Interdisciplinary Studies in Society, Law, and Politics 2025; 4(2): 21-38

ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

# Analysis of Legal Challenges and Data Protection Strategies in the Era of Artificial Intelligence in the International Legal System

Zahrasadat. Naghibzakerin[1*], Mitra. Shahabsafa[2], Mohammadreza. Mollahoseini Ardakani[3], Kamal. Mirzaie[3], Seyed Alireza. Azimidokht Shooroki[4]

[1] Master of Science in Artificial Intelligence and Robotics, Meybod Branch, Islamic Azad University, Meybod, Iran
[2] Master of International Trade Law, University of Tehran, Tehran, Iran
[3] Assistant Professor, Department of Computer Engineering, Meybod Branch, Islamic Azad University, Meybod, Iran
[4] Assistant Professor, Department of Philosophy and Islamic Theology, Meybod Branch, Islamic Azad University, Meybod, Iran

*** Corresponding author email address**: z.naghib@iau.ir

**Received:** 2024-09-24 **Revised:** 2024-12-13 **Accepted:** 2024-12-23 **Published:** 2025-04-01

The protection of personal data in the era of artificial intelligence has become an international challenge due to the cross-border nature of data and the complexities of this technology. This study aims to examine and understand the status of the existing international legal system in addressing these challenges. Data for this research were collected through interviews with 14 experts in the field and analyzed using a qualitative approach based on the grounded theory method of Strauss and Corbin (1998). The findings indicate that the international legal system faces inefficiencies in this area, which can be categorized into two main dimensions: "structural challenges" (such as the insufficient coverage of artificial intelligence-specific challenges in international legal instruments, difficulties in enforcing national laws at the international level, and the lack of effective mechanisms for international cooperation) and "conceptual and operational challenges related to artificial intelligence" (such as ambiguities in determining legal liability and the need to define new legal concepts). Therefore, pursuing strategies such as the development of a comprehensive international legal framework, strengthening international cooperation, and ultimately enhancing capacities and establishing international accountability mechanisms is essential to addressing these challenges. This study underscores the necessity of serious attention to the international legal dimensions of data protection in the era of artificial intelligence.

***Keywords:*** *International law, artificial intelligence, privacy, emerging technologies, opportunities, and challenges.*

**How to cite this article:**

Naghibzakerin, Z., Shahabsafa, M., Mollahoseini Ardakani, M. R., Mirzaie, K., & Azimidokht Shooroki, S. A. (2025). Analysis of Legal Challenges and Data Protection Strategies in the Era of Artificial Intelligence in the International Legal System. *Interdisciplinary Studies in Society, Law, and Politics, 4*(2), 21-38. https://doi.org/10.61838/kman.isslp.4.2.3

## 1. Introduction

Ensuring and realizing the needs and demands of society within the framework of law has always been one of the fundamental objectives and key indicators of any legal and political system, both within national borders and in the international arena. This process of evolution has progressed toward perfection over time, alongside the advancement of human thought and the expansion of human needs. The trajectory began with the recognition of the first category of human rights, known as "civil and political rights," and progressed through the second category, encompassing "economic, social, and cultural rights," to the third category, referred to as "solidarity rights." However, in the present era, with the emergence of new technologies and their profound impact on the realization of human rights, prominent scholars such as Burns Weston and Norberto Bobbio argue that recognizing a fourth category of human rights, rooted in technology and associated with digital transformations, is essential and unavoidable. This new category of human rights, heavily influenced by technological advancements, requires a redefinition and the establishment of new legal structures capable of adapting to the challenges and opportunities of the technological age (Babazadeh Moghadam, 2020).

International law, in the domain of human rights, recognizes a list of fundamental rights and freedoms that are universally agreed upon by all states, international organizations, global instruments, international covenants, and customary international law. Consequently, this relatively new technological dimension has been acknowledged in authoritative international documents such as the "European Declaration on Digital Rights" and the "Digital Decade Policy Programme," both adopted by the European Commission. In Section 3 of the European Declaration on Digital Rights, titled "Freedom of Choice," it is emphasized that all individuals must be able to make informed decisions in the digital space, benefiting from artificial intelligence while remaining protected against potential threats and harms that could endanger their health, security, and fundamental rights. The simultaneous use of the terms "benefits" and "threats" in this document illustrates the reality that emerging technologies, including artificial intelligence, bring both advantages and risks. This contrast highlights the necessity of establishing well-defined legal and ethical frameworks to regulate the use of such technologies, ensuring that opportunities are maximized while potential harms are mitigated (Mostafavi Ardabili et al., 2022).

Existing studies have shown that artificial intelligence (AI) is a pervasive and impactful technology that transcends geographical boundaries and affects various generations of human rights. With the expansion of AI applications in areas such as data analysis, automated decision-making, and security systems, new challenges have emerged in relation to privacy, data security, and legal accountability. These challenges extend across multiple domains, including technical, ethical, and social aspects. Aldoseri et al. (2023) emphasize the importance of data quality and management, stating that AI systems require high-quality and large-scale datasets. However, challenges related to data quality, volume, and integration often pose significant issues for users. Therefore, ensuring data privacy and security, preventing bias and discrimination, and maintaining fairness are crucial for the effective deployment of AI (Aldoseri et al., 2023).

Similarly, Saghiri et al. (2022) highlight ethical and social concerns surrounding AI, discussing issues such as algorithmic bias, data protection, and potential job displacement due to automation. They argue that addressing these concerns requires a thorough examination and the development of ethical guidelines and legal frameworks (Saghiri et al., 2022). Additionally, Shaw et al. (2019) focus on the issue of explainability and transparency in AI, asserting that AI systems often function as "black boxes," making it difficult to understand their decision-making processes. This lack of transparency can undermine trust and accountability, necessitating the development of explainable AI models (Shaw et al., 2019).

With the advent and expansion of AI technologies, the protection of personal data has transcended national borders and become an international challenge. The cross-border nature of data, its processing by AI systems across different regions, and the lack of a coherent and harmonized international legal framework have created significant legal challenges in ensuring effective privacy protection. Existing research indicates that international law can play a vital role in establishing global standards, facilitating international cooperation, and defining legal responsibilities for data breaches. The findings of Voigt and Von dem Bussche (2017) demonstrate that the European Union’s General Data Protection Regulation (GDPR), as one of the most advanced laws in this field, has not only influenced EU member states but also served as a model for other countries in developing national data protection regulations (Voigt & Von dem Bussche, 2017). However, despite its significant role, GDPR still faces various technical and legal challenges. Consequently, examining these challenges—particularly in the field of international law, which has been largely overlooked in previous studies—holds particular importance.

The literature on data protection and artificial intelligence (AI) highlights significant legal challenges and regulatory gaps across different jurisdictions.

Studies in Indonesia (Ramadhan et al., 2024), Russia (Okishev, 2024), and China (Li, 2024) emphasize the urgent need for AI-specific regulations to safeguard personal data. These studies reveal that current national legal frameworks are insufficient to address the complexities of AI-driven data processing and call for greater legal certainty, regulatory oversight, and alignment with international standards. Similar concerns are echoed in Nigeria (Duch-Brown et al., 2017) and Ukraine (Bielova & Byelov, 2023), where research highlights insufficient transparency in AI systems, challenges in controlling automated decision-making, and risks of algorithmic discrimination. Notably, the Nigerian study stresses the importance of adaptive legal frameworks that balance innovation and privacy protection, while the Ukrainian study underscores threats such as unauthorized access, identity theft, and AI-driven data manipulation. The role of data anonymization and encryption as key countermeasures has also been emphasized in these studies. From a global governance perspective, the importance of international regulatory harmonization is reflected in research conducted in Germany (Poscher, 2021), the European Union (Hacker, 2018; Zuiderveen Borgesius, 2020), and the United Kingdom (Kingston, 2017). Poscher (2021) argues that instead of focusing on individual data processing, AI regulation should assess broader data processing systems to ensure greater accountability and transparency (Poscher, 2021). Zuiderveen Borgesius (2020) critically examines the shortcomings of EU laws in preventing algorithmic discrimination and proposes stronger enforcement mechanisms to protect individuals against AI-driven biases (Zuiderveen Borgesius, 2020). Hacker (2018) similarly explores the intersection of anti-discrimination laws and AI governance, advocating for algorithmic impact assessments to mitigate hidden biases in automated decision-making (Hacker, 2018). Kingston (2017) further investigates the role of rule-based AI models in ensuring compliance with GDPR, suggesting that such models provide greater explainability and auditability than machine-learning approaches (Kingston, 2017). Meanwhile, studies in China (An & Wang, 2021) and the EU emphasize the need for data-sharing models and encryption-based governance mechanisms to strengthen legal protections for AI and IoT applications. Additionally, research from Iran (Babazadeh Moghadam, 2020; Mostafavi Ardabili et al., 2022) highlights AI as part of the fourth generation of human rights, stressing the necessity of new international laws to address AI's ethical and legal challenges. Collectively, these studies suggest that the current legal frameworks are inadequate to address the evolving risks of AI, and global coordination, algorithmic transparency, and enforceable international regulations are essential for safeguarding data privacy and digital rights in the AI era.

Given the primary focus of this research, a fundamental question arises: From an international legal perspective, what are the main challenges and implications of personal data protection in the era of artificial intelligence? This study aims to answer this question by analyzing international data protection laws, identifying legal challenges associated with AI usage, and exploring possible solutions to address these challenges.

## 2. Review of Theoretical Foundations

### 2.1. *Artificial Intelligence and Its Types*

The term "Artificial Intelligence" was first introduced by John McCarthy in 1956 at the first academic conference dedicated to this subject. The ability of machines to think had been discussed even in earlier periods. In his report "As We May Think," Vannevar Bush predicted the development of a mechanical system designed to enhance human knowledge and understanding. In 1945, he wrote: *"Imagine a future device... in which an individual stores all books, records, and communications in such a way that it can be consulted quickly and flexibly due to its mechanized nature. This will serve as an efficient extension of the user's memory."* (Khoei, 2018).

From a logical standpoint, the foundation of artificial intelligence is rooted in logic itself. Logic was the first tool that natural intelligence created for itself. In the modern era, Vannevar Bush (1945) predicted the principle of machine thinking. A few years later, Alan Turing introduced the concept of simulating human behavior through chess-playing machines. Based on this perspective, artificial intelligence is viewed and defined through several key assumptions, among which the most significant are the following (Adiani, 2019):

1. Artificial intelligence is an advanced human technology. This technology is remarkably human-like, positioning artificial intelligence within a human framework. As a result, human

intelligence itself contains diverse and unexplored aspects.

2. Artificial intelligence is a superior branch of computer science, structured within intelligent robotic systems that study and design intelligent elements through systemic intelligent agents. It is derived from real intelligence and is fundamentally based on goal-oriented principles.
3. Artificial intelligence functions as a precise computational system with cognitive and memory capabilities. While this functionality differs from the human mind, it enables rational contemplation.
4. Artificial intelligence operates as a computational force based on sensor-driven simulations. It does not inherently exist as a fundamental principle but rather serves as a conceptual framework that helps explain real intelligence. Therefore, it symbolizes real intelligence, even though it cannot comprehensively capture all its features.
5. Artificial intelligence is a form of programmed language, based on logical reasoning, inference, and computation. It functions through algorithmic language and performs logical calculations.

Artificial intelligence is generally classified into three types:

- Narrow or Weak AI
- General or Strong AI
- Superintelligent AI

### 2.2. *Personal Data and Its Role in Artificial Intelligence*

According to Article 4, Paragraph 1 of the General Data Protection Regulation (GDPR) of the European Union, personal data is defined as: "any information relating to an identified or identifiable natural person." The same provision further clarifies that an identifiable person is one whose identity may not be directly apparent but can be determined through reference to specific identifiers (European Union, 2016).

Fundamentally, artificial intelligence is built upon technologies such as machine learning and deep neural networks, both of which require access to large volumes of high-quality, accurate data for optimal performance. Personal data serves as a critical component in the development of AI and the enhancement of its algorithmic efficiency. These data represent part of individuals' rights and obligations in the real world and, in some cases, their precise and ethical processing is necessary to ensure the protection of associated individuals' interests and to comply with ethical standards, preventing any potential harm (Hosseini, 2024). Consequently, legal systems must be capable of safeguarding individuals against the adverse consequences of AI on private information while ensuring that AI's technological progress and development are not obstructed.

In recent decades, countries such as the United States and China have significantly advanced their digital economies and AI sectors by adopting open data policies. The United States' digital economy vastly surpasses that of other nations, including the combined economies of European Union member states (Bureau of Economic Analysis, 2022). In response, the European Union has recently introduced laws such as the Open Data Directive and the Data Governance Act to facilitate European tech companies' access to data. However, some experts argue that one of the fundamental reasons for the EU's slower progress in this competitive global arena is its strict regulations, particularly those imposed by the GDPR, which restrict the free flow of data and secondary usage by European digital platforms (Ciriani et al., 2015).

### 2.3. *Types of Personal Data and Protection Methods*

Personal data in artificial intelligence encompasses various categories, with different protection approaches introduced to ensure that sensitive information is processed without revealing users' identities. The most significant types of personal data include:

1. Sensitive Personal Data: This includes medical records, genetic information, and real-time location data. Homomorphic encryption is used to process such data while keeping it encrypted, ensuring no exposure during computation. This technique allows mathematical operations on encrypted data without decryption (Lauter, 2021).
2. Shared Distributed Data: These data are distributed among multiple users or devices and often exist across multiple locations. Transferring such data to a centralized server

for processing poses security risks. Privacy-preserving methods such as federated learning combined with differential privacy are employed to prevent data exposure. Instead of sending raw data to a central server, only model updates are transmitted, or artificial noise is added to obscure sensitive details. The combination of these techniques provides an effective solution for protecting shared distributed data (Wei et al., 2019).

3. Synthetic Data Generation: Synthetic data are artificially generated using AI models like Generative Adversarial Networks (GANs) to preserve the statistical properties of real data while ensuring privacy protection. This method allows the use of artificially generated datasets instead of real data (Triastcyn & Faltings, 2018).
4. Private Data in Streaming Environments: In real-time streaming environments where data is continuously generated and processed, secure query and private processing techniques rely on advanced encryption methods (Stepanov, 2020).
5. Privacy-Preserving Learning under Covariate Shift: In cases where training data distributions differ from target data distributions, statistical adaptation techniques combined with differential privacy ensure secure processing and privacy protection (Sarpatwar et al., 2019).

### 2.4. *Legal Foundations of Data Protection and Privacy*

#### 2.4.1. *Privacy*

The right to privacy has been defined in Black's Law Dictionary as "the state or condition of being free from public attention to the degree that an individual's actions or decisions are not subject to interference or disturbance" (Garner, 2004). Another legal scholar has described privacy as "a right that protects individuals from unauthorized interference in their personal lives" (Landwehr et al., 2011).

A legal document published during the Conference of Jurists on Privacy in Norway (1976) defines privacy in Article 2 as "the right to solitude, living according to personal choices, and minimal interference from others." Additionally, this document states that privacy, as a civil right, includes protection against intrusions by third parties, unauthorized audio and video recordings, and unlawful surveillance of an individual's communications. According to Article 2 of the Privacy Bill, privacy is defined as: "A domain of an individual's life where, in accordance with legal principles and explicit personal consent, others are prohibited from accessing, monitoring, or interfering without authorization. This includes personal belongings, private residences, workplaces, personal data, and confidential interactions with others."

In Western philosophy, there are two main approaches to privacy: reductionism and essentialism. Reductionists deny the independent existence of privacy, whereas essentialists argue for its fundamental and intrinsic importance (Staples, 2007). Even among those who recognize privacy as an essential right, there is a debate between two perspectives: one considers privacy an absolute right, independent of external factors, while the other sees privacy as a conditional right, dependent on specific contextual limitations (Soroush, 2014).

Privacy discussions are analyzed from multiple perspectives:

1. As a negative right, implying that privacy delineates a space where government intervention is restricted.
2. As a positive right, where criminal policy mechanisms are examined to protect and enforce privacy.
3. As a legally regulated right, which acknowledges that certain legal mechanisms allow for the limitation of privacy under specific circumstances (Nekonam, 2024).

Privacy is recognized as a fundamental right in the Universal Declaration of Human Rights and numerous international treaties. In the European Union, privacy is protected under Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Bygrave, 1998).

#### 2.4.2. *Right to Data Ownership*

The rapid advancement of information technology and data analytics has led to an increased awareness of the economic value of data, transforming it into a new form of asset. Within the European Union, recognizing data as a legal subject is not a novel concept; rather, what has evolved is the definition of ownership itself. As data has become a vital resource in the digital economy, the legal framework surrounding property rights over data has gained significant importance (Attar & Parvin, 2021).

Studies indicate that none of the EU's data protection laws explicitly define data ownership. The concept remains ambiguous and contentious, often entangled with overlapping rights, responsibilities, and economic opportunities (European Commission, 2018). Typically, rights and obligations related to data are governed by intellectual property laws, data protection regulations, contract law, and competition law. This issue has both positive and negative aspects:

- From a positive perspective, data ownership facilitates commercialization and economic benefits through intellectual property and contract law.
- From a negative perspective, violations of contracts and intellectual property rights may result in damages and enforcement actions.

Current legal developments indicate that "data law" is emerging as a new legal domain (Kemp, 2014).

The concept of data ownership has sparked legal debates, attracting both supporters and opponents. From a legal standpoint, opponents argue that data's non-exclusive, reproducible, and shareable nature contradicts traditional concepts of ownership (Kemp, 2014). Additionally, they point to conflicts with privacy laws and data protection regulations, such as the right to data portability under the GDPR.

From an economic perspective, critics argue that establishing ownership rights over data lacks sufficient economic justification. They contend that such a framework could restrict data access, hinder innovation, and slow the development of new products and services. Economists further oppose data ownership rights, citing the low production cost of data in the digital economy and the potential increase in transaction costs and market inefficiencies (Stepanov, 2020).

Conversely, proponents of data ownership rights view its recognition as a step toward creating a comprehensive legal framework for data protection. From a legal standpoint, they argue that data ownership could function as a universal (erga omnes) right, safeguarding individuals from data misuse and enhancing legal certainty. Additionally, flexible ownership models, rather than absolute ownership, could provide a balanced solution (Purtova, 2011).

From an economic perspective, supporters claim that recognizing data ownership rights reduces uncertainty, promotes efficient resource allocation, and incentivizes investment in data production and processing (Duch-Brown et al., 2017). The "information paradox theory" (Kerber, 2016) further supports market expansion through data ownership rights, arguing that such rights would provide buyers with confidence that their data will not be misused or disclosed without consent.

### *2.5. International Laws and Regulations on Data Protection*

#### *2.5.1. General Data Protection Regulation (GDPR)*

The General Data Protection Regulation (GDPR) has been in effect across all European Union (EU) member states since 2018. The provisions of this regulation can be categorized into two main groups (Babazadeh Moghadam, 2020):

A. Obligations for Data Controllers and Processors – This category includes rules designed to monitor their activities and define their legal responsibilities.

B. Delegation Regulations for Data Subjects – These provisions establish legal rights for individuals, enabling them to exert direct control over data processing activities.

The first category is based on the principles outlined in Article 5 of the GDPR, which data controllers and processors must adhere to. Regulatory authorities responsible for data protection oversight are also required to monitor compliance automatically, regardless of whether a complaint has been filed regarding violations (Hosseini, 2024).

The second category consists of data subject rights, as specified in Articles 12–23 of the GDPR. These rights enable individuals to exercise control over how their personal data is processed by controllers and processors. The most significant rights include:

- Right of access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object to processing (European Union, 2016, p. 679).

### *2.5.2. International Instruments on Privacy and Data Protection*

International legal instruments related to privacy and data protection can be classified into two main groups:

First Group: General Human Rights Instruments on Privacy

These documents emphasize the necessity of privacy protection in broad terms. Key instruments include:

- Article 12 of the Universal Declaration of Human Rights (1948)
- Article 5 of the International Convention on the Elimination of All Forms of Racial Discrimination (1965)
- Article 17 of the International Covenant on Civil and Political Rights (1966)
- Article 18 of the International Human Rights Declaration (Tehran Declaration, 1968)
- Article 11 of the American Convention on Human Rights (1969)
- Article 9 of the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)
- Article 18 of the Cairo Declaration on Human Rights in Islam (1990)

All these instruments emphasize the protection of private life, family life, home, and correspondence, prohibiting arbitrary and unlawful interference by states.

Second Group: Specific Regulations on Electronic Communications and Data Privacy

Certain modern legal frameworks specifically address privacy in the digital and electronic communications era. Notable instruments include:

1. EU Data Protection Directive (1995) – Established a framework for regulating the processing of personal data within EU member states.
2. Directive on the Protection of Individuals Against Personal Data Processing and Free Data Movement (1995) – Required EU member states to ensure privacy protection in personal data processing.
3. ePrivacy Directive (2002) – Aimed at protecting electronic communication service providers (e.g., Internet Service Providers, ISPs) and preventing unauthorized data collection through surveillance, behavior analysis, and spying techniques. Article 6 mandated the deletion or anonymization of users' internet traffic data.
4. Data Retention Directive (2006) – Introduced 17 provisions modifying previous directives by specifying which types of data may be stored, storage duration, oversight responsibilities, and penalties for privacy violations.
5. United Nations Human Rights Declaration (2013, revised edition) – Recognized the protection of personal data privacy as a fundamental human right. This resolution emphasized that online communications should be protected, and national laws must prevent privacy violations while ensuring transparency in government surveillance of data transfers (Sharwood, 2013).
6. EU General Data Protection Regulation (GDPR) (2016) – On April 27, 2016, the European Parliament and the Council of the European Union adopted the GDPR, defining data protection as a fundamental right applicable regardless of nationality or residency.
7. Regulation on the Processing of Personal Data by EU Institutions (2018) – Established data protection rules for EU institutions and assigned responsibilities to the EU Data Protection Officer. Additionally, in May 2018, the EU adopted the Directive on Personal Data Protection in Criminal Matters, setting specific guidelines for law enforcement data processing.

The 2016 GDPR stands out among other EU and international privacy regulations due to its unified legal framework, innovative tools for maximum data protection, cross-border data protection measures, and specific provisions for sensitive personal data (Paal, 2022).

8. EU Artificial Intelligence Act (2024) – This law establishes a regulatory framework for the safe and ethical use of artificial intelligence. Key provisions include risk-based classification of AI systems and the prohibition of AI systems that pose a fundamental threat to human rights. The law also mandates transparency requirements for AI applications in service delivery.

### 2.5.3. *Data Protection and AI Regulations in Iran*

Iran has also implemented various laws and policies on data protection and artificial intelligence, with some of the latest initiatives outlined below:

1. National Artificial Intelligence Strategy of the Islamic Republic of Iran (2024) – Approved by the Supreme Council of the Cultural Revolution, this document aims to position Iran among the top 10 AI leaders globally by 2033. The strategy emphasizes the development of AI technology based on Islamic and indigenous values, focusing on human resource empowerment, infrastructure enhancement, and AI regulation in big data management and intellectual property. Additionally, the policy advocates for AI integration into sectors such as education, healthcare, industry, and governance (Laws & Regulations of the Country, 2024).
2. Draft Law on Data Protection and Privacy in Cyberspace (2018) – This draft law aims to create a comprehensive legal framework for data protection and online privacy. It defines key concepts such as "personal data," "sensitive data," and "informed consent" and establishes conditions for cross-border data transfers. However, this legislation has not yet been finalized (Mohiqi, 2023).
3. Citizens' Rights Charter (2016) – Recognizes citizens' rights to privacy and data protection. It guarantees individuals the right to know how their personal data is collected, used, and stored and provides legal recourse in cases of data breaches.
4. Freedom of Information Act (2009) – This law promotes government transparency while ensuring data protection. It mandates public institutions to disclose non-private information while safeguarding personal privacy.

## 3. Methodology

This study is applied in terms of its objective and qualitative in terms of its methodological approach. It employs the grounded theory method in an analytical-descriptive manner. This method enables an in-depth examination of phenomena within their real-world context and facilitates the development of a conceptual framework.

Data collection was conducted through two methods: (1) library research (using note-taking tools) and (2) survey research (through semi-structured interviews). The primary research questions in this study revolve around identifying contextual conditions, causal conditions, intervening conditions, the central phenomenon, consequences, and strategies for data protection in the era of artificial intelligence within the framework of international law.

The statistical population of this study consisted of two main groups:

1. Managers and experienced professionals working at various operational, middle, and senior levels in leading computer and AI companies.
2. University faculty members with expertise in computer science and artificial intelligence.

Participants were selected through purposive and random sampling.

The research process was structured as follows: After extensive literature review and consultations with experts, the final interview questions were designed and the interview process commenced. Data collection continued until theoretical saturation was reached, which occurred after interviewing 14 participants.

To design the interview questions, the researcher first examined theoretical frameworks and literature and then formulated the questions based on these studies. Participants were allowed to discuss details relevant to the research topic based on their professional and academic experiences. Each interview lasted between 25 and 45 minutes, depending on the participant’s willingness to elaborate.

For recording the interviews, the researcher used a mobile device. Each interview was then transcribed verbatim and saved as a Word file on a computer. The data were subsequently entered into MAXQDA (version 12) for analysis.

Data analysis followed Strauss and Corbin’s (1998) grounded theory approach, which consists of three coding phases:

1. Open Coding – In this phase, the researcher identifies key concepts emerging from raw data and categorizes them based on their

characteristics and dimensions. The initial categories are extracted through open coding.

2. Axial Coding – At this stage, the connections between categories become more abstract and systematic (Farastkhah, 2010).
3. Selective Coding – In this final stage, all aspects of the data are examined simultaneously, and the core category that unites the data around a central concept is identified.

The Strauss-Corbin grounded theory approach is fundamentally inductive, meaning that instead of testing existing theories, the researcher constructs a new theory based on empirical findings.

4. Ensuring Validity and Reliability

To enhance research validity and reliability, several strategies were employed, including:

- Participant review (allowing participants to verify the accuracy of their responses).
- Independent coding by multiple researchers to ensure consistency.
- Thorough documentation of the research process to maintain transparency.

Additionally, ethical considerations were strictly observed, including:

- Obtaining informed consent from participants.
- Ensuring confidentiality of all data.
- Allowing participants to withdraw from the study at any stage.

This research methodology enabled the researcher to attain a deep and comprehensive understanding of the key components of data protection in artificial intelligence applications from an international law perspective.

## 4. Findings

Descriptive statistics of the interviewees indicated that 28.5% of the sample were women (4 individuals) and 71.5% were men (10 individuals). The mean age of the sample was 41.5 years, with ages ranging from 29 to 61 years. In terms of education, 21.5% held a bachelor's degree while the remainder possessed doctoral degrees. The average work experience of the sample was 15.5 years, with the maximum being 29 years and the minimum 9 years.

After conducting the interviews and collecting the data, the analysis was performed based on Strauss and Corbin’s (1998) method—which includes open coding, axial coding, and selective coding. In the first phase (open coding), the results were presented by differentiating among causal conditions, contextual conditions, intervening conditions, the central phenomenon, as well as strategies and consequences, with their respective codes, concepts, and categories, as described below.

### *4.1. Causal Conditions*

Causal conditions refer to the events and circumstances that affect the phenomenon of personal data protection when using artificial intelligence and serve as the primary context leading to it; they are temporally prior to data protection. Respondents described the phenomenon of personal data protection from a legal perspective, particularly with regard to international law. From their statements, initial codes were extracted. Later, common and emphasized codes were identified as final codes:

**Table 1**

*Identified Categories and Concepts Related to Causal Conditions*

| Main Category | Concept | Final Codes |
|---|---|---|
| Causal Conditions | Lack of Awareness of International Privacy Rights | - Unfamiliarity with relevant international instruments<br>- Lack of alignment between domestic laws and international standards<br>- Inadequate understanding of the transnational nature of data and its related rights<br>- Insufficient education and awareness regarding international privacy rights among users |
| | Weakness of International Oversight Mechanisms | - Insufficient international institutions with adequate enforcement power<br>- Lack of effective cooperation among countries in terms of information exchange and monitoring violations<br>- Absence of unified standards for evaluating and supervising the performance of cross-border companies in data protection |

| | | |
|---|---|---|
| | | - Lack of effective mechanisms for enforcing judicial rulings and decisions regarding privacy violations at the international level |
| | The Transnational Nature of Data in Cyberspace | - Problems in determining judicial jurisdiction<br>- Lack of unified international laws regarding data |
| | Rapid Technological Advancement and the Incongruence of International Law | - Failure to anticipate AI challenges in international instruments<br>- Need for the formulation of new international conventions |

### 4.2. *Contextual Conditions*

Contextual conditions refer to components that influence the intensity of the causal conditions. These conditions naturally and unexpectedly emerge and also serve to clarify the situation. Respondents provided explanations and examples regarding the contextual conditions of personal data protection. After refinement, the most important codes became the final codes for contextual conditions.

**Table 2**

*Identified Categories and Concepts Related to Contextual Conditions*

| Main Category | Concept | Final Codes |
|---|---|---|
| Contextual Conditions | Cultural and Legal Differences Between Countries | - Differences in the definition of privacy<br>- Variations in the importance placed on data protection |
| | Economic and Political Interests of States | - Competition among countries in the field of technology<br>- Prioritization of national interests over international cooperation<br>- Instrumental use of data for political and security purposes by governments |
| | Lack of Global Consensus on Ethical Principles of AI | - Different interpretations of ethics in the use of artificial intelligence<br>- Absence of international ethical standards for artificial intelligence |
| | Influence of Major Powers and International Organizations | - Role of the United Nations and its affiliated bodies<br>- Influence of major powers in the formulation and enforcement of international laws<br>- Efforts by major powers to impose their standards on data protection on other countries |

### 4.3. *Intervening Conditions*

Intervening conditions are stable patterns intertwined with specific times and locations that create circumstances in which individuals and organizations respond. These factors can sustain and intensify the phenomenon. After final refinement, the main concepts and significant final codes related to intervening conditions are presented as follows:

**Table 3**

*Identified Categories and Concepts Related to Intervening Conditions*

| Main Category | Concept | Final Codes |
|---|---|---|
| Intervening Conditions | Actions of International Organizations | - Formulation of new international documents and conventions<br>- Establishment of international oversight institutions |
| | International Cooperation Among States | - Exchange of information and experiences<br>- Conclusion of bilateral and multilateral treaties |
| | Role of International Non-Governmental Organizations | - Support for human rights in cyberspace<br>- Oversight of the performance of governments and companies at the international level |
| | Dominant Paradigms in Technology and Data Policy-Making | - The "data as an economic resource" paradigm and its impact on policy-making<br>- Predominance of "national security" approaches over privacy protection in some countries<br>- Influence of a "culture of trust in technology" and acceptance of associated risks<br>- Shift from a "preventive protection" paradigm to a "reactive response" following data breaches |

### 4.4. *Central Category and Phenomenon*

Causal conditions give rise to the central category (phenomenon), which may have multiple dimensions and sub-concepts. Based on respondents' answers, the final concepts and codes for the central phenomenon are presented. According to the interviewees, despite the technical and operational measures employed for data protection, the primary legal phenomenon in this field is the inefficiency of the existing international legal system in addressing the challenges of data protection in the era of artificial intelligence. This inefficiency is divided into structural and conceptual challenges.

**Table 4**

*Identified Categories and Concepts Related to the Central Category*

| Main Category | Concept | Final Codes |
|---|---|---|
| Inefficiency of the Existing International Legal System in Addressing the Challenges of Data Protection in the Era of Artificial Intelligence | Structural Challenges of the International Legal System | - Insufficient coverage of AI-specific challenges in existing international instruments<br>- Difficulties in enforcing national laws regarding data processed by AI systems at the international level<br>- Lack of effective mechanisms for international cooperation in investigating and pursuing crimes related to AI and data<br>- Issues in delineating responsibility and accountability for privacy violations |
| | Conceptual and Operational Challenges Related to Artificial Intelligence | - Ambiguity in determining legal liability for data breaches by AI systems<br>- Need to define new legal concepts suited to the characteristics of artificial intelligence (e.g., "legal personality of AI") |

### 4.5. *Strategies and Actions*

Respondents provided detailed explanations regarding strategies and actions for protecting personal data in the era of artificial intelligence within the framework of international law. During data analysis, final concepts and codes were extracted through first-level coding.

**Table 5**

*Identified Categories and Concepts Related to Strategies and Actions*

| Main Category | Concept | Final Codes |
|---|---|---|
| Strategies and Actions | Development of a Comprehensive International Legal Framework | - Preparation of binding international conventions in the field of data protection and artificial intelligence<br>- Establishment of international standards for data processing with a focus on privacy principles<br>- Formulation of international protocols for information exchange and judicial cooperation concerning cybercrimes related to data and AI<br>- Establishment of an independent international body to oversee the implementation of data protection laws and standards globally |
| | Strengthening International Cooperation | - Creation of formal and effective mechanisms for information exchange and judicial cooperation among countries<br>- Formation of international working groups to examine legal challenges arising from artificial intelligence and provide uniform solutions for all countries<br>- Support for capacity building in developing countries for the implementation of international data protection standards<br>- Encouragement to conclude bilateral and multilateral treaties concerning data protection and cooperation in combating cybercrimes |
| | Development of National and International Capacities | - Training legal, technical, and judicial experts in international law related to data and artificial intelligence<br>- Enhancing public awareness regarding international privacy rights through educational and media programs |

| | | |
|---|---|---|
| | | - Supporting scientific research on the legal and ethical challenges of artificial intelligence and data protection |
| | | - Establishing programs for knowledge and experience exchange between countries on best practices for data protection |
| | Establishment of International Accountability Mechanisms | - Precise determination of the legal responsibilities of governments, technology companies, and AI developers for data breaches |
| | | - Creation of effective mechanisms for compensating victims of privacy violations at the international level |
| | | - Formulation of international ethical principles for the development and use of AI with an emphasis on data protection |
| | | - Establishment of an international court or arbitration body to resolve disputes related to data protection globally |

### 4.6. *Consequences*

Analysis of the interviews and respondents' opinions revealed very positive consequences. These outcomes include increased employee satisfaction due to perceived justice, enhanced participation in managerial processes, transparency in management, and adherence to national standards—all of which may indicate effective human resource development and the appointment of political and administrative managers at both internal and external organizational levels.

**Table 6**

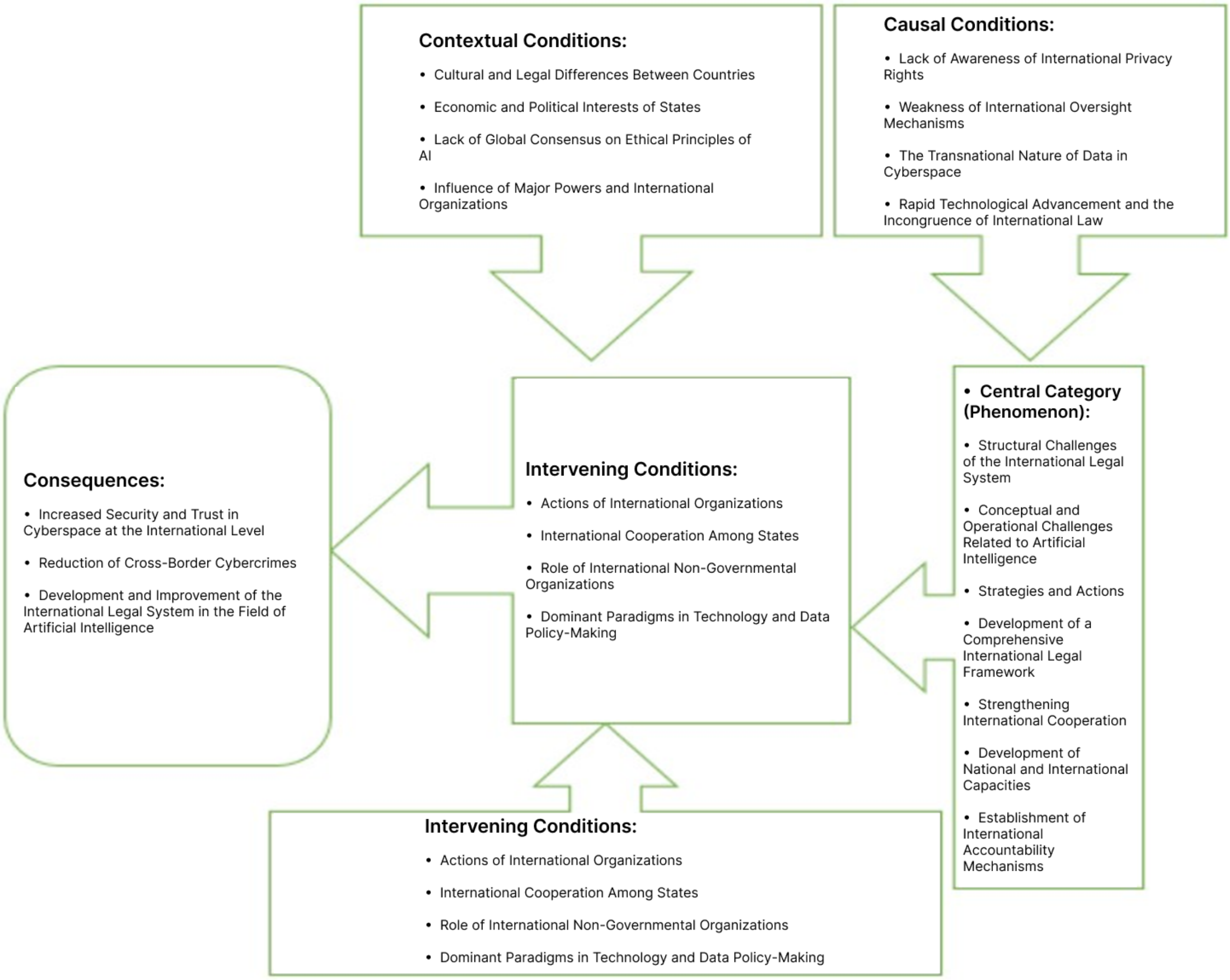
*Identified Categories and Concepts Related to Consequences*

| Main Category | Concept | Final Codes |
|---|---|---|
| Consequences | Increased Security and Trust in Cyberspace at the International Level | - Effective protection of personal data globally and enhanced user control over their own data |
| | | - Reduction in instances of privacy violations and data misuse |
| | | - Increased user trust in AI technologies and online services, facilitating the utilization of these technologies' benefits |
| | | - Development of the digital economy and cross-border e-commerce through a secure and reliable environment |
| | | - Strengthening international cooperation in cybersecurity and information exchange |
| | Reduction of Cross-Border Cybercrimes | - More effective countermeasures against crimes related to data and AI through international cooperation and harmonized laws |
| | | - Reduction of financial and non-financial damages resulting from cybercrimes |
| | | - Prevention of the use of AI for criminal purposes |
| | | - Increased deterrence against cybercrimes via effective penalties at the international level |
| | | - Improved processes for identifying, tracking, and apprehending cross-border cybercriminals |
| | Development and Improvement of the International Legal System in the Field of Artificial Intelligence | - Establishment of a unified and coordinated legal framework at the international level for data protection and artificial intelligence |
| | | - Advancement of international law in light of new challenges arising from AI and creation of legal transparency |
| | | - Development of a more up-to-date legal framework for the ethical development and use of AI |
| | | - Strengthening the role of international organizations in the formulation and enforcement of laws and standards |
| | | - Creation of an appropriate platform for resolving legal disputes related to data protection and AI at the international level |

With the dimensions and components identified during open coding, the next phase (axial coding) involved preparing a paradigm model that illustrates the relationships among causal conditions, the central phenomenon, strategies, intervening conditions, contextual conditions, and consequences. In other words, the main and sub-categories are interrelated through a paradigm model.

**Figure 1**

*Paradigm Model of Data Protection in the Era of Artificial Intelligence from the Perspective of International Law*



Contextual Conditions:

- Cultural and Legal Differences Between Countries
- Economic and Political Interests of States
- Lack of Global Consensus on Ethical Principles of AI
- Influence of Major Powers and International Organizations

Causal Conditions:

- Lack of Awareness of International Privacy Rights
- Weakness of International Oversight Mechanisms
- The Transnational Nature of Data in Cyberspace
- Rapid Technological Advancement and the Incongruence of International Law

Consequences:

- Increased Security and Trust in Cyberspace at the International Level
- Reduction of Cross-Border Cybercrimes
- Development and Improvement of the International Legal System in the Field of Artificial Intelligence

Intervening Conditions:

- Actions of International Organizations
- International Cooperation Among States
- Role of International Non-Governmental Organizations
- Dominant Paradigms in Technology and Data Policy-Making

- Central Category (Phenomenon):

- Structural Challenges of the International Legal System
- Conceptual and Operational Challenges Related to Artificial Intelligence
- Strategies and Actions
- Development of a Comprehensive International Legal Framework
- Strengthening International Cooperation
- Development of National and International Capacities
- Establishment of International Accountability Mechanisms

Intervening Conditions:

- Actions of International Organizations
- International Cooperation Among States
- Role of International Non-Governmental Organizations
- Dominant Paradigms in Technology and Data Policy-Making

The model derived from the interview analysis indicates six main dimensions. In this model, the causal conditions serve as the motivating and enabling factors (or conditions that set the stage) for protecting personal data in the era of artificial intelligence. These factors—which include lack of awareness of international privacy rights; weakness of international oversight mechanisms; the transnational nature of data in cyberspace; and rapid technological advancement coupled with the incongruence of international law—exert both temporal and conditional influence on the central phenomenon.

Contextual conditions (or clarifying factors) indicate the important underlying factors that affect the protection of private data in the intelligent era. Cultural and legal differences between countries, economic and political interests of states, the lack of global consensus on the ethical principles of artificial intelligence, and the influence of major powers and international organizations are key elements that must be addressed.

Unlike contextual conditions, intervening conditions are those factors that influence the selection of mechanisms for protecting personal data and can facilitate and expedite their implementation. These include the actions of international organizations, international cooperation among states, the role of international non-governmental organizations, and dominant paradigms in technology and data policy-making.

Examination of the primary consequences identified the inefficiency of the existing international legal system in addressing the challenges of data protection in the era of artificial intelligence as the central issue. The components influencing this inefficiency—the structural and conceptual challenges of the international legal system related to AI—must be taken into account.

In the domain of strategies and actions, the primary interventions and activities that can resolve the main issue (i.e., the inefficiency of the existing international legal system) are discussed. Unlike the central phenomenon, the concepts and categories in this domain are action-oriented, focusing on measures that can improve the overall process.

Finally, in the domain of consequences, the expected outcomes from the recommended actions are discussed. These include increased international security and trust in cyberspace, reduction in cross-border cybercrimes, and ultimately the development and improvement of the international legal system in the field of artificial intelligence. Such outcomes may benefit societies that are rapidly adopting artificial intelligence and new technologies.

In the final phase—selective coding—the researcher developed a theory regarding the relationships among the categories extracted during axial coding. At a macro level, this theory provides an abstract explanation of the process under study. In qualitative research based on grounded theory, the results may culminate in propositions (or "claims," as termed by Strauss and Corbin, 1998) that specify the interrelationships among the categories.

At this stage, the decisive propositions or claims governing the internal relationships among the categories are formulated as follows:

**Hypothesis 1:**

Lack of awareness of international privacy rights (i.e., unfamiliarity with relevant international instruments, lack of alignment between domestic laws and international standards, inadequate understanding of the transnational nature of data and its related rights, and insufficient education and awareness regarding international privacy rights among users); weakness of international oversight mechanisms (i.e., insufficient international institutions with adequate enforcement power, lack of effective cooperation among countries in terms of information exchange and monitoring violations, absence of unified standards for evaluating and supervising the performance of cross-border companies in data protection, and lack of effective mechanisms for enforcing judicial rulings and decisions regarding privacy violations at the international level); the transnational nature of data in cyberspace (i.e., issues in determining judicial jurisdiction, lack of unified international laws regarding data); and rapid technological advancement coupled with the incongruence of international law (i.e., failure to anticipate AI challenges in international instruments and the need for formulating new international conventions) are considered the causal conditions for the inefficiency of the existing international legal system in addressing the challenges of data protection in the era of artificial intelligence.

**Hypothesis 2:**

The central phenomenon—namely, the inefficiency of the existing international legal system in addressing the challenges of data protection in the era of artificial intelligence—is divided into two categories:

- **Structural challenges of the international legal system:** (i.e., insufficient coverage of AI-specific challenges in existing international instruments, difficulties in enforcing national laws regarding data processed by AI systems at the international level, lack of effective mechanisms for international cooperation in investigating and pursuing crimes related to AI and data, and issues in delineating responsibility and accountability for privacy violations)
- **Conceptual challenges of the international legal system:** (i.e., ambiguity in determining legal liability for data breaches by AI systems and the need to define new legal concepts suited to the characteristics of artificial intelligence, such as "legal personality of AI")

These categories constitute the central phenomenon.

**Hypothesis 3:**

Contextual conditions, including cultural and legal differences between countries (i.e., differences in the definition of privacy and variations in the importance placed on data protection); economic and political interests of states (i.e., competition among countries in technology, prioritization of national interests over international cooperation, and instrumental use of data for political and security purposes by governments); the lack of global consensus on the ethical principles of artificial intelligence (i.e., differing interpretations of ethics in the use of AI and the absence of international ethical standards for AI); and the influence of major powers and international organizations (i.e., the role of the United Nations and its affiliated bodies, the influence of major powers in formulating and enforcing international laws, and efforts by major powers to impose their standards on data protection on other countries) create a specific context for the development and appointment of administrative and political managers.

**Hypothesis 4:**

Intervening conditions, including actions of international organizations (i.e., formulation of new international documents and conventions and establishment of international oversight institutions); international cooperation among states (i.e., exchange of information and experiences, and conclusion of bilateral and multilateral treaties); the role of international non-governmental organizations (i.e., support for human rights in cyberspace and oversight of the performance of governments and companies at the international level); and dominant paradigms in technology and data policy-making (i.e., the "data as an economic resource" paradigm and its impact on policy-making, the predominance of "national security" approaches over privacy protection in some countries, the influence of a "culture of trust in technology" and acceptance of associated risks, and the shift from a "preventive protection" paradigm to a "reactive response" following data breaches) together create a general foundation and infrastructure for the protection of personal data in the era of artificial intelligence.

**Hypothesis 5:**

Actions such as the development of a comprehensive international legal framework (i.e., preparation of binding international conventions in the field of data protection and artificial intelligence, establishment of international standards for data processing with a focus on privacy principles, formulation of international protocols for information exchange and judicial cooperation concerning cybercrimes related to data and AI, and establishment of an independent international body to oversee the implementation of data protection laws and standards globally); strengthening international cooperation (i.e., creation of formal and effective mechanisms for information exchange and judicial cooperation among countries, formation of international working groups to examine legal challenges arising from AI and provide uniform solutions for all countries, support for capacity building in developing countries for implementing international data protection standards, and encouragement to conclude bilateral and multilateral treaties concerning data protection and cooperation in combating cybercrimes); and development of national and international capacities (i.e., training legal, technical, and judicial experts in international law related to data and AI, enhancing public awareness regarding international privacy rights through educational and media programs, supporting scientific research on the legal and ethical challenges of AI and data protection, and establishing programs for knowledge and experience exchange between countries on best practices for data protection) constitute the primary and significant strategies for protecting personal data in the era of artificial intelligence.

## 5. Discussion and Conclusion

This study aimed to identify the challenges of international law in protecting personal data in the era of artificial intelligence (AI). Accordingly, we sought to examine the theoretical foundations related to this topic while addressing the main research question. The results, derived from a qualitative study using grounded theory (Strauss & Corbin, 1998), confirm that the inefficiency of the existing international legal system in confronting the challenges of data protection in the AI era is the central phenomenon. This inefficiency manifests in two main categories:

1. Structural challenges of the international legal system.
2. Conceptual and operational challenges related to artificial intelligence.

Regarding structural challenges, the findings indicate that existing international legal instruments have not adequately addressed AI-specific challenges, creating a significant legal vacuum at the global level. Additionally, difficulties in enforcing national laws concerning data processed by AI systems at an international scale and the lack of effective mechanisms for international cooperation in investigations and prosecution of AI and data-related crimes have been identified as key structural challenges. These findings align directly with recent studies conducted in various countries. For instance, research in Indonesia (Ramadhan et al., 2024), Russia (Okishev, 2024), and China (Li, 2024) underscores the need for more comprehensive and transparent legislation for protecting personal data in AI governance. These studies, similar to the present research, highlight the importance of legal certainty, regulatory oversight, and the harmonization of national laws with international standards.

Regarding conceptual and operational challenges, the findings emphasize ambiguities in determining legal responsibility for data breaches by AI systems and the necessity of defining new legal concepts compatible with the nature of AI technology, such as “legal personality of AI.” These findings align with current legal debates on AI accountability and the need for new legal frameworks for AI governance. Research in Nigeria and Ukraine (Bielova & Byelov, 2023) also addresses issues such as insufficient transparency in AI systems, complexity in controlling automated decision-making, algorithmic discrimination, and the inadequacy of data anonymization. These concerns overlap significantly with the conceptual and operational challenges identified in this study.

Furthermore, the findings reveal that various causal conditions contribute to this inefficiency, including lack of awareness of international privacy rights, weak international oversight mechanisms, challenges stemming from the transnational nature of data, and the rapid advancement of technology without corresponding updates in international law. Additionally, contextual conditions such as cultural and legal differences between countries, economic and political interests of governments, the absence of global consensus on AI ethics, and the influence of major powers and international organizations exacerbate this inefficiency. Intervening conditions, including dominant paradigms in technology and data policy-making, further act as sustaining and intensifying factors in this situation. These findings are consistent with research emphasizing the role of social, cultural, economic, and political factors in shaping laws and policies related to technology and data governance. Specifically, the focus on the influence of major powers in imposing their standards aligns with studies on the geopolitics of data and technology.

Finally, this research proposes strategies to address these challenges, including:

- Developing a comprehensive international legal framework.
- Enhancing international cooperation.
- Expanding national and international capacities.
- Establishing international accountability mechanisms.

Implementing these strategies can yield positive outcomes such as increased security and trust in cyberspace at the international level, reduced cross-border cybercrimes, and the advancement of the international legal system in the field of AI governance. These strategies align with recommendations in global data governance and AI regulation studies conducted in China (An & Wang, 2021), Germany (Poscher, 2021), and the European Union (Hacker, 2018; Zuiderveen Borgesius, 2020). Notably, the emphasis on increasing transparency in AI systems and addressing algorithmic discrimination, which has been a focal point in these studies, is also reflected in the proposed strategies of this research.

Additionally, the findings of this study align with domestic research (Babazadeh Moghadam, 2020; Mostafavi Ardabili et al., 2022), which highlights the need for international legal frameworks for privacy protection in the AI era. These studies also stress the importance of strengthening international participatory processes, establishing working groups and international commissions, and promoting investment in AI-affected sectors.

## Authors’ Contributions

Authors contributed equally to this article.

## Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

## Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

## Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

## Declaration of Interest

The authors report no conflict of interest.

**Funding**

According to the authors, this article has no financial support.

**Ethical Considerations**

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

## References

Adiani, S. Y. (2019). *Rational Reflections on Artificial Intelligence*. Islamic Consultative Assembly Research Center, Political-Legal Research Department, Fundamental Government Studies.

Aldoseri, A., Al-Khalifa, K., & Hamouda, A. (2023). Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges. *Applied Sciences*. https://doi.org/10.3390/app13127082

An, N., & Wang, X. (2021). Legal protection of artificial intelligence data and algorithms from the perspective of internet of things resource sharing. *Wireless Communications and Mobile Computing*, *2021*, 8601425. https://doi.org/10.1155/2021/8601425

Attar, S., & Parvin, F. (2021). European Union Law and the Challenge of Recognizing the Right to Property in Data in the Digital Economy. *International Law Journal*, *38*(65), 281-304. https://doi.org/10.22066/cilamag.2021.245186

Babazadeh Moghadam, H. (2020). *An Introduction to the Fourth Generation of Human Rights: Protecting Human Dignity in the Age of Communication* (Vol. 34). News Sciences.

Bielova, M., & Byelov, D. (2023). Challenges and threats of personal data protection in working with artificial intelligence. *Uzhhorod National University Herald. Series: Law*.

Bureau of Economic Analysis. (2022). *New and Revised Statistics of the U.S. Digital Economy*.

Bygrave, L. (1998). Data protection pursuant to the right to privacy in human rights treaties. *Int. J. Law Inf. Technol.*, *6*, 247-284. https://doi.org/10.1093/IJLIT/6.3.247

Ciriani, S., Drexl, J., Hilty, R., Desaunettes-Barbero, L., Greiner, F., Kim, D., Richter, H., Surblyte, G., & Wiedemann, K. (2015). The Economic Impact of the European Reform of Data Protection Data Ownership and Access to Data. *COMMUNICATIONS & STRATEGIES*, *97*. https://doi.org/10.2139/ssrn.2833165

Duch-Brown, N., Martens, B., & Mueller-Langer, F. (2017). *The Economics of Ownership, Access and Trade in Digital Data*.

European Commission. (2018). *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*.

European Union. (2016). General Data Protection Regulation.

Farastkhah, M. (2010). *Qualitative Research Method in Social Sciences with Emphasis on "Grounded Theory"*. Agah Publications.

Garner, B. A. (2004). *Black's Law Dictionary*. Thomson West.

Hacker, P. (2018). Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*.

Hosseini, S. A. (2024). The Right to Protection of Personal Data in Algorithmic Processing, Challenges, and Solutions. *Quarterly Journal of Law and Government*, *5*(1), 99-122.

Kemp, R. (2014). Legal Aspects of Managing Data. *Kemp It Law*. https://doi.org/10.1016/j.clsr.2014.07.006

Kerber, W. (2016). A New (Intellectual) Property Right for Nonpersonal Data? *MAGKS Joint Discussion Paper Series in Economics*, *37-2016*.

Khoei, S. M. (2018). *Artificial Intelligence and Legislative Research in Artificial Intelligence and Legislation*. Islamic Consultative Assembly Research Center, Fundamental Government Studies Department.

Kingston, J. K. C. (2017). Using artificial intelligence to support compliance with the General Data Protection Regulation. *Artificial Intelligence and Law*, *25*, 429-443. https://doi.org/10.1007/s10506-017-9206-9

Landwehr, C. E., Heitmeyer, C. L., & McLean, J. (2011). A security model for military message systems: Retrospective. *Naval Research Laboratory Washington DC*.

Lauter, K. (2021). Private AI: Machine Learning on Encrypted Data. *IACR Cryptol. ePrint Arch.*, *2021*, 324.

Laws, N. I. C. f., & Regulations of the Country. (2024). *National Document on Artificial Intelligence*.

Li, F. (2024). Research on the legal protection of user data privacy in the era of artificial intelligence. *Science of Law Journal*.

Mohiqi, M. M. (2023). Personal Data Protection in the Iranian Legal System. *Journal of Politics and Law*, *16*(3), 10-20. https://doi.org/10.5539/jpl.v16n3p10

Mostafavi Ardabili, S. M. M., Taghizadeh Ansari, M., & Rahmati Far, S. (2022). Functions and Requirements of Artificial Intelligence from the Perspective of Fair Trial. *New Technologies Law*, *3*(6), 47-60.

Nekonam, V. (2024). Requirements for Investigating the Privacy of Communicative and Informative Data in Cyberspace. *New Technologies Law*, *5*(9), 27-40.

Okishev, B. A. (2024). Features of the legal protection of personal data processed using artificial intelligence technologies. *Economic Problems and Legal Practice*. https://doi.org/10.33693/2541-8025-2024-20-2-70-75

Paal, B. P. (2022). Artificial Intelligence as a Challenge for Data Protection Law: And Vice Versa. In *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives*. Cambridge Law Handbooks. https://doi.org/10.1017/9781009207898.023

Poscher, R. (2021). Artificial intelligence and the right to data protection. https://doi.org/10.2139/ssrn.3769159

Purtova, N. (2011). *Property Rights in Personal Data: A European Perspective*. Kluwer Law International.

Ramadhan, M. H. R., Ramadhani, K., Isrok, M., Anggraeny, I., & Prasetyo, R. (2024). Legal protection of personal data in artificial intelligence for legal protection viewed from legal certainty aspect. *Kne Social Sciences*.

Saghiri, A., Vahidipour, S., Jabbarpour, M., Sookhak, M., & Forestiero, A. (2022). A Survey of Artificial Intelligence Challenges: Analyzing the Definitions, Relationships, and Evolutions. *Applied Sciences*. https://doi.org/10.3390/app12084054

Sarpatwar, K., Shanmugam, K., Ganapavarapu, V., Jagmohan, A., & Vaculín, R. (2019). Differentially Private Distributed Data Summarization under Covariate Shift. *ArXiv*, *abs/1910.12832*.

Sharwood, S. (2013). United Nations Signs Off on 'right to Privacy in the Digital age".

Shaw, J., Rudzicz, F., Jamieson, T., & Goldfarb, A. (2019). Artificial Intelligence and the Implementation Challenge. *Journal of medical Internet research*, *21*. https://doi.org/10.2196/13659

Soroush, M. (2014). *The Foundations of Privacy*. Samt Publications.

Staples, W. G. (2007). *Encyclopedia of Privacy*. Greenwood Press. https://doi.org/10.5040/9798216001393

Stepanov, I. (2020). Introducing a Property Right over Data in the EU: the Data Producer's Right - an Evaluation. *International Review of Law, Computers & Technology*, *34*(1). https://doi.org/10.1080/13600869.2019.1631621

Triastcyn, A., & Faltings, B. (2018). Generating Artificial Data for Private Deep Learning. *arXiv: Learning*.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Wei, K., Li, J., Ding, M., Yang, H., Farhad, F., Jin, S., Quek, T., & Poor, H. (2019). Federated Learning With Differential Privacy: Algorithms and Performance Analysis. *Ieee Transactions on Information Forensics and Security*, *15*, 3454-3469. https://doi.org/10.1109/TIFS.2020.2988575

Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, *24*, 1572-1593. https://doi.org/10.1080/13642987.2020.1743976