International Journal Publishing
INFLUENCE: International Journal of Science Review
Volume 8, No. 3, 2026
https://influence-journal.com/index.php/influence/index

The Role of Artificial Intelligence in Shaping Privacy Laws: A Comparative Analysis of Global Regulatory Frameworks

Any Farida
Universitas Darul Ulum Islamic Centre Sudirman, Semarang, Indonesia
Email: anyfarida@undaris.ac.id

Abstract. The rapid advancement of Artificial Intelligence has significantly transformed the processing and utilization of personal data, creating increasingly complex privacy challenges that extend beyond the scope of conventional data protection frameworks. Existing privacy laws in many jurisdictions have struggled to keep pace with the evolving capabilities of AI technologies, particularly regarding automated decision-making, algorithmic processing, cross-border data transfers, and large-scale data analytics. These developments have prompted governments and international organizations to reform legal frameworks in order to establish effective AI governance while maintaining the protection of fundamental rights and supporting technological innovation. This study aims to comparatively analyze privacy law frameworks governing Artificial Intelligence across major jurisdictions and to examine the regulatory gaps and future directions for AI-oriented privacy law reform. This research employs normative legal research using statutory, comparative, and conceptual approaches by analyzing international legal instruments, national legislation, and relevant scholarly literature concerning privacy protection and Artificial Intelligence governance. The findings demonstrate that the European Union, the United States, China, and Indonesia have adopted distinct regulatory approaches reflecting different legal traditions, governance priorities, and policy objectives, resulting in varying levels of protection, accountability, enforcement, and AI oversight. The study further identifies fragmented regulations, jurisdictional conflicts, cross-border data transfer issues, algorithmic accountability, transparency concerns, and enforcement limitations as the principal legal challenges that continue to hinder the effectiveness of global AI governance. Accordingly, future privacy law reform should prioritize adaptive and risk-based regulation, strengthen international regulatory harmonization, integrate privacy by design and human oversight into AI governance, and promote global cooperation to establish a balanced legal framework capable of safeguarding privacy while supporting responsible Artificial Intelligence innovation.

Keywords: *Artificial Intelligence, Privacy Law, AI Governance, Data Protection, Comparative Law.*

A. INTRODUCTION

The advancement of Artificial Intelligence (AI) technology has brought about significant changes in how personal data is collected, processed, analyzed, and utilized across social, economic, governmental, and public service activities. Virtually all sectors now rely on AI-driven systems to enhance operational efficiency, accelerate decision-making, and deliver more personalized services. The use of this technology is no longer confined to large-scale tech companies; it has expanded into healthcare, education, finance, transportation, e-commerce, national security, and public administration. The widening adoption of AI has led to a steady increase in the volume of personal data being processed, thereby placing the protection of privacy rights at the forefront of legal policymaking in many countries. This situation demonstrates that while digital technology advancements offer opportunities to improve service quality and productivity, they also entail legal consequences that demand increasingly comprehensive regulatory responses (Sharma & Sharma, 2024).

The enhanced capacity of AI to process large-scale data has fundamentally altered the nature of personal information usage. Systems that once served merely as data repositories have evolved into tools capable of linking disparate data sources, identifying individual behavioral patterns, performing automated classification, generating predictions, and

formulating recommendations based on data derived from public digital activity. These processes operate continuously through the integration of various digital platforms, often leaving individuals unaware of the extent to which their data is being utilized for specific purposes. This scenario reveals that personal data management has reached a level of complexity that far outpaces the regulatory frameworks established to date for privacy protection. Consequently, nations are increasingly challenged to ensure that technological advancements remain within boundaries that respect the fundamental rights of every individual (Egbert & Ulbricht, 2024).

Changes in data processing characteristics have also heightened attention regarding the relationship between technological advancement and the protection of human rights. Privacy is no longer viewed merely as a matter of personal information confidentiality; it has evolved into a crucial element in safeguarding an individual's freedom to control how information about themselves is used. As Artificial Intelligence (AI) systems become capable of generating highly detailed analyses of an individual's behavior, preferences, location, health status, economic activities, and social connections, the resulting legal implications become increasingly far-reaching. Information gathered through various digital activities can be used to construct comprehensive individual profiles, thereby influencing significant decisions—such as access to financial services, employment opportunities, healthcare, and other forms of public service. This situation demonstrates that privacy protection is no longer solely about data security; it is also linked to the protection of various civil rights that could be impacted by the use of AI-based technologies (Theodorakopoulos & Theodoropoulou, 2024).

The growing adoption of Artificial Intelligence coincides with the rise of digital economic models that treat data as a primary business asset. Companies across various sectors are racing to develop AI-driven analytics systems to gain deeper insights into consumer behavior, devise more effective marketing strategies, optimize supply chains, and enhance service quality. Meanwhile, government institutions are also leveraging similar technologies to support public services, administrative systems, security monitoring, and data-driven policymaking. The widespread use of these technologies underscores that personal data processing has become an integral part of modern activity. As reliance on data grows, so does the need for a legal framework that provides certainty regarding the limits of personal data usage, ensuring that technological adoption does not compromise the protection of public rights (Lv et al., 2024).

This situation is further complicated by the fact that Artificial Intelligence systems operate without regard for national jurisdictional boundaries when processing data. Various digital services operate across borders, utilizing cloud computing infrastructure, international data centers, and global communication networks that allow personal data to move rapidly from one legal jurisdiction to another. This situation means that the application of privacy laws no longer relies solely on national regulations but is also influenced by the interplay between various legal systems that adopt differing approaches to personal data protection. Such disparities often create uncertainty regarding the applicable law when data processing activities involve more than one country. This issue is of increasing importance, given that most Artificial Intelligence service providers are global companies serving users across multiple jurisdictions simultaneously (Tang, 2022).

Countries are responding to the evolution of Artificial Intelligence by establishing or refining regulations governing personal data protection, employing approaches that vary significantly. Some nations have developed legal frameworks that treat privacy as a fundamental right, thereby ensuring that individual protection holds a robust position in all data processing activities. Others prioritize balancing privacy protection with the interests of technological innovation and digital economic growth. Some jurisdictions grant governments

greater latitude to utilize data for national security and public administration purposes. These differing orientations result in considerable variation regarding data subject consent, the obligations of data controllers, the liability of AI developers, oversight mechanisms, and the nature of sanctions for violations (Peck Pinheiro & Batista Battaglini, 2022).

This diversity in regulatory approaches demonstrates that the formulation of privacy laws can no longer be decoupled from rapid technological advancement. Regulations drafted when data processing was still conducted conventionally struggle to accommodate the characteristics of AI systems, which can generate automated decisions by leveraging vast amounts of data. Such changes have prompted many countries to evaluate the effectiveness of existing regulations, whether by enacting new laws or amending current provisions. These efforts reflect a growing governmental focus on striking a balance between protecting individual rights and sustaining technological innovation (Radanliev, 2025).

Beyond differences in national regulations, another challenge arises because the evolution of Artificial Intelligence far outpaces the legislative process. Technology continues to advance, introducing new capabilities that were not previously addressed in legal instruments. These changes compel policymakers to make continuous adjustments to ensure regulations remain capable of effectively protecting the public. If lawmaking lags too far behind, data usage practices may evolve significantly before an adequate legal framework is in place to govern them. Conversely, if regulations are drafted too rigidly without regard for technological progress, innovation could face obstacles that undermine a nation's digital economic competitiveness. This situation indicates that the formulation of legal policy requires an adaptive approach capable of keeping pace with technological developments without compromising legal certainty (Walter, 2024).

Attention to privacy protection has intensified alongside the rising number of cases involving the large-scale use of personal data. Incidents such as data breaches, the misuse of user information, data utilization without adequate consent, and the deployment of automated systems to monitor public activity have heightened public awareness regarding the importance of legal protection for personal information. Public trust in digital services is heavily influenced by a system provider's ability to safeguard the data they manage. Consequently, regulations that provide certainty regarding the rights and obligations of all parties serve as a crucial factor in supporting the sustainability of digital transformation across various sectors (Qureshi & Koo, 2026).

International policy trends also reveal a growing focus on the responsible governance of Artificial Intelligence. International organizations, regional cooperation forums, and national governments are increasingly developing principles to guide technology usage—ensuring respect for human rights, accountability, transparency, and robust personal data protection. However, the implementation of these principles varies significantly, as countries possess distinct legal systems, development priorities, economic interests, and policy orientations. These differences have led to the emergence of diverse regulatory models; comparing them offers valuable insights into the trajectory of privacy law in the face of advancements in Artificial Intelligence (Wang & Xie, 2025).

Examining the relationship between Artificial Intelligence and privacy law has become increasingly vital, as regulatory evolution is driven not only by the need for data protection but also by the demand for legal certainty in the global use of digital technology. Nations are continuously updating their policies in response to the proliferation of AI-based systems, resulting in a variety of approaches that reflect the unique characteristics of each jurisdiction. A comparative analysis of these regulatory frameworks illuminates emerging trends in international privacy law and highlights alternative regulatory models that can serve as references for future policy development. Given these circumstances, this study aims to analyze

the role of Artificial Intelligence in shaping the evolution of privacy law through a comparative analysis of regulatory frameworks implemented across various countries, thereby providing a more comprehensive understanding of the direction of regulation-making capable of balancing privacy rights protection with technological advancement.

B. LITERATURE REVIEW

1. Artificial Intelligence

Artificial Intelligence (AI) is a branch of computer science focused on mimicking human thought processes and applying them to machine systems, particularly computers. According to John McCarthy, intelligence encompasses a combination of knowledge, experience, and the reasoning ability required for decision-making and action, alongside a sound moral foundation. The primary goal of AI is to create computer systems capable of thinking more intelligently and to enhance the utility of machines. Rich and Knight describe AI as the discipline concerned with designing computers to perform tasks that are currently better executed by humans. Furthermore, Artificial Intelligence is understood as a concept involving the design of intelligent software capable of completing tasks typically performed by humans. In line with this, Waterman states that artificial intelligence is a field of computer science essential for developing advanced software intelligence (Alkatheiri, 2022).

According to Nugraha and Winiarti, Artificial Intelligence is a branch of science concerned with utilizing machines to solve complex problems in a manner that mimics human approaches. This is typically achieved by emulating the characteristics and thought processes of human intelligence and implementing them as algorithms executable by computers. Depending on specific requirements, a flexible and efficient approach can be adopted, which in turn shapes the nature of the artificial intelligence's behavior. Meanwhile, Solikhun, M. Safii, and Agus Trisno define Artificial Intelligence as the intelligence exhibited by an artificial entity—typically a computer system. In this context, intelligence is created and embedded into a machine (computer) to enable it to perform tasks similar to those performed by humans (Jaboob et al., 2024).

2. Privacy Law

Privacy represents a fundamental concept that has developed across various legal systems, social norms, and ethical frameworks throughout human history. The recognition of privacy reflects the understanding that individuals possess certain interests, personal spaces, and forms of autonomy that require protection from excessive interference by other individuals, organizations, or the state. Although the meaning and scope of privacy continue to evolve alongside social and technological changes, the protection of privacy remains closely associated with the preservation of individual dignity, freedom, and personal control over information and personal affairs (Gestrein & Beaulieu, 2022).

The modern development of privacy rights is strongly associated with the work of Samuel D. Warren and Louis D. Brandeis through their influential article entitled “The Right to Privacy” published in 1890. Warren and Brandeis introduced the idea that privacy should be recognized as an independent legal interest, defining privacy as the “right to be let alone.” This concept emphasized that individuals should have the ability to maintain control over aspects of their personal lives without unnecessary intrusion from external parties. According to Warren and Brandeis, privacy protection is not merely related to physical isolation but also involves the protection of human personality, emotions, thoughts, and personal experiences. They argued that certain aspects of individual existence require legal protection because they represent essential elements of human dignity and personal autonomy (Ye et al., 2024).

The development of privacy rights has expanded significantly beyond the original understanding proposed by Warren and Brandeis. In contemporary legal systems, privacy is no longer limited to protection against physical or personal interference but also includes protection against unauthorized access, collection, processing, and dissemination of personal information. The expansion of digital technologies, particularly the growth of data-driven systems and Artificial Intelligence, has transformed privacy into a broader legal and policy concern. Personal information has become a valuable resource that can influence individual opportunities, social relationships, economic activities, and access to public or private services. Consequently, privacy protection increasingly requires regulatory frameworks capable of controlling how personal data is collected, processed, stored, and utilized (Guo et al., 2024).

In the context of modern governance, privacy policy functions as an important mechanism to establish rules, responsibilities, and limitations regarding the management of personal information. A privacy policy is not only concerned with preventing misuse of data but also aims to ensure transparency, accountability, and fairness in information processing activities. Through privacy policies, organizations and governments are expected to provide clear explanations regarding the purposes of data collection, the methods of processing, the rights of individuals, and the obligations of data controllers. Therefore, privacy policy has developed into a crucial instrument for balancing technological innovation with the protection of fundamental individual rights (Calzada, 2022).

C. METHOD

This study employs a normative legal research method with a comparative approach as its primary framework for analyzing the evolution of privacy regulations influenced by the adoption of Artificial Intelligence across various countries. This approach was selected because the research focuses on analyzing legal norms, policies, and regulatory instruments governing personal data protection and Artificial Intelligence governance across different jurisdictions. The analysis utilizes a statutory approach to examine applicable legislation in each country, a conceptual approach to understand the legal theories underpinning these regulations, and a comparative law approach to identify similarities, differences, and trends in privacy regulation within various global regulatory frameworks. By combining these three approaches, the study aims to gain a comprehensive understanding of how privacy law is evolving in response to advancements in Artificial Intelligence technology. Research data were gathered through a literature review utilizing primary and secondary legal sources relevant to the study's focus. Primary legal materials include legislation, regulations, and policies regarding personal data protection and Artificial Intelligence governance from the countries selected for comparison. Meanwhile, secondary legal materials were obtained from scholarly articles and academic publications relevant to the issues under examination. All collected legal materials underwent qualitative analysis, involving inventory, classification, interpretation, and comparison of regulatory frameworks—to identify regulatory characteristics, discern trends in legal development, and draw conclusions aligned with the research objectives (Rizkia & Fardiansyah, 2023).

D. RESULT AND DISCUSSION

1. Artificial Intelligence as a Driver of Contemporary Privacy Challenges

The rapid advancement of Artificial Intelligence has significantly transformed the way institutions manage and utilize data for operational activities and decision-making processes. Developments in computing capacity, data storage, and large-scale information processing have positioned Artificial Intelligence as a central element of digital transformation across various sectors, including healthcare, finance, e-commerce, manufacturing, education,

transportation, and public administration. These applications continuously generate extensive digital records that provide valuable resources for AI systems to perform automated analysis and prediction. As AI increasingly depends on the availability of large-scale data, the relationship between technological development and privacy protection has become inseparable. The broader adoption of Artificial Intelligence has expanded the volume and complexity of personal information being processed, creating new challenges for privacy regulation in the digital era.

The data-intensive nature of Artificial Intelligence has fundamentally changed the characteristics of personal data processing compared to conventional digital systems. AI applications require diverse and extensive datasets to improve analytical accuracy, enhance predictive capabilities, and generate outputs tailored to user needs. Such information is not only obtained from data voluntarily provided by individuals but also collected through continuous digital activities, including search histories, location information, online transactions, social media interactions, communication patterns, and device usage behavior (Abdalla, 2022). The integration of these sources enables AI systems to construct detailed representations of individuals, expanding the scope of information that can be utilized for commercial, administrative, and institutional purposes. However, continuous data collection and processing also create significant privacy concerns because individuals often lack sufficient knowledge regarding what information is collected, how it is analyzed, and for what future purposes it may be used.

The increasing capability of Artificial Intelligence to perform automated decision-making has further intensified privacy challenges. Organizations now utilize AI-based systems to support decisions related to credit assessment, employment recruitment, insurance evaluation, financial monitoring, risk identification, and public service delivery. Although these systems improve efficiency and accelerate decision-making processes, they also raise concerns regarding transparency and accountability when automated decisions directly affect individual rights, opportunities, or access to essential services. The difficulty of understanding how algorithms generate specific outcomes creates uncertainty regarding whether individuals are able to challenge decisions made through automated processes. Therefore, legal protection concerning automated decision-making has become an essential component of contemporary privacy governance.

AI-driven profiling represents another major challenge because the integration of multiple data sources allows systems to generate detailed assessments of individual characteristics, preferences, behaviors, and potential future actions. Profiling mechanisms are widely used for targeted advertising, consumer segmentation, risk assessment, and service personalization. While these practices may improve efficiency and user experience, extensive profiling also creates risks of excessive surveillance and secondary use of personal information beyond the original purpose of collection. The more comprehensive the profile generated by AI systems, the greater the possibility that personal data may be used to influence individual behavior without sufficient awareness or control from the data subject.

The expansion of facial recognition and biometric processing technologies demonstrates how Artificial Intelligence has broadened the scope of sensitive data utilization. Facial recognition systems are increasingly implemented for authentication, security management, public surveillance, financial services, and governmental identification processes. Despite providing significant benefits in improving efficiency and security, these technologies create concerns regarding continuous monitoring and identification without meaningful individual awareness or consent. Similar concerns arise from the processing of biometric information, such as fingerprints, voice patterns, facial characteristics, and retinal data, which possess permanent characteristics that distinguish them from ordinary personal

data. Unlike passwords or other replaceable information, biometric data cannot easily be changed when compromised. Consequently, the increasing use of AI-based biometric processing requires stronger legal safeguards due to the potential severity of misuse and unauthorized access.

Artificial Intelligence has also expanded the use of predictive analytics by enabling organizations to forecast individual behavior, preferences, and possible future actions based on historical data patterns. Predictive systems are applied in various areas, including business strategy, healthcare management, digital marketing, risk evaluation, and law enforcement. Although predictive analytics provides substantial benefits in improving efficiency and supporting policy development, it also raises legal concerns because individuals may be evaluated based on predicted characteristics rather than actual actions. Such practices create possibilities for unfair treatment, inaccurate assumptions, and decisions influenced by algorithmic assessments that are difficult to verify or challenge.

The widespread adoption of Artificial Intelligence has consequently increased various privacy risks throughout the entire data processing lifecycle. These risks extend beyond conventional data breaches and include unauthorized secondary use, excessive data collection, long-term retention, integration of information from multiple sources, and unclear responsibility among organizations involved in data processing. The complexity of AI ecosystems makes it increasingly difficult to determine which actors are responsible for specific stages of data utilization, particularly when information is transferred among multiple providers through technological partnerships and digital infrastructures. This situation demonstrates that privacy protection in the AI era requires broader regulatory approaches that address not only data security but also the governance of data utilization.

Algorithmic surveillance has further expanded these concerns by enabling continuous monitoring through the automated analysis of location data, online activities, financial transactions, communications, and behavioral patterns. Unlike traditional surveillance mechanisms that rely primarily on human observation, AI-based surveillance systems can operate at a large scale with minimal human intervention (Mettler, 2024). Although such systems may support security and administrative efficiency, excessive reliance on algorithmic monitoring may threaten individual privacy and create conditions of constant observation. Therefore, effective regulation is required to establish proportional boundaries between legitimate security interests and the protection of personal freedoms.

Another significant challenge concerns the effectiveness of consent mechanisms in AI-based data processing. Traditional consent models often rely on lengthy digital agreements provided at the beginning of service use, while AI systems continue to develop new capabilities and purposes that may not have been anticipated when consent was initially provided. As a result, individuals may agree to data processing without fully understanding the extent of future utilization. This condition demonstrates that privacy protection cannot rely solely on formal consent but must also ensure meaningful transparency regarding how personal information is collected, analyzed, and applied.

Transparency has therefore become a fundamental issue in contemporary AI governance. Many AI systems operate through complex computational processes that make it difficult for individuals to understand how decisions are generated, what factors influence outcomes, and how personal information contributes to automated analysis. Limited transparency reduces public trust and weakens the ability of individuals to exercise their privacy rights, particularly when AI-generated decisions have significant consequences. Accordingly, transparency and accountability must become essential elements of privacy regulation to ensure that Artificial Intelligence development remains aligned with legal protection and individual rights.

These challenges demonstrate that Artificial Intelligence has fundamentally transformed the scope of privacy protection. Privacy concerns in the AI era are no longer limited to data storage and security but extend across the entire process of data collection, integration, analysis, decision-making, and application. As AI systems become increasingly capable of generating new insights from personal information, legal frameworks must continue to evolve to address emerging risks while maintaining a balance between technological innovation and the protection of fundamental privacy rights.

2. Comparative Analysis of Privacy Law Frameworks in Major Jurisdictions

The development of Artificial Intelligence has significantly influenced the direction of privacy law reform across different jurisdictions. Although most countries share similar objectives, namely protecting personal data while supporting digital innovation, each jurisdiction has developed distinct regulatory approaches based on its legal tradition, policy priorities, and economic interests. These differences can be observed in the formulation of legal foundations, individual data rights, obligations of data controllers, accountability mechanisms, enforcement systems, and AI governance structures. Comparative analysis is therefore essential to understand how different legal systems respond to the challenges created by Artificial Intelligence and to identify emerging principles that are increasingly recognized in global privacy governance (Mustafa et al., 2025).

The European Union represents one of the most comprehensive jurisdictions in regulating privacy protection in the context of Artificial Intelligence. Its regulatory framework is primarily established through the General Data Protection Regulation (GDPR), which has applied since 2018, and is further strengthened by the Artificial Intelligence Act adopted in 2024. Unlike approaches that primarily view AI as a matter of technological development, the European Union places AI governance within the broader framework of fundamental rights protection. Under GDPR Article 6, every processing activity involving personal data must be supported by a valid legal basis, including consent, contractual necessity, legal obligations, vital interests, public tasks, or legitimate interests. This approach requires organizations using Artificial Intelligence to justify the legality of data processing rather than relying solely on technological capability or commercial interests.

Consent occupies an important position within the European framework because GDPR requires consent to be freely given, specific, informed, and expressed through a clear affirmative action. This requirement ensures that individuals understand how their personal information will be processed before being utilized by AI systems. In addition, individuals retain the right to withdraw consent when no alternative legal basis exists. The GDPR approach demonstrates a strong emphasis on individual control over personal data compared with jurisdictions that provide broader flexibility for organizations to determine data utilization practices.

The protection of individual rights is also reflected in GDPR Article 22 concerning automated decision-making. This provision grants individuals the right not to be subject to decisions based solely on automated processing when such decisions produce legal effects or significantly affect them. The regulation is particularly relevant as Artificial Intelligence is increasingly used in credit assessments, employment selection, insurance evaluation, and public services. Although certain exceptions exist, organizations must provide mechanisms for human intervention, allow individuals to express their views, and enable challenges against automated decisions. Furthermore, the GDPR principle of data minimization requires organizations to collect only information necessary for specific purposes, creating important limitations for AI systems that depend on extensive datasets. This principle requires developers and data controllers to evaluate the relevance and proportionality of data used in AI development and operation.

The European accountability framework extends beyond general compliance obligations by requiring organizations to demonstrate that data processing activities comply with legal requirements. GDPR establishes obligations such as documentation of processing activities, Data Protection Impact Assessments for high-risk processing, appointment of Data Protection Officers in certain circumstances, and implementation of appropriate technical and organizational measures. These obligations are reinforced by the AI Act, which introduces additional requirements for high-risk AI systems, including risk management, data quality assessment, technical documentation, transparency obligations, human oversight, and post-market monitoring. Enforcement mechanisms further strengthen this framework, as data protection authorities may conduct investigations, issue corrective measures, and impose administrative fines of up to €20 million or 4% of global annual turnover. Through these mechanisms, the European Union positions privacy protection as an essential component of responsible AI governance.

In contrast, the United States adopts a more decentralized and sector-based approach to privacy and Artificial Intelligence regulation. Unlike the European Union, the United States does not currently have a comprehensive federal privacy law or a single AI regulation applicable across all sectors. Instead, privacy protection is developed through sector-specific legislation, Federal Trade Commission (FTC) enforcement authority, and state-level regulations. This approach reflects the broader American regulatory philosophy that prioritizes flexibility, market innovation, and industry adaptation. Consequently, privacy protection standards vary significantly between jurisdictions.

California represents one of the most advanced examples of state-level privacy regulation through the California Consumer Privacy Act (CCPA), strengthened by the California Privacy Rights Act (CPRA). These regulations provide consumers with rights to access personal information, request deletion, opt out of data sales, and receive protection against discriminatory practices related to exercising privacy rights. However, unlike GDPR, the California framework generally emphasizes consumer control after data collection rather than requiring strict legal justification before processing occurs. This difference demonstrates the contrast between the European preventive approach and the American consumer-oriented model.

Regarding automated decision-making, the United States does not yet provide a comprehensive federal equivalent to GDPR Article 22. Instead, AI-related risks are addressed through existing consumer protection, anti-discrimination, and unfair business practice frameworks. The FTC has increasingly emphasized that AI systems causing privacy violations, discriminatory outcomes, or deceptive practices may become subject to enforcement actions under its existing authority. At the federal level, the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence issued in 2023 also encouraged responsible AI development, risk management, transparency, and protection of public interests, although implementation remains dependent on coordination among federal agencies.

Data minimization and accountability requirements are generally less restrictive in the United States compared with the European model. Organizations often have greater flexibility to collect and process information as long as their activities comply with applicable sectoral regulations or state laws. While this approach may support AI innovation by providing broader access to data resources, it also raises concerns regarding excessive data collection and limited consumer control. Accountability mechanisms are therefore developed primarily through organizational practices, industry standards, and emerging risk assessment frameworks rather than through comprehensive legal obligations comparable to GDPR.

The comparison between the European Union and the United States illustrates two contrasting models of AI privacy governance. The European Union adopts a rights-based and

comprehensive regulatory approach that emphasizes legal certainty, individual protection, accountability, and risk control. Meanwhile, the United States relies on a more flexible innovation-oriented model that allows broader technological development while addressing harms through sectoral regulation and enforcement mechanisms. These differences demonstrate that AI privacy governance is shaped not only by technological developments but also by distinct legal philosophies, institutional structures, and policy priorities. Both approaches provide important perspectives in understanding how jurisdictions attempt to balance privacy protection with the continued advancement of Artificial Intelligence.

China and Indonesia demonstrate two distinct approaches to privacy regulation in the context of Artificial Intelligence, differing from the rights-based model of the European Union and the innovation-oriented framework of the United States. China has developed a state-centered data governance model that integrates privacy protection with digital economic development, cybersecurity, and national security interests. This approach is reflected in three major legal instruments: the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (PIPL) (2021). These regulations establish a comprehensive framework governing cybersecurity, data governance, and personal information protection. Alongside these instruments, China has introduced AI-specific regulations, including the Provisions on the Administration of Algorithmic Recommendation Services (2022), the Provisions on the Administration of Deep Synthesis Internet Information Services (2023), and the Interim Measures for the Management of Generative Artificial Intelligence Services (2023). These developments demonstrate that China views Artificial Intelligence not only as a technological issue but also as a matter involving social governance, information security, and regulatory control over algorithmic systems.

The Personal Information Protection Law serves as the primary legal foundation for personal data processing in China. Similar to the European Union's General Data Protection Regulation (GDPR), PIPL establishes principles concerning lawful processing, individual rights, and obligations of data processors. However, its regulatory orientation differs significantly from GDPR. While GDPR primarily emphasizes the protection of fundamental rights, PIPL operates within a broader framework that incorporates cybersecurity, state governance, and control over cross-border data flows. Consequently, privacy protection in China is closely connected with national strategies concerning digital development and information management.

Regarding consent, PIPL requires personal information processing to generally rely on voluntary, informed, and explicit consent from individuals. This approach reflects similarities with GDPR by recognizing individual control over personal information. However, PIPL provides broader exceptions that allow processing without consent under certain circumstances, including legal obligations, administrative duties, emergencies, and public interests. The regulation also provides enhanced protection for sensitive personal information, such as biometric data, health information, financial records, and location data, requiring additional safeguards before processing. Thus, although consent remains an important element, its application is balanced with broader state interests.

China has also developed more specific regulatory mechanisms concerning algorithmic decision-making. Regulations on algorithmic recommendation services require providers to ensure that recommendation systems do not violate legal requirements, mislead users, or create discriminatory outcomes. Providers must also provide mechanisms allowing users to modify or reject certain forms of algorithmic personalization. These requirements indicate that China has recognized the potential impact of Artificial Intelligence on individual rights, particularly when algorithmic systems influence access to information and digital services. However, unlike GDPR Article 22, which explicitly establishes protections against solely automated

decisions, China's framework remains primarily based on administrative regulations rather than a unified legal right regarding automated decision-making.

The principle of data minimization is also incorporated into PIPL through requirements that personal information collection must be limited to a specific and legitimate purpose. Data processors are prohibited from collecting excessive information unrelated to the intended processing objective. This principle demonstrates convergence with international privacy standards, particularly GDPR. Nevertheless, implementation remains influenced by other regulatory requirements related to state supervision and cybersecurity obligations. Therefore, China's privacy framework reflects an attempt to balance individual protection with broader governmental interests in managing digital information.

Accountability mechanisms in China have developed alongside the expansion of Artificial Intelligence. Under PIPL, data processors must implement technical and organizational measures to protect personal information, conduct risk assessments for certain processing activities, appoint responsible personnel where required, and notify authorities and affected individuals in cases of data breaches. AI-specific regulations further require providers of generative AI services to manage training data responsibly, ensure data quality, and prevent the generation of unlawful content. Enforcement is primarily conducted through the Cyberspace Administration of China (CAC) and other governmental authorities, which possess broad powers to conduct investigations, impose administrative penalties, restrict processing activities, and suspend services. PIPL establishes significant penalties, including fines of up to RMB 50 million or five percent of annual revenue for serious violations, reflecting strong governmental involvement in AI and data governance.

In contrast, Indonesia remains in the process of developing a more comprehensive regulatory framework for Artificial Intelligence. Unlike China, Indonesia does not yet possess specific legislation governing AI systems. However, personal data protection has gained a stronger legal foundation through Law No. 27 of 2022 on Personal Data Protection (PDP Law). Additional regulatory references include Law No. 11 of 2008 on Electronic Information and Transactions, as amended most recently by Law No. 1 of 2024, Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, and the Ministry of Communication and Informatics Circular Letter No. 9 of 2023 concerning Artificial Intelligence Ethics. Although these instruments provide initial guidance for responsible AI use, the AI Ethics Circular remains a soft law instrument without the binding authority of legislation.

The Indonesian PDP Law adopts several principles similar to GDPR, including lawful processing, individual rights, consent requirements, and obligations of data controllers. Consent functions as one of the primary legal bases for processing personal information, strengthening individual control over personal data. However, unlike GDPR and PIPL, Indonesia has not established detailed provisions specifically addressing AI-related processing activities. The regulation also does not yet provide a comprehensive framework concerning automated decision-making, algorithmic transparency, explainability, or the right to human intervention when decisions are generated through Artificial Intelligence systems.

Indonesia has adopted the principle of data minimization by requiring personal data processing to be limited, specific, and proportional to the purpose of collection. Nevertheless, practical implementation remains challenging because AI systems often require large datasets for training and operation. Without more detailed technical regulations, balancing data protection requirements with AI development needs remains a significant regulatory challenge. Similarly, accountability obligations under the PDP Law primarily focus on general personal data governance, including confidentiality, security, accuracy, and breach notification. Unlike the EU AI Act or China's AI-specific regulations, Indonesia has not yet established mandatory

AI risk assessments, algorithm audits, or specific obligations concerning training data governance.

Regarding enforcement, Indonesia's PDP Law introduces administrative and criminal sanctions for violations of personal data protection obligations. However, the effectiveness of enforcement depends on institutional capacity, regulatory coordination, and the establishment of a strong supervisory mechanism. Compared with the EU's data protection authorities and China's CAC, Indonesia's oversight framework requires further development to effectively address increasingly complex AI-related privacy issues.

Overall, the comparison demonstrates significant differences among jurisdictions in regulating Artificial Intelligence and privacy protection. China adopts a state-centered governance model that integrates privacy, cybersecurity, and national interests, while Indonesia remains focused on strengthening its foundational privacy framework through the PDP Law. Compared with the comprehensive European approach and the flexible American model, both countries illustrate alternative regulatory pathways shaped by their respective legal systems, institutional structures, and policy priorities.

Table 1. Comparative Analysis of Privacy Law Frameworks Governing Artificial Intelligence

Aspect	European Union	United States	China	Indonesia
Legal Basis	GDPR; AI Act	CCPA/CPRA; FTC Act	PIPL; DSL; CSL	UU PDP; UU ITE
Regulatory Approach	Rights-based	Sectoral	State-centric	Emerging
Consent	Strong	Moderate	Strong	Strong
Automated Decision	Regulated	Limited	Regulated	Limited
Data Minimization	Yes	Partial	Yes	Yes
Accountability	High	Medium	High	Developing
Enforcement	DPAs	FTC & States	CAC	PDP Supervisory Institution
AI Governance	Comprehensive	Flexible	Comprehensive	Emerging

Table 1 summarizes the principal characteristics of privacy law frameworks governing Artificial Intelligence across the European Union, the United States, China, and Indonesia. Although all four jurisdictions recognize the importance of protecting personal data in the digital era, they adopt different regulatory approaches regarding legal foundations, consent requirements, automated decision-making, accountability mechanisms, enforcement, sanctions, and AI governance. These similarities and differences provide a useful basis for understanding the diverse legal models that have emerged in response to AI-driven privacy challenges and serve as the foundation for the comparative analysis presented below.

This comparison demonstrates that the development of Artificial Intelligence has spurred the emergence of various governance models reflecting the legal philosophies, institutional structures, and policy priorities of each jurisdiction. The European Union places individual rights at the core of its regulatory framework through a comprehensive, risk-based approach. The United States opts for a more adaptive strategy, offering flexibility to innovators while reinforcing the role of sectoral regulators. China combines personal data protection with national security interests and state oversight of algorithmic usage. Indonesia is currently in a transitional phase; while its data protection foundation is strengthening, it still requires the

development of regulations specifically addressing Artificial Intelligence governance. These differences reveal that there is currently no universally applicable regulatory model; consequently, the legal framework for privacy in the age of Artificial Intelligence will continue to evolve in response to technological advancements, the need to protect public rights, and the strategic interests of individual nations (Aubert-Hassouni & Cloarec, 2022).

3. Regulatory Gaps and Legal Challenges in AI Governance

The rapid development of Artificial Intelligence has significantly transformed existing privacy and data protection frameworks. The ability of AI systems to process massive amounts of information, generate automated decisions, and integrate data from multiple sectors has advanced much faster than regulatory development. As a result, many jurisdictions face a gap between technological capabilities and the ability of legal systems to regulate their use effectively. Traditional privacy regulations, which were primarily designed for conventional data processing activities, increasingly encounter difficulties in addressing AI characteristics, particularly because AI systems can continuously learn, generate new insights, and create new forms of data utilization. Therefore, contemporary AI governance challenges extend beyond personal data protection and involve the broader capacity of legal systems to provide certainty, accountability, and protection in rapidly changing technological environments.

One of the most significant challenges in AI governance is regulatory fragmentation. Currently, there is no unified international legal framework establishing common standards for AI development and deployment. Different jurisdictions have adopted different regulatory approaches based on their legal traditions, policy priorities, and institutional structures. The European Union has developed a comprehensive framework through the General Data Protection Regulation (GDPR) and Artificial Intelligence Act, while the United States continues to rely on sectoral regulations, state-level privacy laws, and enforcement mechanisms such as the Federal Trade Commission. China has adopted a state-centered approach through the Cybersecurity Law, Data Security Law, Personal Information Protection Law (PIPL), and AI-specific regulations concerning algorithms and generative AI. Indonesia, meanwhile, continues to strengthen its privacy framework through Law No. 27 of 2022 on Personal Data Protection, while AI governance remains primarily guided by ethical principles rather than binding legislation. These differences create compliance challenges for organizations operating across multiple jurisdictions because similar AI practices may receive different legal treatments depending on the applicable regulatory environment.

Regulatory fragmentation is closely connected with challenges concerning cross-border data transfer. Modern AI systems frequently rely on cloud computing, international data centers, and global digital infrastructures that enable personal information to move across jurisdictions. Data collected in one country may be processed in another jurisdiction, used for AI model training elsewhere, and subsequently applied globally. This complex processing chain creates uncertainty regarding applicable laws and the level of protection provided to personal information (Rong et al., 2025). The GDPR addresses this issue by requiring appropriate safeguards before transferring personal data to third countries, including adequacy decisions, Standard Contractual Clauses, and Binding Corporate Rules. China adopts a stricter approach through PIPL and the Data Security Law by maintaining stronger governmental oversight over certain categories of cross-border data transfers. Meanwhile, the United States lacks a unified federal framework, and Indonesia is still developing detailed mechanisms for international data transfers. These differences demonstrate that harmonizing cross-border data governance remains one of the central challenges in global AI regulation.

The global nature of AI processing also creates jurisdictional conflicts. A single AI service may involve multiple jurisdictions, including the location where data is collected,

where companies operate, where servers are located, and where AI models are developed. Consequently, several legal systems may claim authority over the same processing activity, creating uncertainty regarding applicable law, supervisory authority, and dispute resolution mechanisms (Orhan et al., 2025). Although GDPR applies extraterritorially to certain organizations outside the European Union that process EU residents' data, such mechanisms do not completely resolve the challenges created by the borderless nature of Artificial Intelligence.

Another fundamental challenge concerns explainability and transparency in AI decision-making. Many advanced AI systems, particularly those based on deep learning, operate through complex computational processes that make it difficult to understand how specific outcomes are generated. This becomes a significant legal concern when AI decisions influence access to employment, financial services, healthcare, insurance, or public services. Individuals affected by automated decisions may not understand what factors influenced the outcome or how their personal data contributed to the decision-making process. GDPR addresses this issue through transparency obligations and protections against solely automated decision-making under Article 22, while the AI Act strengthens these requirements by imposing documentation, information disclosure, and monitoring obligations for high-risk AI systems. These developments demonstrate that explainability has become a central element of responsible AI governance.

Explainability is closely related to accountability because complex AI systems involve multiple actors, including data providers, developers, technology companies, infrastructure providers, and organizations implementing AI solutions. Determining legal responsibility becomes increasingly difficult when harm results from interconnected technical processes involving several parties. The European Union addresses this challenge through a risk-based regulatory approach under the AI Act, which requires high-risk AI providers to implement risk management systems, ensure data quality, conduct testing, maintain technical documentation, apply human oversight, and perform post-market monitoring. International standards such as ISO/IEC 42001:2023 on Artificial Intelligence Management Systems further support organizational accountability by establishing governance structures for responsible AI management.

Algorithmic bias and discrimination represent additional challenges arising from AI dependence on training data. AI systems may reproduce or reinforce existing social inequalities when datasets contain historical biases, incomplete representation, or inaccurate information. These risks are particularly significant when AI is applied in employment recruitment, credit evaluation, healthcare, law enforcement, and public services, where automated decisions may directly affect individual rights and opportunities. Consequently, ensuring data quality, fairness, and non-discrimination has become an essential component of AI regulation. The AI Act and various international AI governance frameworks emphasize the importance of risk assessment and monitoring to prevent harmful algorithmic outcomes.

Beyond legal compliance, the development of ethical AI principles has become an important complementary approach to regulatory governance. International frameworks such as the OECD AI Principles (2019), UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (2024) emphasize human rights protection, fairness, transparency, accountability, and democratic values. These instruments demonstrate that AI governance is no longer limited to technological management or privacy protection but has become closely connected with broader societal values and fundamental rights.

Despite significant regulatory developments, regulatory uncertainty remains a persistent challenge because AI innovation frequently progresses faster than legislative processes. Emerging technologies, particularly generative AI, have expanded globally before many jurisdictions established specific legal frameworks. This situation creates uncertainty for both individuals seeking privacy protection and organizations attempting to determine compliance requirements. Furthermore, enforcement difficulties remain significant because regulators often face limitations in accessing AI models, training data, and technical documentation. Effective AI governance therefore requires not only comprehensive legal frameworks but also stronger institutional capacity, international cooperation, technical expertise, and continuous adaptation of regulatory approaches. Ultimately, future AI regulation must achieve an appropriate balance between protecting privacy rights and enabling responsible technological innovation.

Table 2. Major Regulatory Gaps and Legal Challenges in AI Governance

Regulatory Issue	Current Legal Challenge	Implications for Privacy Protection	Future Regulatory Direction
Fragmented regulations	Different AI and privacy laws across jurisdictions	Legal uncertainty for global AI deployment	International regulatory harmonization
Cross-border data transfer	Different transfer mechanisms and adequacy requirements	Inconsistent protection of personal data	Interoperable cross-border data governance
Jurisdictional conflicts	Multiple jurisdictions claim authority over AI processing	Difficulties in determining applicable law	Enhanced international cooperation
Explainability	Black-box AI models reduce transparency	Individuals cannot understand automated decisions	Explainable AI requirements
Accountability	Unclear allocation of legal responsibility	Difficulties identifying liable parties	Algorithm accountability framework
Algorithm bias	Biased training datasets	Discrimination and unfair outcomes	Mandatory AI risk assessment
Transparency	Limited disclosure of AI processing	Reduced public trust	Transparency obligations
Enforcement	Limited regulatory capacity	Weak implementation of AI governance	Stronger supervisory authorities
Innovation vs Privacy	Excessive regulation may hinder innovation	Regulatory imbalance	Risk-based regulatory approach

Table 2 demonstrates that the principal legal challenges associated with Artificial Intelligence are interconnected rather than isolated. Fragmented regulations, jurisdictional conflicts, limited algorithm transparency, accountability gaps, and enforcement difficulties collectively contribute to regulatory uncertainty and weaken the effectiveness of privacy protection. The comparison further indicates that future AI governance should adopt a coordinated and risk-based regulatory approach capable of addressing these challenges while maintaining an appropriate balance between technological innovation and the protection of fundamental rights.

4. Future Directions for AI-Oriented Privacy Law Reform

The rapid development of Artificial Intelligence has demonstrated that privacy law can no longer rely on static regulatory approaches. The continuous evolution of AI technologies has created new forms of data processing that were not previously anticipated within conventional legal frameworks. Regulations designed to govern traditional data processing activities often face difficulties in addressing AI characteristics, particularly its ability to process massive datasets, generate autonomous outputs, and create new information through continuous learning mechanisms. Therefore, future privacy law reform requires an adaptive regulatory approach that enables legal frameworks to respond effectively to technological developments while maintaining adequate protection of individual rights. Adaptive regulation does not imply reducing legal certainty, but rather establishing flexible mechanisms through periodic evaluation, technical standards, and stronger supervisory institutions. The European Union Artificial Intelligence Act illustrates this approach by combining binding legal obligations with technical requirements that can evolve alongside technological advancements.

A significant direction in future AI regulation is the increasing adoption of risk-based regulation. Unlike traditional regulatory models that apply uniform obligations across technologies, risk-based regulation allows policymakers to differentiate legal requirements according to the potential impact of AI systems on individuals and society (Currie et al., 2025). The European Union AI Act represents the most prominent example of this approach by classifying AI systems into different categories, including prohibited, high-risk, limited-risk, and minimal-risk systems. This model enables stronger restrictions on AI applications that may significantly affect fundamental rights while allowing lower-risk innovations to develop with fewer regulatory burdens. Such an approach provides a balance between privacy protection and technological advancement, making it increasingly relevant for other jurisdictions seeking to regulate AI without limiting innovation.

Beyond national regulatory frameworks, future privacy law reform also requires stronger international harmonization. AI operates through global digital infrastructures involving cross-border data flows, international cloud services, and multinational technology providers. Consequently, differences between national privacy regimes create regulatory uncertainty and compliance challenges. Various international instruments, including the OECD AI Principles (2019), UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (2024), demonstrate growing efforts to establish common principles for responsible AI governance. Although these instruments have different legal characteristics, they reflect a global movement toward ensuring that AI development remains consistent with human rights, democratic values, and the rule of law.

Future AI governance must also strengthen principles that integrate legal, technical, organizational, and ethical considerations throughout the AI lifecycle. Effective AI governance cannot be limited to controlling data usage but must include mechanisms for transparency, accountability, security, and human rights protection. International standards such as ISO/IEC 42001:2023 on Artificial Intelligence Management Systems contribute to this development by providing organizational frameworks for identifying risks, assigning responsibilities, and evaluating AI systems continuously. This indicates that future privacy regulation will increasingly depend on the interaction between formal legal rules and technical governance standards.

One of the most important principles in future privacy reform is privacy by design. This principle requires privacy protection to be incorporated from the earliest stages of AI system development rather than addressed only after risks emerge. Article 25 of the General Data

Protection Regulation (GDPR) recognizes this approach through the requirement of data protection by design and by default. In the context of AI, privacy by design becomes increasingly important because many privacy risks originate from initial stages of data collection, model development, and system architecture. Integrating privacy considerations during the design process can reduce excessive data processing, improve security mechanisms, and enhance public trust in AI applications.

Future regulatory frameworks must also reinforce human oversight and algorithm accountability. Although AI systems can improve efficiency and accuracy, decisions that significantly affect individuals should not rely entirely on automated processes without meaningful human supervision. The EU AI Act emphasizes human oversight requirements for high-risk AI systems to ensure that automated decisions remain subject to monitoring, evaluation, and potential intervention by human operators. Alongside human oversight, algorithm accountability must become a central element of AI governance. Accountability should include obligations related to data quality assessment, bias identification, technical documentation, auditing mechanisms, and responsibility allocation among developers, providers, and users of AI systems. This approach recognizes that AI-related harms often result from complex interactions between multiple actors rather than from a single decision-maker.

Given the global nature of AI development, international cooperation will become increasingly important in strengthening privacy protection. Cross-border data transfers, international AI development, and cloud-based infrastructures require cooperation among regulatory authorities to improve enforcement, information exchange, and the development of compatible regulatory standards (Radanliev, 2025). International initiatives such as the G7 Hiroshima AI Process, OECD frameworks, and regional cooperation mechanisms provide important platforms for establishing shared approaches to AI governance. Without stronger cooperation, differences between national regulations may continue to create uncertainty and weaken the effectiveness of privacy protection.

At the same time, privacy reform should maintain space for technological innovation through mechanisms such as regulatory sandboxes. These frameworks allow AI developers to test emerging technologies under regulatory supervision while enabling authorities to identify potential risks before large-scale implementation. The EU AI Act encourages the establishment of AI regulatory sandboxes as a means of supporting innovation while maintaining legal safeguards. For developing countries such as Indonesia, regulatory sandboxes may provide an opportunity to accelerate AI development while ensuring that technological progress remains consistent with privacy protection principles.

E. CONCLUSION

This study concludes that the rapid development of Artificial Intelligence has fundamentally reshaped the legal landscape of privacy protection, requiring regulatory frameworks to evolve beyond conventional data protection approaches. Comparative analysis demonstrates that major jurisdictions have adopted different regulatory models in responding to AI-driven privacy challenges. The European Union has established the most comprehensive framework through the integration of the General Data Protection Regulation and the Artificial Intelligence Act, emphasizing fundamental rights, risk-based governance, accountability, and transparency. The United States continues to rely on a sectoral and innovation-oriented approach, while China combines personal data protection with broader objectives relating to national security and digital governance. Indonesia, through the Personal Data Protection Law, has established an important legal foundation for privacy protection but has yet to develop a comprehensive legal framework specifically governing Artificial Intelligence. These differences illustrate that AI governance remains fragmented across jurisdictions, creating legal

uncertainty, jurisdictional conflicts, challenges in cross-border data transfers, algorithmic accountability issues, and difficulties in ensuring consistent enforcement. The findings further indicate that future privacy law reform should move toward adaptive, risk-based, and internationally coordinated regulatory frameworks capable of responding to the evolving characteristics of Artificial Intelligence. Effective governance requires the integration of privacy by design, human oversight, algorithm accountability, transparency, and ethical AI principles throughout the entire AI lifecycle, supported by stronger international cooperation and interoperable legal standards. Regulatory innovation, including the development of AI regulatory sandboxes and harmonized governance principles, should be complemented by institutional strengthening and enhanced regulatory capacity to ensure that legal systems remain responsive to technological change. Consequently, the future direction of privacy law should not merely focus on protecting personal data, but also on establishing a balanced legal ecosystem that simultaneously safeguards fundamental rights, promotes legal certainty, supports responsible innovation, and fosters sustainable AI development in the global digital environment.

REFERENCES

Abdalla, H. B. (2022). A brief survey on big data: technologies, terminologies and data-intensive applications. *Journal of Big Data*, *9*(1), 107.

Alkatheiri, M. S. (2022). Artificial intelligence assisted improved human-computer interactions for computer systems. *Computers and Electrical Engineering*, *101*, 107950.

Aubert-Hassouni, C., & Cloarec, J. (2022). Privacy regulation in the age of artificial intelligence. *Digital Marketing*, *544*.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129-1150.

Currie, W. L., Leimeister, J. M., Schlagwein, D., & Willcocks, L. (2025). Rethinking technology regulation in the age of AI risks. *Journal of Information Technology*, *40*(3), 236-245.

Egbert, S., & Ulbricht, L. (2024). Data integration and analysis platforms as digital platforms: A conceptual proposal. *Information, Communication & Society*, 1-22.

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, *35*(1), 3.

Guo, Z., Hao, J., & Kennedy, L. (2024). Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law. *Computer Law & Security Review*, *52*, 105928.

Jaboob, A., Durrah, O., & Chakir, A. (2024). Artificial intelligence: An overview. *Engineering applications of artificial intelligence*, 3-22.

Lv, B., Deng, Y., Meng, W., Wang, Z., & Tang, T. (2024). Research on digital intelligence business model based on artificial intelligence in post-epidemic era. *Management Decision*, *62*(9), 2937-2957.

Mettler, T. (2024). The connected workplace: Characteristics and social consequences of work surveillance in the age of datification, sensorization, and artificial intelligence. *Journal of Information Technology*, *39*(3), 547-567.

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*, *67*(1), 37-55.

Orhan, Z., Orhan, M., Lund, B. D., Mannuru, N. R., Bevara, R. V. K., & Porter, B. (2025). Artificial intelligence standards in conflict: Local challenges and global ambitions. *Standards*, *5*(4), 27.

Peck Pinheiro, P., & Batista Battaglini, H. (2022). Artificial intelligence and data protection: a comparative analysis of AI regulation through the lens of data protection in the EU and Brazil. *GRUR International*, *71*(10), 924-932.

Qureshi, R., & Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. *Applied Sciences*, *16*(3), 1511.

Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78.

Radanliev, P. (2025). Frontier AI regulation: What form should it take?. *Frontiers in Political Science*, *7*, 1561776.

Rizkia, N. D., & Fardiansyah, H. (2023). *Metode penelitian hukum (normatif dan empiris)*. Penerbit Widina.

Rong, K., Ling, Y., Yang, T., & Huang, C. (2025). Cross-border data transfer: patterns and discrepancies. *Journal of International Business Policy*, *8*(1), 10-32.

Sharma, A. K., & Sharma, R. (2024). Comparative analysis of data protection laws and AI privacy risks in BRICS nations: A comprehensive examination. *Global Journal of Comparative Law*, *13*(1), 56-85.

Tang, M. (2022). The challenge of the cloud: Between transnational capitalism and data sovereignty. *Information, Communication & Society*, *25*(16), 2397-2411.

Theodorakopoulos, L., & Theodoropoulou, A. (2024). Leveraging big data analytics for understanding consumer behavior in digital marketing: A systematic review. *Human behavior and emerging technologies*, *2024*(1), 3641502.

Walter, Y. (2024). Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, *4*(1), 14.

Wang, X., & Xie, F. (2025). Global artificial intelligence governance research in the digital and intelligent era: advances, trends and countermeasures. *Journal of Knowledge Management*.

Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Telecommunications Policy*, *48*(10), 102851.