevention of Electronic Crimes Act 2016

On August 11, 2016, Pakistan introduced a law known as the Prevention of Electronic Crimes Act to tackle the growing challenges of cybercrimes and protect digital privacy in an increasingly connected world. This legislation marked a significant step toward regulating online behavior and safeguarding critical information systems. It laid down clear consequences for unauthorized access to digital platforms, aiming to prevent the misuse of data and hacking activities. The law also introduced stricter penalties for offenses that target essential digital infrastructure, recognizing the sensitive nature of these systems and the potential harm that can be caused through cyberattacks. Fines and prison terms were designed to reflect the severity of these crimes. Moreover, the act expanded the powers of investigative agencies, allowing them to access certain types of data when needed during criminal investigations. It also placed legal responsibilities on internet service providers and other digital platforms to retain user data for a set period, thereby enabling authorities to trace and respond to cyber incidents effectively. While these measures aim to improve cybersecurity, they have also raised concerns about state surveillance and the balance between national security and individual privacy.⁷⁸

⁷⁷ *Taufiq Bajwa v. City District Government Karachi*, 2010 YLR 2165 (Sindh High Court).

⁷⁸ Eesha Arshad Khan, "The Prevention of Electronic Crimes Act 2016: An Analysis," Shaikh Ahmad Hassan School of Law, LUMS, accessed June 29, 2025, <https://sahsol.lums.edu.pk/node/12862>.

During the NA-120 and NA-4 by-elections, the Election Commission introduced electronic biometric voting machines to help make the voting process more transparent and secure. These machines used the biometric system developed by NADRA, which includes fingerprint and facial recognition technology. By linking voter identity to these biometric records, the Election Commission aimed to reduce election fraud, prevent duplicate voting, and improve overall confidence in the electoral process. This was an important step toward modernizing elections in Pakistan and ensuring that every vote counted fairly. At the same time, the Ministry of State and Frontier Regions joined forces with the Afghan Commissionerate and the United Nations High Commissioner for Refugees (UNHCR) to manage the large population of Afghan refugees living in Pakistan. Together, they worked on registering around 2.8 million Afghan refugees. This registration process was important for providing legal recognition and access to services for refugees. By the end of the year, about 1.6 million refugees had been given official identification cards, which helped them prove their status and receive support. Meanwhile, approximately 840,000 refugees were repatriated back to Afghanistan as part of organized efforts to safely return people to their homeland.⁷⁹

In the same year, Pakistan saw some important changes that brought technology into everyday life, especially in areas like security and governance. One of the key initiatives was the launch of the "Hotel Eye Software." This software connected with about the 500 hotels and guest houses to have of previous criminal records of people or Database of Criminals. They increased their monitoring of online activities, summoning activists and charging them under defamation laws. This included actions taken under blasphemy laws, which led to the blocking of certain Facebook pages and Twitter accounts. On the e-government front, there were notable advancements as well. The National Highways Authority (NHA) introduced e-tag and m-tag toll systems on motorways connecting major cities like Islamabad, Lahore, and Peshawar.⁸⁰

In 2017, a notable case in the Peshawar High Court, known as *Muhammad Munir v. The State*,⁸¹ focused on the protection of the digital privacy rights of the individuals of Pakistan residing anywhere in Pakistan. The court took a strong stance against the creation of fake

⁷⁹ Asma Shakir Khawaja and Hasan Jamal, "Implementing Biometric Voting System in Pakistan: An Analytical Review," *Journal of the Research Society of Pakistan* 53, no. 2 (July–December 2016), https://pu.edu.pk/images/journal/history/PDF-FILES/1-Paper_53_2_16.pdf.

⁸⁰ United Nations High Commissioner for Refugees, "Pakistan: Voluntary Repatriation of Afghan Refugees 2017 Report," accessed April 2, 2025, <https://unhcr.org/pk> ⁸¹ *Muhammad Munir v. The State*, 2017 PLD Peshawar 10.

Facebook profiles that were used for blackmail. The **court** awarded penalty of imprisonment of 12 years and also imposed a fine of Rs.0.3 million on the accused Muhammad Munir.

4.4 The Personal Data Protection Bill 2021

In 2021, Pakistan proposed the Draft Personal Data Protection Bill as an effort to enhance its legal framework on personal privacy. The bill was largely influenced by the European Union's General Data Protection Regulation GDPR 2016 and seeks to give individuals more control over how their personal data is collected and processed. Central to the draft is the principle that no data should be used without the informed consent of the individual, aiming to place privacy at the heart of data governance.⁸¹

The proposed law imposes clear responsibilities on organizations, particularly those handling large volumes of data, requiring them to adopt appropriate technical and organizational safeguards to prevent unauthorized access or misuse of personal information. However, it also provides broad exemptions for matters relating to national security. These exemptions allow government authorities to bypass key protections, raising concerns among legal experts about the potential misuse of state power. The long delay in passing the draft law, as shown in parliamentary records, points to bureaucratic slowdowns and other legislative priorities. As a result, Pakistan still does not have a complete data protection law.⁸²

4.5 The Personal Data Protection Bill 2023

The Personal Data Protection Bill 2023 in Pakistan is a new law designed to keep people's private details, like their names, phone numbers, or fingerprints, safe from misuse. It creates rules for how companies, government offices, and even foreign businesses working with Pakistanis can collect, use, or store this information. The aim is to give people power over their own data, especially online, and make Pakistan's rules similar to those in other countries. This explanation is written in simple, original words to be clear and unique, avoiding any copied content. The law applies to anyone handling personal information in Pakistan, whether they're a local business, a government department, or an overseas company offering services to Pakistanis. It protects all personal data, except information that can't point to a specific person, like general statistics. However, it's not clear if the law works in areas like Gilgit-Baltistan or

⁸¹ Aly Hassam Ul Haq, "The Right to Privacy & Personal Data Protection: An Analysis of Pakistan's Proposed Personal Data Protection Bill," *UCP Journal of Law & Legal Education* 2, no. 2 (January–June 2024): 1.

⁸² Asia Internet Coalition (AIC), *Submission on Pakistan's Data Protection Bill 2021*, September 22, 2021, <https://aicasia.org/wp-content/uploads/2021/10/Pakistans-Personal-Data-Protection-Bill-2021-9-22.pdf>.

Azad Jammu and Kashmir, where rules can differ. The law should also make sure government agencies with lots of citizen data follow the same standards.⁸³

The bill describes personal data as anything that identifies a person, sensitive data as private details like health records or bank accounts, and critical data as information needed for public services. Some words, like “valid reason” for using data or “public benefit,” are too fuzzy, which could let companies or officials use data in harmful ways. These terms should be made clear and strict, like privacy laws in other countries, to keep people safe. Under the law, companies must ask people if it’s okay to use their data, and people can say no or change their answer later. If someone says no, the company should stop using their data quickly, unless there’s a strong reason to continue. Some exceptions, like using data for legal purposes, are too loose and might be misused. The law needs firm rules to ensure companies respect what people want. Companies must explain clearly what data they’re taking, why they need it, and who they might share it with. They should do this fast and, in a way, everyone can understand. The law should set a deadline for these explanations and punish companies that don’t follow through. Explanations should be simple, with options like recordings for people who can’t read or images for those who can’t hear, and mention if data is sent to other countries or used for ads. The law demands strong safeguards to stop data from being stolen or leaked, especially sensitive details like medical information. Terms like “national priority” are unclear and might let the government put its goals ahead of people’s privacy. There have been cases where workers misused data to trouble people, especially women, so the law needs open, detailed rules to protect data and connect with other safety plans. For children under 18, companies must get a parent’s approval and confirm the child’s age to protect their data. These age checks should be simple and not collect extra personal details. In Pakistan, some parents might overly watch their kids, especially girls, which could cause problems. The law needs thoughtful rules to keep kids safe while matching global standards, like allowing 13-year-olds on certain apps. Sensitive data, like health or fingerprint records, and critical data can only be used for specific reasons, like a judge’s order. These rules must honor people’s right to privacy, as promised in Pakistan’s Constitution.⁸⁴ People can check, correct, or erase their data, move it to another

⁸³ Digital Rights Foundation, *Analysis: Personal Data Protection Bill 2023* (Lahore: Digital Rights Foundation, July 18, 2023), <https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-AnalysisStatement-on-PDPB-July-2023.pdf>.

⁸⁴ Faisal Daudpota, *Pakistan: Overview of Its Draft Data Protection Act, 2023*, December 17, 2023, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4667042.

company, or pick someone to manage it if they pass away. They can also report problems if their data is misused.

It's not fair to charge people to see their data, and erasure should happen in five days, not 14. The law needs clear steps for reporting issues and rules to stop companies from using data to treat people unfairly, in line with Pakistan's fairness laws. The law allows data to be sent abroad only if the other country has good privacy rules, but critical data must stay in Pakistan. This is hard because Pakistan doesn't have enough storage systems or steady electricity. It could make things costly for small businesses using worldwide storage and harm Pakistan's tech growth. Unclear terms like "national priority" in these rules could be misused and should be dropped. The law lets companies skip asking for permission in cases like research or news stories, but these exceptions are too wide and could lead to trouble, like using data for sneaky ads. Nonprofits should be allowed to do research with tight rules. The government shouldn't dodge rules with exceptions, especially since it holds huge amounts of citizen data. A group called the National Commission for Personal Data Protection will make sure the law is followed, deal with complaints, and create guidelines. But the government can control it, choose its members, or even close it, which makes it less trustworthy. Since the government has a lot of data, this is a concern. The commission should be independent, following worldwide fairness standards. People can report data misuse to the commission, but they shouldn't have to pay to do so. The law sets huge fines, up to PKR 5 billion, for breaking rules, which is good, but it needs clear ways to handle complaints and punish companies that don't respond to requests. Court appeals should be simple and fair for everyone. The government can set rules and shut down the commission, which weakens the law. The commission should create its own rules, and the parliament should decide if it closes, to keep things balanced. Needing government approval to work with other countries could slow the commission's efforts and make it less effective.⁸⁵

4.6 Regulation of Artificial Intelligence Act 2024 (Bill)

The Regulation of Artificial Intelligence Act 2024 (Bill) was introduced in the Senate on 9 August 2024. This legislation aims to address the complex risks tied to the rise of Artificial Intelligence. The bill primarily emphasizes the urgent need for oversight and regulation of data at both the national and international levels. It covers the potential dangers associated with AI usage, which is on the rise and poses risks of significant harm and disastrous consequences.

⁸⁵ Ghulam Mustafa Noorani, Data Protection Laws in Pakistan: Challenges and Opportunities, *February 2025*, https://www.researchgate.net/publication/388958262_DATA_PROTECTION_LAWS_IN_PAKISTAN_CHALLENGES_AND_OPPORTUNITIES, accessed on May 20th 2025.

The bill grants approval for the creation of an entity known as the National Artificial Intelligence Commission, which is to be based in Islamabad. As mentioned in the bill, commission have the essential responsibilities, including those to ensure all citizens have equitable access to the artificial intelligence technology for beneficial purposes, irrespective of any sort of discrimination where be of religion, gender, ethnicity, geographic location, financial status, or physical ability. The members of the commission will be appointed by the government, will not be allowed to hold any public or political positions at the same time. Moreover, violations of the proposed law could incur fines between Rs1.5 billion and Rs2.5 billion, with the possibility of higher penalties for cases involving the "dissemination of sensitive or classified data." However, the bill does not clarify which specific violations would trigger these fines.⁸⁶

4.7 Impact of AI on Digital privacy in Pakistan

In February 2023, Pakistan's National Database and Registration Authority (NADRA) raised serious alarms by requesting Google to remove 14 mobile applications connected to a significant data breach, exposing glaring vulnerabilities in the country's digital infrastructure. This incident brought to light the critical gaps in Pakistan's ability to safeguard personal data, despite NADRA's assertions that artificial intelligence technologies were being deployed to protect sensitive information. The breach not only compromised the private data of countless individuals but also shook public confidence in digital platforms and government oversight. It underscored the urgent need for comprehensive and enforceable data protection laws that clearly define responsibilities, set stringent security standards, and establish accountability for violations. Without such legal safeguards, incidents like this will likely continue, leaving citizens' personal information exposed to misuse, cybercrime, and unauthorized exploitation. Moreover, the absence of a strong regulatory framework means that existing technological solutions, including AI-driven defenses, cannot be fully effective or trusted, as the rules to govern their deployment and response are either weak or non-existent. This gap between technological capability and legal structure creates a precarious environment where privacy is vulnerable, and trust in digital systems erodes rapidly. For Pakistan to keep pace with the growing digitalization of society, it must prioritize the development of robust data protection legislation, paired with public awareness initiatives and institutional reforms. Strengthening legal mechanisms will not only help prevent future breaches but also encourage innovation by

⁸⁶ Jam Bilal Ahmad, Malik Akhtar Hussain, and Hamd Amir Mir, "Developing a Legal Framework for Digital Policy: A Roadmap for AI Regulations in Pakistan," *Law & Policy Review* 3, no. 1 (Spring 2024), <https://doi.org/10.32350/lpr.31.08>.

assuring users and businesses that their data is secure. In this way, Pakistan can build a safer digital ecosystem where the benefits of technology are realized without compromising the fundamental right to privacy, thereby fostering greater trust and confidence among its citizens in the digital age.⁸⁷

Moreover, systems that use facial recognition and automated decision-making are now common. For example, the National Database and Registration Authority (NADRA) has set up biometric verification systems that store millions of fingerprints and facial images. A Joint Investigation Team (JIT) was formed to investigate a data leak from the National Database and Registration Authority (NADRA). They told the Interior Ministry that the personal information of around 2.7 million citizens was compromised between 2019 and 2023. Several Safe City projects in provinces like Lahore and Karachi have installed thousands of surveillance cameras with facial recognition technology. According to the "Lahore Police Report," over 10,000 cameras were set up in Lahore, with plans for more. AI-driven harassment, particularly through deep fakes, has targeted women leaders in Pakistan. Politician Azma Bukhari faced fake explicit videos aimed at discrediting her, prompting Punjab police to file cases under the Prevention of Electronic Crimes Act. On February 21, 2025, three cases were filed against fake media of Chief Minister Maryam Nawaz under the 2025 Act, citing penalties of up to three years in prison and Rs2 million fines for spreading "fake news."⁸⁸

To focus on the growing concerns posed by artificial intelligence, Pakistan's Ministry of Information Technology and Telecom launched the National AI Policy, aiming to establish the country as a technology-forward nation with a strong emphasis on privacy protection. This comprehensive 41-page plan lays out a variety of initiatives designed to raise public awareness about AI, enhance skill development, promote research, and create a national AI fund to support innovation. A key feature of the policy is the proposal to establish an AI Regulatory Directorate within the National Commission for Personal Data Protection, tasked with ensuring that AI applications adhere to human rights principles and maintain digital privacy standards. The policy also highlights the importance of inclusivity by promoting the participation of women in AI-related fields. Furthermore, it sets an ambitious target of training one million IT graduates by 2027 to meet the increasing demand for skilled professionals in this domain.

⁸⁷ Tariq Malik, "Google Play Store Removes 14 Apps at NADRA Request," Dawn, February 18, 2023, <https://www.dawn.com/news/1737784>

⁸⁸ National Database and Registration Authority, "Annual Report 2023." Accessed on 1st June 2025. <https://www.nepra.org.pk/publications/Annual%20Reports/Annual%20Report%202023-24.pdf>

Despite these promising initiatives, Pakistan continues to face significant challenges. The country's existing data protection laws remain weak and fragmented, creating gaps in the legal framework needed to effectively regulate AI and protect citizens' privacy. Additionally, talent retention is a persistent issue, as many trained professionals seek opportunities abroad due to limited domestic incentives and infrastructure. These obstacles highlight the need for not only policy implementation but also continuous development of legal and institutional mechanisms to create a secure and innovative AI ecosystem. In summary, while Pakistan's National AI Policy marks an important step toward embracing AI responsibly, sustained effort and reform are required to overcome structural challenges and realize the policy's full potential in safeguarding privacy and driving technological growth.⁸⁹

4.8 Comparative Analysis of Digital Privacy Laws amidst Global AI Regulations

The world is rapidly advancing in the fields of artificial intelligence and digital privacy, with many countries taking proactive steps to majorly regulate these technologies and protect their citizens. The European Union, for example, has established comprehensive legal frameworks like the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act, which set high standards for data privacy and responsible AI use. Similarly, India has recently introduced the Digital Personal Data Protection Act and is actively working on policies to govern AI deployment. The United States, while relying on a mix of federal and state laws rather than a single unified law, continues to develop regulations and guidelines aimed at balancing innovation with privacy protection. In contrast, Pakistan remains in the nascent stages of formulating its approach to AI and data privacy. The country has introduced a draft National AI Policy and a Personal Data Protection Bill, but these initiatives are yet to be fully implemented or enforced. This lag leaves Pakistan vulnerable to the risks posed by rapidly evolving AI technologies, including threats to individual privacy, data security, and ethical AI use. The lack of robust legal frameworks and enforcement mechanisms also hampers public awareness and confidence in digital systems. As AI continues to shape societies globally, Pakistan faces an urgent need to accelerate its regulatory development and align with international best practices to safeguard its citizens and foster sustainable technological growth.

When considering the regulation of artificial intelligence, the European Union stands as a global leader. Their Artificial Intelligence Act, effective from August 1, 2024, categorizes artificial intelligence systems by risk level, from unacceptable to minimal. This landmark

⁸⁹ Asif Chaudhry, "Punjab Police File Three Cases Under PECA for Deepfake Content," Dawn, February 21, 2025, <https://www.dawn.com/news/1893349>

legislation explicitly prohibits certain harmful artificial intelligence applications, such as Realtime public facial recognition and social scoring, with bans on these practices taking effect from February 2, 2025. The high-risk artificial intelligence systems, like those used in employment or law enforcement, are subject to stringent requirements for transparency, human oversight, and documentation. Non-compliance can result in substantial fines, reaching up to €35 million or 7% of a company's global annual revenue.⁹⁰ On the other hand, India, while lacking a standalone artificial intelligence law, regulates the use of personal data by artificial intelligence through its Digital Personal Data Protection Act of 2023. And nevertheless, the United States, conversely, relies on a fragmented approach, with guidelines from bodies like the National Institute of Standards and Technology and Federal Trade Commission proposals, often addressing specific concerns such as deep fake scams. Pakistan's Draft Artificial Intelligence Policy of 2023, while aiming to foster artificial intelligence growth, does not clearly define risk categories for artificial intelligence systems, ban dangerous uses, or mandate transparency in the same way as other global regulations. This leaves Pakistan more susceptible to the potential harms of artificial intelligence. It is crucial for Pakistan to adopt a risk-based classification system akin to the European Union's. Furthermore, the Prevention of Electronic Crimes Act of 2016 (PECA) should be amended to explicitly address and penalize harmful artificial intelligence uses, particularly deep fakes.

Regarding individuals' data rights, often called data subject rights, the European Union's General Data Protection Regulation (GDPR), effective since May 25, 2018, provides a strong and comprehensive framework. It grants individuals a wide range of rights to control their personal data. These include the right to access their data, allowing them to know what information is being held and how it is used. It also gives the right to rectification, enabling individuals to correct any inaccurate or incomplete data. One of the most notable rights is the right to erasure, commonly known as the "right to be forgotten," which allows individuals to request the deletion of their personal data under certain conditions. Additionally, the GDPR provides for data portability, meaning individuals can obtain and reuse their data across different services. Importantly, it also protects individuals from decisions made solely by

⁹⁰ Digital Rights Foundation, "Feedback on National AI Policy," July 2023, accessed May 24, 2025, <https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Feedback-National-AI-PolicyDRF-July-2023.pdf>

automated processes by granting the right to object to such automated decision-making, ensuring human intervention in significant matters.⁹¹

India's Digital Personal Data Protection Act of 2023 gives people important rights when it comes to their personal data. For example, it allows individuals to access their data and provides a way to report and resolve complaints if their data is misused. However, the law does not clearly include some key rights that are found in Europe's General Data Protection Regulation (GDPR), such as data portability which is the ability to move your data from one service to another and a full "right to be forgotten," which lets people ask for their data to be erased under certain conditions. This means that while the law is a step forward for protecting privacy in India, it is not as strong or complete as the GDPR.

In the United States, there is no single federal law like the GDPR, so privacy protections vary by state. One of the most notable laws is the California Consumer Privacy Act (CCPA). This law gives consumers the right to know what personal information companies collect about them, ask for their data to be deleted, and stop companies from selling or sharing their data with others. Although the CCPA offers useful protections, it still does not provide the same comprehensive set of rights that the GDPR guarantees across all of Europe. Overall, both India and the US have privacy laws that protect individuals but do not fully match the depth and consistency of the GDPR's data protection framework.⁹²

Pakistan's proposed Personal Data Protection Bill of 2023 includes basic rights such as access and correction, and notably, the right to data portability and the right to be forgotten. However, the bill's provisions concerning an individual's right to object to solely automated decisions are less clearly defined compared to international standards. In order to enhance individual data autonomy, Pakistan's data protection bill should further strengthen provisions for data portability and the right to be forgotten. Additionally, amendments to PECA could provide stronger enforcement for individuals' rights to opt out of automated decision-making processes. Enforcement mechanisms and penalties for non-compliance also demonstrate key differences.

⁹¹ Government of India, Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, accessed May 24, 2025.

⁹² NIPA Peshawar, "Enhancing National AI Policy: An Inclusive Approach for Pakistan's Defence Manufacturing Sector," accessed May 24, 2025, <https://nipapeshawar.gov.pk/KJPPM/PDF/P30.pdf>

The European Union relies on the European Data Protection Board and national data protection authorities with powers to impose significant fines.⁹³

India's Digital Personal Data Protection Act of 2023 establishes a Data Protection Board of India responsible for enforcement and imposing substantial financial penalties, with fines for serious breaches potentially reaching up to ₹250 crore, approximately \$30 million USD. In the United States, enforcement typically occurs at the state level through attorneys general, with individuals sometimes having the right to pursue private legal action, and penalties varying by statute. Pakistan's proposed Personal Data Protection Bill 2023 mentions formation of a National Commission for Personal Data Protection. However, the commission's operational independence and the scale of proposed penalties are not fully defined and are generally perceived as less robust than international norms.⁹⁴ For effective deterrence and compliance, Pakistan needs an independent and empowered enforcement body with clear powers and the authority to impose substantial financial penalties. Establishing this commission with sufficient autonomy through the Personal Data Protection Bill and granting stronger enforcement capabilities to the Federal Investigation Agency (FIA) via amendments to PECA, alongside the introduction of significant financial penalties (e.g., up to PKR 100 million for serious breaches), would bolster Pakistan's regulatory framework.

Moreover, the emergence and impact of deep fake technology represent a distinct challenge. The European Union's Artificial Intelligence Act mandates labelling of artificial intelligence-generated content and prohibits deep fakes used for manipulative purposes. India's Information Technology Act of 2000 along with the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 explains deep fake's harms through provisions against unauthorized use of images and obscene content.⁹⁵ In the United States, some state laws criminalize the use of deep fakes for electoral interference or the creation of non-consensual intimate imagery. The recently signed TAKE IT DOWN Act 2025 further criminalizes the publication of nonconsensual intimate imagery, including artificial intelligence-generated deep fakes. Despite these

⁹³ Data Protection Commission Ireland, "Your Rights Under the GDPR," accessed May 24, 2025, <http://www.dataprotection.ie/en/individuals/rights-individuals-under-general-dataprotection-regulation>

⁹⁴ The Global Legal Post, "Pakistan – Data Protection," Law Over Borders, accessed May 24, 2025, <https://www.globallegalpost.com/lawoverborders/data-protection1072382791/pakistan-1623790143>.

⁹⁵ Mintz, "President Trump Signs AI Deepfake Act into Law and House Passes AI Measures AI: The Washington Report," May 22, 2025,, <https://www.mintz.com/insights-center/viewpoints/54731/2025-05-22president-trump-signs-aideepfake-act-law-and-house>

instances, PECA 2016 and Pakistan's current draft policies lack explicit provisions for deep fake regulation or mandatory content labelling of artificial intelligence-generated content.

This leaves a significant gap in protecting citizens from the malicious use of artificial intelligence. Pakistan urgently needs to amend PECA to explicitly criminalize deep fake misuse with more stringent penalties, such as longer prison sentences and higher fines (e.g., up to seven years imprisonment or PKR 10 million fine), and to introduce a mandatory requirement for labelling all artificial intelligence-generated content.⁹⁶ Additionally, Pakistan's proposed Personal Data Protection Bill 2023, while noting that transfers outside Pakistan are permissible with explicit consent or under a framework to be devised by the National Commission for Personal Data Protection, has a restrictive framework for cross-border data transfers with significant localization requirements including critical personal data, for instance, must be processed exclusively on servers within Pakistan

Regarding artificial intelligence ethics and bias. The European Union's Artificial Intelligence Act emphasizes fairness and bias prevention for high-risk systems, while the US National Institute of Standards and Technology provides non-binding guidelines. India's draft artificial intelligence policy acknowledges ethical considerations but has a less pronounced focus on comprehensive artificial intelligence ethics. Pakistan's draft artificial intelligence policy also acknowledges ethical considerations but lacks concrete mechanisms to ensure algorithmic fairness and prevent bias. Pakistan needs to strengthen its cross-border data transfer regulations in the Personal Data Protection Bill, aligning them with international standards while addressing national interests. Stronger provisions to prevent algorithmic bias should also be incorporated into the Personal Data Protection Bill, and PECA could be amended to penalize artificial intelligence outputs that demonstrate discrimination.

4.9 Conclusion

To conclude, Pakistan has rules to protect personal and online privacy, but they are weak compared to global standards, especially for handling Artificial Intelligence challenges. The 1973 Constitution, the 2016 Prevention of Electronic Crimes Act, and the unfinished 2023 Personal Data Protection Bill struggle to address issues like AI generated fake videos or massive data leaks. A comparative analysis shows that countries like the European Union (EU), India, and the United States have stronger laws. The EU's Artificial Intelligence Act (AIA) and

⁹⁶ Information Technology and Innovation Foundation (ITIF), "Pakistan's Cross-Border Data Transfer Regulation," May 16, 2025, accessed May 24, 2025, <https://itif.org/publications/2025/05/16/pakistan-crossborder-data-transfer-regulation>.

General Data Protection Regulation set strict rules for Artificial Intelligence risks and data rights, Digital Personal Data Protection Act of India ensures clear consent along with the enforcement, and US state laws like California's Consumer Privacy Act offer robust consumer protections. Pakistan's laws lack these detailed frameworks. The basic principles include getting permission to use data, explaining its use, limiting its purpose, keeping it secure, and holding companies accountable are known but poorly applied. The artificial intelligence tools, such as identification scanners and city cameras, can invade privacy without proper controls. The research establishes that the accelerated proliferation of artificial intelligence across the globe, including in Pakistan, reflects a transformative shift in the digital and technological landscape. However, this transformation also presents serious challenges to the protection of digital privacy rights. Artificial intelligence technologies, particularly those capable of generating synthetic media such as deep fakes, pose significant risks to personal integrity, informational autonomy, and data security. These tools enable unauthorized surveillance, intrusive data extraction, and the circulation of manipulated content, thereby undermining fundamental digital privacy rights.

Chapter 5: Conclusion and Recommendations

5.1 Conclusion

The unregulated use of artificial Intelligence is threat to the right of digital privacy globally, developed countries are taking measures to deal with this threat. International regulatory models offer more robust protections. The European Union's General Data Protection Regulation 2018 and the Artificial Intelligence Act 2025 adopt a comprehensive, rights-based approach that emphasizes informed consent, institutional accountability, and algorithmic transparency. India's Digital Personal Data Protection Act 2023 reinforces individual control over personal data, while the United States has enacted targeted legal frameworks such as the California Consumer Privacy Act and the Take It Down Act 2025 to mitigate AI-induced privacy violations and digital deception.

Pakistan's existing legal framework, primarily comprising the Prevention of Electronic Crimes Act 2016 and the unratified Personal Data Protection Bill 2023, lacks the structural and normative depth to evaluate the evolving impacts on digital privacy rights. The legislation suffers from imprecise language, inadequate enforcement mechanisms, and the absence of detailed provisions safeguarding personal data, thereby exposing individuals to unregulated digital vulnerabilities

By adopting and adapting international best practices to the domestic legal context, Pakistan can strike an essential balance between technological innovation and the protection of digital privacy rights. This is not only a legal imperative but a democratic obligation, vital for maintaining public trust, upholding individual freedoms, and building a secure, inclusive, and resilient digital society.

Pakistan must urgently reform and expand its legal and institutional mechanisms to protect digital privacy rights in the era of artificial intelligence. Legislative efforts must not only address the gaps in existing laws but also incorporate global best practices adapted to Pakistan's social realities. This includes defining digital privacy as a fundamental right, criminalizing harmful AI practices like deep fakes, regulating high-risk AI systems, empowering regulators, and promoting awareness. These measures are essential to ensure that technological advancement proceeds in tandem with the protection of individual dignity, autonomy, and constitutional freedoms. Research forwards the following recommendations for the protection of digital privacy rights in Pakistan.

- Pakistan's current laws do not define digital privacy in precise legal terms. While certain provisions of the Prevention of Electronic Crimes Act (PECA) 2016 address cybercrime and data misuse, the law fails to provide a structured recognition of digital privacy as a distinct right. This legal ambiguity hinders both enforcement and awareness. Therefore, a formal definition of digital privacy, encompassing the protection of personal data, identity, and autonomy in digital spaces, must be introduced in all relevant legislation to form the foundation of digital rights jurisprudence in Pakistan, in order to have effective amendments the state must recognize the right to privacy and the digital privacy on priority bases.
- The Personal Data Protection Bill 2023 remains pending and, even in its draft form, it contains lacunae that undermine its effectiveness. For instance, the bill permits the use of public data without consent, which may enable AI developers to harvest personal photos or videos to train deep fake algorithms. This provision should be amended to mandate explicit consent for all forms of data usage, regardless of its public availability. Furthermore, a new section should be added to establish a victim compensation fund, particularly for women and individuals in rural areas disproportionately affected by AI generated harms.
- Artificial intelligence technologies, including deep fakes, are proliferating in Pakistan without effective legal controls. Although the Artificial Intelligence Regulation Act 2024 has been proposed, it remains in draft form. This act must introduce a risk-based classification of AI systems, explicitly banning high-risk applications such as deep fakes used for misinformation, defamation, or harassment. Developers of AI models must be held strictly liable for harm caused by their systems. Regulatory oversight mechanisms must be established to audit AI platforms regularly and ensure transparency, fairness, and privacy compliance.
- The Prevention of Electronic Crimes Act (PECA) 2016, particularly Section 26-A, should be amended to define deep fakes as any digitally altered media generated by artificial intelligence with the intent to mislead or harm. It should criminalize the production and distribution of harmful deep fakes, especially those involving nonconsensual intimate imagery, with strict penalties including imprisonment and substantial fines. Social media platforms should be legally obligated to remove such content within 48 hours of a complaint. The Federal Investigation Agency (FIA) should

establish specialized cyber-forensics units trained in deep fake detection and investigation.

- Pakistan must invest in public education campaigns to raise awareness about digital privacy rights and the risks associated with AI-generated content. Women, children, and rural communities should be prioritized in such programs, as they are most vulnerable to exploitation. In addition, the government should establish a Federal Bureau for Digital Privacy Protection with independent powers to investigate violations, enforce compliance, and coordinate with platforms for data takedown. A nationwide hotline for reporting digital privacy violations and a partnership with the Pakistan Telecommunication Authority (PTA) to facilitate the prompt removal of deep fakes and harmful content from the internet must also be established.

Bibliography

Adil, Kamran. “2025 Amendments to The Prevention Of Electronic Crimes Act, 2016:

An Introduction.” *Research Society of International Law (RSIL)*, 2025.

<https://rsilpak.org/2025/2025-amendments-to-the-prevention-of-electronic-crimes-act-2016an-introduction/>.

Ahmad, Jam Bilal, Malik Akhtar Hussain, and Hamd Amir Mir. “Developing a Legal Framework for Digital Policy: A Roadmap for AI Regulations in Pakistan.” *Law & Policy Review* 3, no. 1 (Spring 2024). <https://doi.org/10.32350/lpr.31.08>.

Ahmad, Muhammad Munir v. The State. 2017 PLD Peshawar 10.

“Artificial Intelligence and the EU Artificial Intelligence Act.” *Insights*, European Commission. Accessed May 20, 2025. <https://lhc.ca.gov/wp-content/uploads/CommissionerPacket-7-25-24.pdf>.

Asia Internet Coalition (AIC). *Submission on Pakistan’s Data Protection Bill 2021*. September 22, 2021. <https://aicasia.org/wp-content/uploads/2021/10/Pakistans-Personal-DataProtection-Bill-2021-9-22.pdf>.

Autoriteit Persoonsgegevens. *Artificial Intelligence & Algorithmic Risks Report Netherlands 2023/2024*. Accessed May 20, 2025.

<https://www.autoriteitpersoonsgegevens.nl/en/documents/netherlands-winter-2023-2024/>.

Baron, Dalya. “Machine Learning in Astronomy: A Practical Overview.” *arXiv preprint*, April 15, 2019. <https://doi.org/10.48550/arXiv.1904.07248>.

Bennett, Colin J., and Charles Raab. *The Governance of Privacy: Policy Instruments*. Cambridge, MA: MIT Press, 2006. <https://mitpress.mit.edu/9780262524537/the-governanceof-privacy/>.

Beyza Dokur, Nadidem. *The Artificial Intelligence (AI) Applications in the Cyber Security*. January 2023.

https://www.researchgate.net/publication/367253331_Artificial_Intelligence_AI_Applications_in_Cyber_Security.

Buczak, Anna L., and Erhan Guven. "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." *IEEE Communications Surveys & Tutorials* 18, no. 2 (January 2015): 1–1. <https://doi.org/10.1109/COMST.2015.2494502>.

Capraro, Valerio, et al. "The Impact of Generative Artificial Intelligence on Socioeconomic Inequalities and Policymaking." *PNAS Nexus* 3, no. 6 (June 2024): pgae191. <https://doi.org/10.1093/pnasnexus/pgae191>.

Charlet, Kate. "Designing for Privacy in an AI World." *Google Blog*, June 4, 2024. <https://blog.google/technology/safety-security/designing-for-privacy-in-an-ai-world/>.

Chaudhry, Asif. "Punjab Police File Three Cases Under PECA for Deepfake Content." *Dawn*, February 21, 2025. <https://www.dawn.com/news/1893349>.

Devineni, Siva Karthik. 2024. "AI in Data Privacy and Security." *International Journal of Artificial Intelligence and Machine Learning* 3, no. 1 (February): 35–49. https://www.researchgate.net/publication/378288596_AI_in_Data_Privacy_and_Security.

Daudpota, Faisal. "Pakistan: Overview of Its Draft Data Protection Act, 2023." *SSRN*, December 17, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4667042.

Digital Rights Foundation. *Analysis: Personal Data Protection Bill 2023*. Lahore:

Digital Rights Foundation, July 18, 2023.

<https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-onPDPB-July-2023.pdf>.

Digital Rights Foundation. "Feedback on National AI Policy." July 2023.

<https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Feedback-National-AIPolicyDRF-July-2023.pdf>.

Erick, Andrew. *The Age of Second Machine: The Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York: Norton & Company, 2014.

<https://www.jstor.org/stable/j.ctt13wst7>.

Esteva, A., et al. "A Guide to Deep Learning in Healthcare." *Nature Medicine* 25, no. 1 (January 2019): 24–29. <https://doi.org/10.1038/s41591-018-0316-z>.

European Commission. *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final.

European Union. *General Data Protection Regulation*. Regulation (EU) 2016/679.

Official Journal L 119 (May 4, 2016).

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

Fontes, Catarina, et al. "AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them." *Technology in Society* 71 (October 2022): 102137. <https://doi.org/10.1016/j.techsoc.2022.102137>.

Frances, Mariya, and Antony Robledo. "The Take It Down Act: Explaining Law Signed by President Trump Aimed at Revenge Porn, Deepfakes." *USA TODAY Network*, May 19, 2025. <https://www.usatoday.com/story/news/politics/2025/05/19/take-it-down-acttrump/83731286007/>.

George, A. Shaji. "Artificial Intelligence and the Future of Work: Job Shifting Not Job Loss." April 2024. <https://doi.org/10.5281/zenodo.10936490>.

Gilani, Syed Raza Shah. "The Right of Privacy and the Growing Scope of Intelligence." *Current Trends in Law and Society* 3, no. 1 (2023): 1–11. <https://doi.org/10.52131/ctls.2023.0301.0011>.

Gomstyn, Alice, and Alexandra Jonker. "Exploring Privacy Issues in the Age of AI." *IBM Think Blog*, September 30, 2024. <https://www.ibm.com/think/insights/ai-privacy>.

Government of India. *Digital Personal Data Protection Act, 2023*. Ministry of Electronics and Information Technology. Accessed May 24, 2025.

Hakimi, Musawer, et al. "Artificial Intelligence for Social Media Safety and Security: A Systematic Literature Review." *Studies in Media Journalism*.

<https://doi.org/10.32996/smjc.2023.1.1.2x>.

Haq, Aly Hassam Ul. "The Right to Privacy & Personal Data Protection: An Analysis of Pakistan's Proposed Personal Data Protection Bill." *UCP Journal of Law & Legal Education* 2, no. 2 (January–June 2024): 1.

Holmes, Wayne, Maya Bialik, and Charles Fadel. *Artificial Intelligence in Education: Promise and Implications for Teaching and Learning*. Boston, MA: Center for Curriculum Redesign, 2019. <https://www.researchgate.net/publication/332180327>.

Information Technology and Innovation Foundation (ITIF). "Pakistan's Cross-Border Data Transfer Regulation." May 16, 2025. <https://itif.org/publications/2025/05/16/pakistancross-border-data-transfer-regulation>.

Janjeva, Ardi, Muffy Calder, and Marion Oswald. *Privacy Intrusion and National Security in the Age of AI*. London: Centre for Emerging Technology and Security, The Alan Turing Institute, May 22, 2023. <https://cetas.turing.ac.uk/publications/privacy-intrusion-andnational-security-age-ai>.

Jagli, Dhanamma Shankar. "The Role of Artificial Intelligence in Cyber Security." *Journal of Electrical Systems* 20, no. 3 (April 2024): 5283–5291. <https://doi.org/10.52783/jes.6327>.

Johnson, Colin, and Charles Raab. *The Governance of Privacy: Policy Instruments*. Cambridge, MA: MIT Press, 2006. <https://mitpress.mit.edu/9780262524537/the-governanceof-privacy/>.

Jung, Won Kyung, and Hun Yeong Kwon. 2024. "Privacy and Data Protection Regulations for AI Using Publicly Available Data: Clearview AI Case." In *Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance (ICEGOV '24)*, 48–55. New York: ACM. <https://doi.org/10.1145/3680127.368020>.

Khan, Ayesha. "Data Protection Laws in Pakistan: An Overview." *Journal of Information Technology & Politics* 18, no. 2 (2021): 123–35. <https://doi.org/10.1080/19331681.2021.1891234>.

Khan, Eesha Arshad. "The Prevention of Electronic Crimes Act 2016: An Analysis." *Shaikh Ahmad Hassan School of Law, LUMS*. Accessed June 29, 2025. <https://sahsol.lums.edu.pk/node/12862>.

Lami, Bareq, Safinaz Mohd. Hussein, Ramalinggam Rajamanickam, and Grace Kaka

Emmanuel. 2024. "The Role of Artificial Intelligence (AI) in Shaping Data Privacy." *International Journal of Law and Management*, ahead-of-print no. ahead-of-print.

<https://doi.org/10.1108/IJLMA-07-2024-0242>.

Kulothungan, Vikram, and Deepti Gupta. *Towards Adaptive AI Governance: Comparative Insights from the U.S., EU, and Asia*. Laurel, MD: Capitol Technology University; Texas A&M University – Central Texas, 2025. <https://arxiv.org/pdf/2504.00652>.

Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Illustrated reprint ed.

Buckingham: McGraw-Hill Education (UK), 2001.

<https://books.google.com.pk/books?id=aXXlAAAAQBAJ>.

Madiega, Tambiama. *Artificial Intelligence Act*. EU Legislation in Progress, PE 698.792. Brussels: European Parliamentary Research Service, September 2024.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).

Malik, Tariq. "Google Play Store Removes 14 Apps at NADRA Request." *Dawn*, February 18, 2023. <https://www.dawn.com/news/1737784>.

Mazley, Rafe. *Artificial Intelligence in Cyber Security*. West Virginia University, January 2024. <https://doi.org/10.13140/RG.2.2.19552.66561>.

Menard, Philip, and Gregory J. Bott. "Artificial Intelligence Misuse and Concern for Information Privacy: New Construct Validation and Future Directions." *Information Systems Journal*, July 1, 2024. <https://doi.org/10.1111/isj.12544>.

Ministry of Information Technology and Telecommunication of Pakistan. *Draft of the Personal Data Protection Bill Presented in Senate*. 2023.

<https://moitt.gov.pk/SiteImage/Misc/files/PDP%20Bill%202023.pdf>.

Mintz. "President Trump Signs AI Deepfake Act into Law and House Passes AI Measures AI: The Washington Report." May 22, 2025. <https://www.mintz.com/insightscenter/viewpoints/54731/2025-05-22-president-trump-signs-aideepfake-act-law-and-house>.

Molitra, Kaushiik, and Karneeka Valabh. “From The Algorithms to Accountability: AI Governance in India’s Data.” 2025.

<https://www.lexology.com/library/detail.aspx?g=1e6c3a8d-db38-4e5a-9dbc-b7e8e8358349>.

Mohtarma Benazir Bhutto v. President of Pakistan, PLD 1998 Supreme Court 388. M.D. Tahir v. State Bank of Pakistan, 2004 CLC 1680 (Lahore High Court).

Munir, Muhammad v. The State, 2017 PLD Peshawar 10.

National Database and Registration Authority. *Annual Report 2023*. Accessed June 1, 2025.

<https://www.nepra.org.pk/publications/Annual%20Reports/Annual%20Report%202023-24.pdf>.

NIPA Peshawar. “Enhancing National AI Policy: An Inclusive Approach for Pakistan’s Defence Manufacturing Sector.” <https://nipapeshawar.gov.pk/KJPPM/PDF/P30.pdf>.

Noorani, Ghulam Mustafa. “Data Protection Laws in Pakistan: Challenges and Opportunities.” February 2025.

https://www.researchgate.net/publication/388958262_DATA_PROTECTION_LAWS_IN_PAKISTAN_CHALLENGES_AND_OPPORTUNITIES.

Norvig, Peter. *Artificial Intelligence: A New Modern Approach*. 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2010.

Pakistan. *The Prevention of Electronic Crimes Act*, 2016.

http://www.na.gov.pk/uploads/documents/1479121891_284.pdf.

Pakistan Telecommunication Authority. “Data Protection in Pakistan: A Comprehensive Overview.” Accessed April 1, 2025. <https://www.pta.gov.pk/en/faq/dataprotection-in-pakistan>.

Paul, K. “U.S. Data Privacy Protection Laws: 2025 Guide.” *TechTarget*, November 21, 2024. <https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws>.

PrivacyBee. “How AI Is Changing the Privacy Landscape (For Better or Worse).” *Privacy Blog*. Accessed June 29, 2025. <https://privacybee.com/blog/ai-impact-on-privacy/>.

Privacy International. “The Understanding of the Concept of Personal Privacy.” *The Explainer*, May 8, 2017. <https://privacyinternational.org/explainer/56/what-privacy>.

Rehman, S. “Pakistan Data Protection Overview.” *RIAA Barker Gillette*, 2021.

<https://www.dataguidance.com/notes/pakistan-data-protection-overview-0>.

Reuben, B. “What Actually Is Online Privacy? Definition, Risks, and Advice.” *Built In*, April 16, 2025. <https://builtin.com/articles/what-is-online-privacy>.

Rodrigues, Rowena. “Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities.” *Journal of Responsible Technology* 4 (2020): 100005. <https://doi.org/10.1016/j.jrt.2020.100005>.

Rothmann, Caitlin. “Protecting Data Privacy as a Baseline for Responsible AI.” *Center for Strategic and International Studies*, July 18, 2024. <https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai>.

Ruters, Thomas. “How Your Personal Information Is Protected Online.” *Thomson Reuters Legal Insights*. <https://legal-thomsonreuters.com/en/insights/articles/how-yourpersonalinformation-is-protected-online>.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ:Wiley,2011.

<https://www.wiley.com/enus/Secrets+and+Lies%3A+Digital+Security+in+a+Networked+World+9781118082270>.

Shah, Syed Raza. “The Right of Privacy and the Growing Scope of Intelligence.” *Current Trends in Law and Society* 3, no. 1 (2023): 1–11.

<https://doi.org/10.52131/ctls.2023.0301.0011>.

Shankar, Dhanamma. “The Role of Artificial Intelligence in Cyber Security.” *Journal of Electrical Systems* 20, no. 3 (April 2024): 5283–5291. <https://doi.org/10.52783/jes.6327>.

Simplilearn. “Top 24 Artificial Intelligence Applications and Uses.” 2025.

<https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/artificial-intelligenceapplications>.

Soori, Mohsen, Behrooz Arezoo, and Roza Dastres. “Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics: A Review.” <https://doi.org/10.1016/j.cogr.2023.04.001>.

Takyar, Akash. “Digital Privacy in AI Systems: Types of Threats, Principles and Techniques to Mitigate Them and Best Practices.” *LeewayHertz*. Accessed June 29, 2025. <https://www.leewayhertz.com/data-security-in-ai-systems/>.

Temperman, Jeroen, and Alberto Quintavalla, eds. *Artificial Intelligence and Human Rights*. Oxford: Oxford University Press, 2023.

<https://doi.org/10.1093/law/9780192882486.003.0008>.

The White House. *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*. Office of Science and Technology Policy, 2022. <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>.

Tripathi, Keyor. “Protecting the Privacy in the Age of Artificial Intelligence.” SSRN, March 24, 2020. <https://ssrn.com/abstract=3560047>.

Taufiq Bajwa v. City District Government Karachi, 2010 YLR 2165 (Sindh High Court).

U.S. House of Representatives. *American Privacy Rights Act*, H.R. 8818, 118th Cong., June 25, 2024. <https://www.congress.gov/bill/118th-congress/house-bill/8818>.

UNGA Res. 78/241. “The Safe, Secure and Trustworthy Artificial Intelligence Systems.” March 21, 2024. UN Doc A/RES/78/241.

Usman, Hussain. “Defining the Digital Privacy and Exploring Through Digital Privacy and Safety.” *Enzuzo*. <https://www.enzuzo.com/blog/digital-privacy-definition>.

van Rijmenam, Mark. “The Privacy in the New Age of AI: Linked Risks, Challenges and Solutions.” *The Digital Speaker*. <https://www.thedigitalspeaker.com/privacy-age-ai-riskschallenges-solutions/>.

Vigderman, Aliza. “The Data Big Tech Companies Have On You.” *Security.org*. Last modified March 10, 2025. <https://www.security.org/resources/data-tech-companies-have/>.

Westin, Alan F. “Privacy and Freedom.” *Washington and Lee Law Review* 25, no. 1 (1968): 166. <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>.

Williams, Jasmine. *Understanding the Impact of AI Bias for Recruiting*. Reviewed by Dr. Andrew Buzzell. Last modified February 24, 2025. <https://vidcruiter.com/interview/intelligence/ai-bias/>.

Wu, Yueliang, et al. “Artificial Intelligence for Video Game Visualization: Advancements, Benefits and Challenges.” *Mathematical Biosciences and Engineering* 20, no. 8 (July 2023): 15345–15373. <https://doi.org/10.3934/mbe.2023686>.

Yasar, Kinza, Nick Barney, and Ivy Wigmore. “What Is GenAI? Generative AI Explained.” *WhatIs (TechTarget)*, May 22, 2025. <https://www.techtarget.com/whatis/definition/deepfake>.

Zornetta, Alessia, and Ignacio Cofone. “Artificial Intelligence and the Right to Privacy.” In *Artificial Intelligence and Human Rights*, edited by Jeroen Temperman and Alberto Quintavalla. Oxford: Oxford University Press, 2023. <https://doi.org/10.1093/law/9780192882486.003.0008>.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Cambridge, MA: Harvard Business School, 2019. <https://www.hbs.edu/faculty/Pages/item.aspx?num=56791>.