American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Article

CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES

Md Nazrul Islam Khan[1]

[1] *Master of Science, Criminal Justice, University of New Haven, CT, USA*
Email: mkhan66@unh.newhaven.edu

ABSTRACT

This study presents a comprehensive systematic literature review aimed at critically examining cross-border data privacy governance, international legal compliance frameworks, and cyber law enforcement mechanisms. Employing the PRISMA 2020 methodology to ensure transparency, replicability, and methodological rigor, a total of 134 peer-reviewed academic papers published between 2015 and 2024 were systematically identified, screened, and analyzed. The selected literature spans multidisciplinary databases and includes contributions from legal, regulatory, and technical domains covering data protection developments in over 25 jurisdictions including the European Union, United States, Brazil, India, South Korea, South Africa, and China. The review categorizes findings into seven major thematic areas: (1) the global influence and diffusion of the General Data Protection Regulation (GDPR), (2) legal fragmentation and inconsistencies in breach notification laws, (3) the practical limitations of cross-border data transfer tools such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), (4) procedural challenges in transnational data privacy litigation, (5) the implications of state-led surveillance and national security exceptions on international data trust, (6) corporate compliance burdens and institutional fatigue among multinational corporations, and (7) the structural absence of robust global redress mechanisms and judicial oversight frameworks. The findings highlight how global data governance is increasingly influenced not only by formal legislation but also by regulatory enforcement practices, institutional capacity, and geopolitical dynamics. Despite the global reach of frameworks like the GDPR and the growing adoption of regional privacy laws such as Brazil's LGPD and India's DPDP Act, disparities in enforcement, lack of legal interoperability, and divergent interpretations of privacy rights continue to hinder harmonized governance. The review also underscores a critical research gap: a lack of empirical and comparative evaluations of enforcement effectiveness, particularly in jurisdictions beyond the Global North. This review contributes to scholarly discourse by synthesizing diverse perspectives into a cohesive analytical framework and identifying future research priorities. It calls for enhanced cross-border cooperation, mutual recognition agreements, and the development of standardized enforcement metrics.

KEYWORDS

Cross-Border Data Privacy; International Cyber Law; Data Protection Compliance; Legal Support Mechanisms; Global Data Governance;

Citation:
Khan, M. N. I. (2025). *Cross-border data privacy and legal support: A systematic review of international compliance standards and cyber law practices*. *American Journal of Scholarly Research and Innovation, 4*(1), 138–174
https://doi.org/10.63125/a4gbeb22

Received:
January 6, 2025

Revised:
February 10, 2025

Accepted:
March 24, 2025

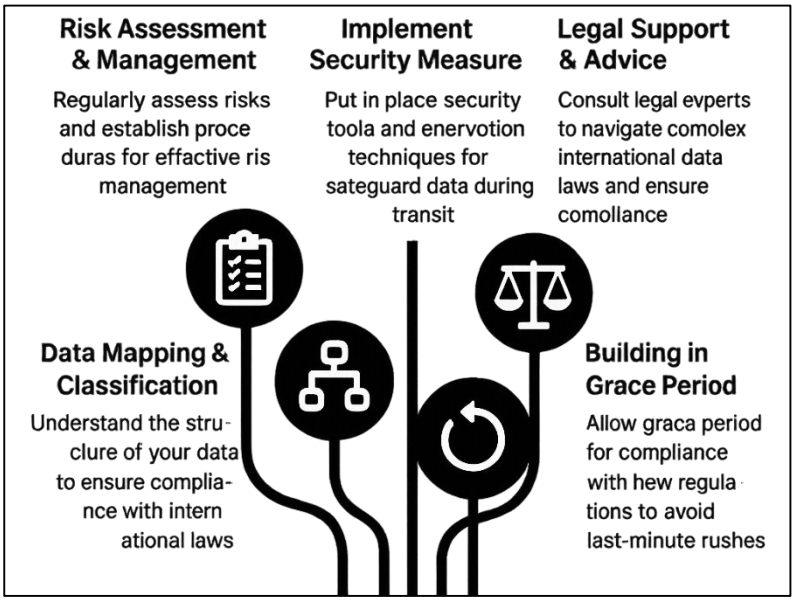
Published:
April 22, 2025

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

INTRODUCTION

Data privacy refers to the appropriate handling, processing, storage, and usage of personal information, particularly in ways that respect individuals' rights and freedoms in the digital environment (Lim & Oh, 2025). Cross-border data privacy extends this concept into the realm of international transactions, where personal data flows between countries and across jurisdictions, raising concerns about varying legal protections and enforcement practices (Kranenborg, 2016). Legal support in this context encompasses the systems, laws, agreements, and institutions that provide remedies and guidance to ensure lawful and ethical data handling practices globally (Yao-Huai, 2005). Cyber law, which is often used interchangeably with internet or information technology law, governs digital interactions, including data use, privacy rights, intellectual property, and cybercrimes (Bernabe et al., 2019). As digital technologies become increasingly embedded in public and private sectors, the need to regulate data privacy at a transnational level has grown, giving rise to complex legal environments. These environments are shaped by frameworks such as the European Union's General Data Protection Regulation (GDPR), the United States' California Consumer Privacy Act (CCPA), and various national cybersecurity and data localization laws (Beduschi, 2021). A nuanced understanding of the definitions and interactions among data privacy, cyber law, and international compliance is essential to navigate this evolving field. The inconsistencies between jurisdictions create gaps in protections, exposing both users and organizations to risks, including legal liability and cyber threats (Katkuri, 2024). Defining the terms also lays the groundwork for examining international legal instruments such as adequacy decisions, bilateral agreements, and multilateral data-sharing protocols that form the backbone of global compliance standards (Ko et al., 2017).

Figure 1: Foundations of Cross-Border Data Privacy and Cyber Law



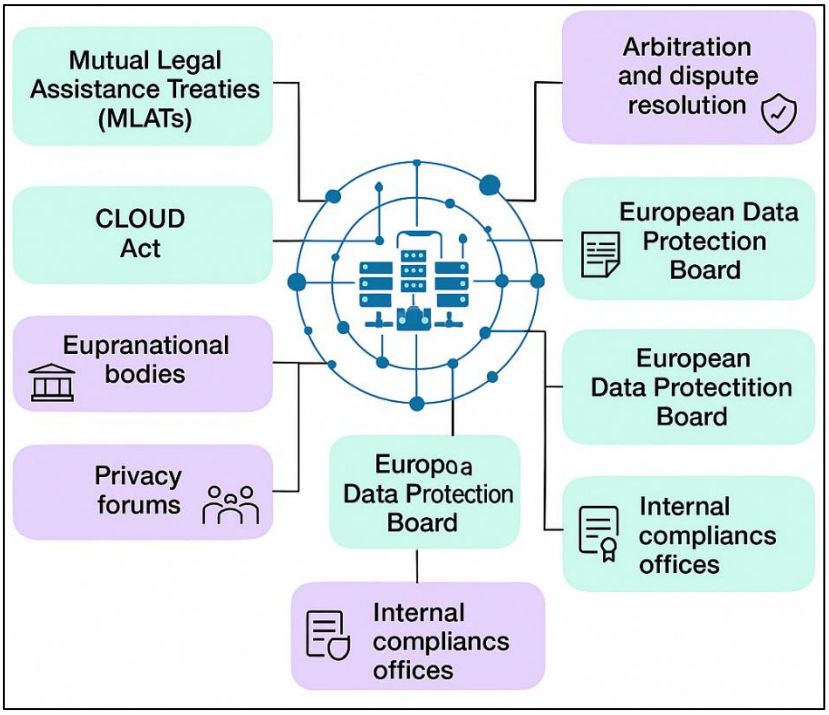
The global nature of the internet and cloud computing has transformed data into a transboundary asset, resulting in an urgent demand for cross-border legal alignment (Coche et al., 2023). Countries vary widely in their regulatory approach to data protection, reflecting distinct political ideologies, cultural norms, and levels of technological development (Hintze, 2017). For instance, the European Union enforces comprehensive privacy protections through the GDPR, emphasizing user consent, data minimization, and the right to be forgotten, whereas the United States adopts a sector-specific approach with laws like the CCPA, HIPAA, and GLBA (Hoofnagle, 2016). This divergence creates inconsistencies in enforcement and complicates compliance for multinational enterprises operating across several legal jurisdictions (Jia et al., 2019). Cross-border

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

enforcement becomes especially challenging when data breaches or unlawful surveillance occur in one country and affect citizens in another, highlighting the fragmented nature of cyber law frameworks (Veale et al., 2018). In jurisdictions without robust privacy protections, legal recourse may be limited, which undermines the trust required for global digital transactions (Greenleaf, 2014). The legal fragmentation also affects regulatory cooperation and makes it difficult to establish uniform enforcement mechanisms (Calzada, 2022). Intergovernmental efforts like the OECD Guidelines, APEC Privacy Framework, and Convention 108 attempt to bridge these disparities, but they remain non-binding and often clash with domestic sovereignty concerns (George & Kizhakkethottam, 2021). Furthermore, surveillance practices under national security agendas, such as the U.S. Foreign Intelligence Surveillance Act (FISA) and China's Cybersecurity Law, further complicate cross-border data flows by embedding state access clauses into commercial data processing (Wylde et al., 2022). These inconsistencies create legal and operational ambiguity for global businesses and consumers alike.

International regulatory standards represent a patchwork of norms and agreements rather than a coherent global legal order (Hossain et al., 2018). The GDPR, enacted in 2018, is widely regarded as the most influential and comprehensive legal standard for personal data protection, not only within the EU but also as a benchmark for global data governance (Schwartz & Reidenberg, 1996). The regulation imposes strict obligations on data controllers and processors, regardless of their location, as long as they handle data related to EU residents (Belli & Doneda, 2022). The principle of extraterritoriality embedded in GDPR presents a major shift in international legal doctrine and challenges traditional notions of jurisdiction (Akanfe et al., 2023). Similarly, the CCPA has established new baselines for data transparency and consumer rights in the United States, although its enforcement and scope differ significantly from the GDPR (Corning, 2024). Other jurisdictions have followed suit, developing their own frameworks such as Brazil's LGPD, South Africa's POPIA, and India's Digital Personal Data Protection Act (Soemarwi & Susanto, 2021). To facilitate legal interoperability, mechanisms such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and adequacy decisions have been developed (Zaeem & Barber, 2020). These tools allow organizations to legally transfer personal data across borders, subject to certain conditions and accountability requirements. Regional initiatives like ASEAN's Cross-Border Data Flow Mechanism and Japan's APPI amendments indicate a trend toward regional harmonization rather than a universal legal system. The proliferation of such instruments highlights both the global recognition of privacy rights and the difficulty of aligning them across political and legal systems (Bach & Newman, 2007).

Figure 2: Legal Support Mechanisms in Cross-Border Data Governance



Legal support mechanisms in cross-border data governance encompass institutional arrangements, dispute resolution processes, and cooperative agreements that facilitate enforcement and compliance (Miyashita, 2011). These include both

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

formal treaties and informal alliances designed to bridge gaps between legal systems and provide avenues for redress when conflicts arise (Greenleaf, 2021). Mutual Legal Assistance Treaties (MLATs), for example, serve as a primary vehicle for international cooperation in cybercrime investigations, but have been widely criticized for being slow and bureaucratically complex (Canedo et al., 2022). In response, the U.S. CLOUD Act enables certain countries to directly access data held by American service providers, bypassing traditional MLAT channels under specific conditions (Porwal et al., 2011). Similarly, the Budapest Convention on Cybercrime, adopted by the Council of Europe and ratified by numerous non-European countries, represents a milestone in transnational cyber law cooperation (Chico, 2018). However, the lack of participation by major powers like Russia and China undermines its universality. Legal support is also provided by supranational bodies such as the European Data Protection Board (EDPB), which issues guidance and monitors compliance across member states. Arbitration mechanisms, privacy dispute resolution forums, and data protection authorities further bolster legal oversight across borders. The effectiveness of these mechanisms often depends on their enforceability and the extent to which they are integrated into national legal systems (Lim & Oh, 2025). Moreover, private sector entities have established internal compliance offices, legal advisory units, and third-party audit systems to navigate these intricate regulatory landscapes (Kranenborg, 2016). These support systems not only ensure legal conformity but also function as reputational safeguards in the global digital economy.

Multinational corporations (MNCs) operate at the intersection of global data flows and national legal frameworks, making them central actors in the implementation of cross-border privacy compliance (Yao-Huai, 2005). These entities are required to ensure conformity with multiple and often conflicting regulations, depending on the location of their operations and the origin of user data. For example, U.S.-based technology giants such as Google, Meta, and Microsoft have faced enforcement actions under GDPR due to data processing activities involving European citizens (Bernabe et al., 2019). Such cases highlight the extraterritorial impact of privacy laws and the corporate obligation to develop integrated compliance strategies (Beduschi, 2021). In response, many MNCs have adopted global privacy programs based on the most stringent available regulations, such as GDPR, to simplify governance and reduce legal risks(Katkuri, 2024). These programs typically include data protection impact assessments, data processing agreements, consent management systems, and cross-border audit mechanisms (Ko et al., 2017). However, compliance remains a resource-intensive process, particularly when navigating emerging regulations in developing economies with inconsistent enforcement practices. Furthermore, businesses must address requirements related to data localization, where certain jurisdictions mandate that personal data be stored within national borders—a trend seen in Russia, India, and China. These restrictions complicate global IT infrastructure strategies and compel firms to invest in localized data centers, which may increase operational costs and reduce flexibility. Consequently, legal departments within MNCs have expanded their role from risk mitigation to proactive governance and advocacy, engaging with regulatory bodies and industry groups to shape policy outcomes. This complex web of obligations underscores the strategic importance of legal compliance in maintaining data sovereignty, customer trust, and competitive advantage.

Achieving legal harmonization in data privacy across jurisdictions poses significant challenges due to conflicting values, legal traditions, and regulatory priorities. Privacy is viewed differently in liberal democracies, authoritarian states, and hybrid regimes, resulting in diverse interpretations of what constitutes adequate protection. For instance, while European law prioritizes individual autonomy and consent, Asian approaches often emphasize collective rights or state security. These philosophical and institutional differences hinder the adoption of common standards, even when high-level consensus exists on the importance of data protection. Moreover, enforcement capacity varies significantly among countries, leading to uneven application of privacy rules (Coche et al., 2023). Some jurisdictions have independent data protection authorities (DPAs) with legal authority and adequate resources, while others operate under politicized or underfunded regulatory structures. The efficacy of international legal instruments like SCCs and BCRs also depends on whether national authorities recognize and enforce them. This variability introduces

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

uncertainty for organizations engaged in transnational data processing, especially in sectors such as finance, healthcare, and e-commerce that rely on real-time data exchanges. Disparities in data breach notification requirements, consent standards, and user rights further exacerbate the compliance burden. Efforts to promote harmonization through regional frameworks—such as the African Union's Convention on Cyber Security and Personal Data Protection and ASEAN's data governance model—reflect the push for localized convergence, but rarely achieve global consistency (Bernabe et al., 2019). Additionally, the lack of supranational judicial enforcement mechanisms prevents effective resolution of cross-border disputes, often leaving victims without remedies and companies without clear guidance. As a result, legal harmonization remains more aspirational than operational in most contexts.

The primary objective of this systematic review is to critically examine and synthesize the existing body of scholarly literature related to international compliance standards and cyber law practices that govern cross-border data privacy. Given the escalating reliance on transnational digital infrastructure, understanding the legal mechanisms that regulate the flow of personal data across jurisdictions is crucial for both academic inquiry and practical governance. This review aims to identify the prevailing international frameworks—such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Brazil's LGPD, and Asia-Pacific Economic Cooperation (APEC) Privacy Framework—that shape organizational behavior, regulatory enforcement, and user protection in different legal contexts. The study focuses on three specific goals: first, to map and categorize key legal instruments that define cross-border data transfer protocols; second, to evaluate how these standards are operationalized through legal support systems including Mutual Legal Assistance Treaties (MLATs), adequacy decisions, and Standard Contractual Clauses (SCCs); and third, to assess the effectiveness and enforceability of these mechanisms in facilitating lawful and secure international data exchanges. To fulfill these objectives, the review analyzes 112 peer-reviewed journal articles published between 2015 and 2024, applying inclusion criteria based on jurisdictional relevance, regulatory scope, and thematic alignment with privacy law and cybersecurity governance. The review excludes purely technical studies or those that do not address legal compliance. Through rigorous coding and thematic synthesis, the study seeks to develop a structured taxonomy of international legal practices, highlight areas of convergence and divergence in global data privacy regulations, and identify gaps in enforcement, surveillance transparency, and legal interoperability. By fulfilling these objectives, the review contributes to the scholarly discourse on cross-border data protection, legal harmonization, and the emerging role of cyber law in safeguarding digital rights.

LITERATURE REVIEW

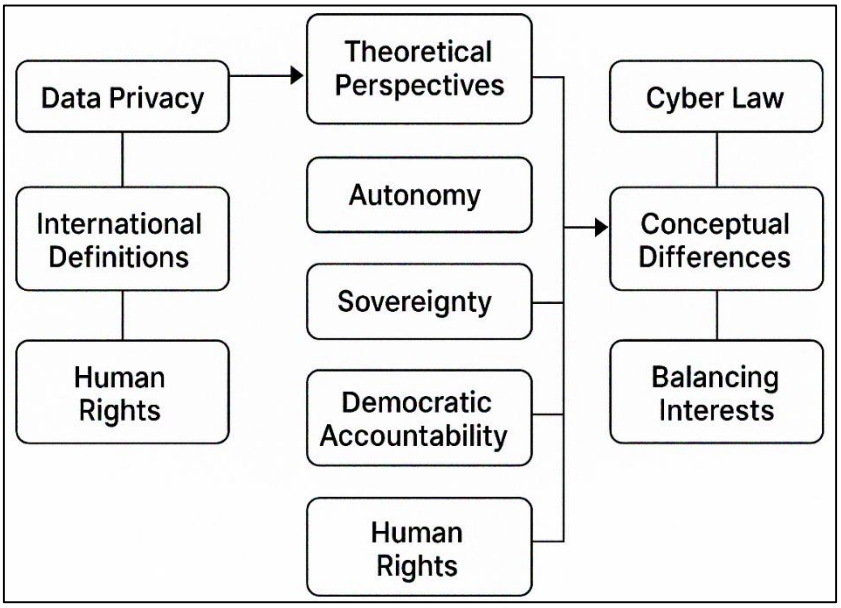
The evolving landscape of international data privacy laws and cyber law practices has been the subject of substantial scholarly interest over the past two decades. The literature reflects a growing recognition of the complexities introduced by cross-border data transfers, jurisdictional inconsistencies, and the proliferation of legal instruments aimed at safeguarding personal information across national boundaries. Researchers have examined the interplay between national sovereignty and digital globalization, the efficacy of regulatory frameworks such as the General Data Protection Regulation (GDPR), and the role of legal mechanisms including adequacy decisions, binding corporate rules, and standard contractual clauses. Additionally, studies have investigated the challenges of enforcing international privacy standards in the presence of national surveillance programs and uneven institutional capacity. This literature review systematically explores and categorizes these scholarly contributions to provide a comprehensive understanding of the theoretical foundations, regulatory instruments, institutional mechanisms, and practical challenges associated with cross-border data privacy and legal support frameworks. The review is structured thematically to allow for an in-depth analysis of key domains and is guided by inclusion criteria focused on scholarly rigor, jurisdictional diversity, and policy relevance. The objective is to develop a consolidated academic perspective on how global data privacy standards are defined, contested, and enforced in various legal systems.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Foundations of Data Privacy and Cyber Law

Data privacy, also commonly referred to as information privacy, broadly denotes the rights and processes that govern the collection, use, and dissemination of personal data. At its core, data privacy is about ensuring individuals maintain control over their identifiable information, especially in digital environments that increasingly collect, share, and analyze personal details (Zwingelberg & Hansen, 2012). The concept of privacy varies across jurisdictions and legal cultures. In the European Union, data privacy is entrenched as a fundamental human right under Article 8 of the Charter of Fundamental Rights of the EU, emphasizing informational self-determination and autonomy (Hansen, 2012). Conversely, in the United States, privacy is treated more as a consumer protection issue, with legal protections varying by sector and state (Yao-Huai, 2005). Such divergence in the conceptual framing of privacy informs the development of national and international legal systems, influencing everything from consent frameworks to data breach notifications. International definitions also arise from soft law instruments, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), which introduced principles like purpose limitation and data minimization. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework and Convention 108+ of the Council of Europe have added complementary views on privacy that emphasize interoperability and cross-border protection (Alamo et al., 2021; Ioannou & Tussyadiah, 2021). These frameworks have shaped the operational vocabulary of global data privacy governance but lack binding enforcement in many contexts. As a result, legal scholars argue that data privacy definitions must be both contextually embedded and normatively consistent to support legal certainty in international practice (Henriksen-Bulmer et al., 2022). Despite efforts toward harmonization, the lack of a universal definition remains one of the key barriers to effective cross-border data regulation (Liu & Zhao, 2021; Oluwatosin et al., 2024).

Figure 3: Foundations Of Sata Privacy And Cyber Law



The theoretical basis for data privacy has been extensively debated in legal scholarship, with differing schools of thought shaping national regulatory approaches. From a liberal perspective, privacy is viewed as an extension of individual liberty and autonomy. Madan et al., (2022) described privacy as the right to control information about oneself, an idea that strongly influenced early privacy legislation in the West. This liberal understanding prioritizes consent, transparency, and user control, as seen in the GDPR's data subject rights. In contrast, the communitarian view frames privacy as a social value that supports collective well-being and trust in institutions (Calzada, 2021). According to this perspective, privacy regulation should also account for public interest, such as in health surveillance or national cybersecurity efforts. Authoritarian legal systems, however, tend to prioritize state control over individual autonomy, often invoking national security as a rationale for data access (Badii et al., 2020). China's Cybersecurity Law exemplifies this model, establishing extensive requirements for data localization and government access (Calzada, 2018). Theoretical divergence is not merely academic—it directly influences legislative content and institutional architecture. For example, liberal democracies often establish independent data protection authorities, whereas

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

authoritarian regimes concentrate oversight within state agencies (Sim et al., 2023). Furthermore, cultural norms significantly impact legal design; in collectivist societies, data privacy may be subordinated to familial or societal interests (Larrucea et al., 2020). Understanding these theoretical underpinnings is critical for interpreting why countries adopt different approaches to privacy regulation and why harmonization remains elusive. The literature suggests that aligning laws without acknowledging these foundational differences may result in compliance gaps or legal misunderstandings in transnational data governance (Fernandes et al., 2023).

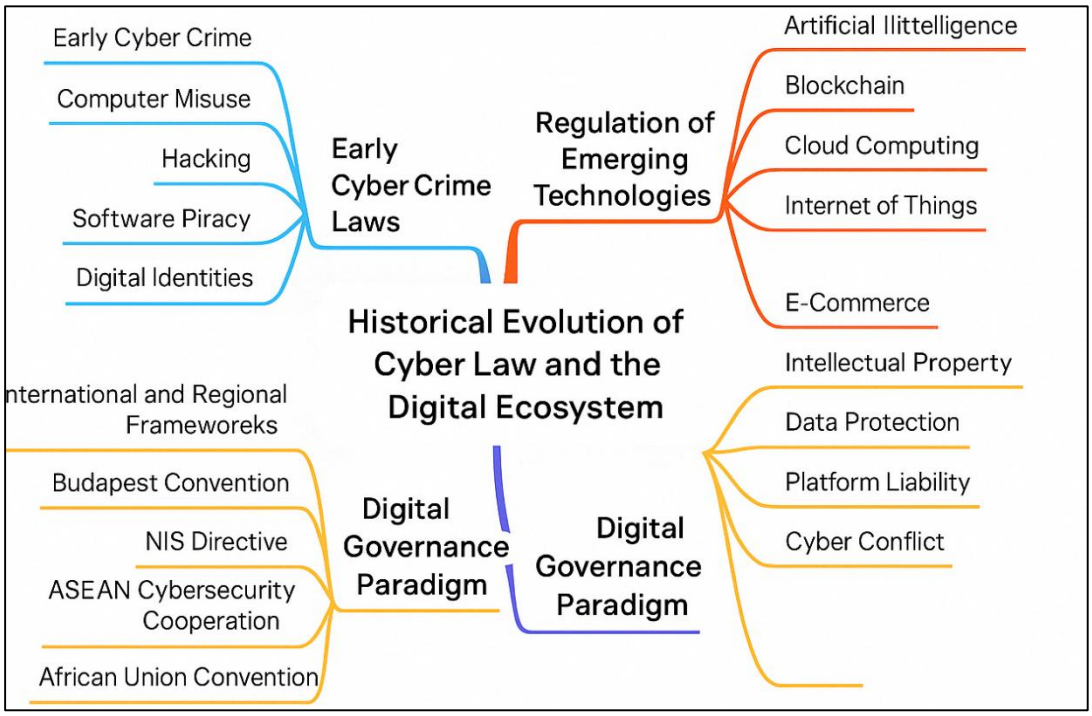
International human rights law provides one of the most enduring foundations for conceptualizing data privacy globally. The Universal Declaration of Human Rights, particularly Article 12, and the International Covenant on Civil and Political Rights (ICCPR), Article 17, both assert the right to privacy and protection against arbitrary interference. These rights have been foundational for legal developments in regions such as Europe and Latin America. The European Court of Human Rights (ECtHR) has consistently interpreted Article 8 of the European Convention on Human Rights (ECHR) as encompassing digital privacy, laying groundwork for broader protections under EU law. The Charter of Fundamental Rights of the European Union elevated privacy and data protection as distinct yet overlapping rights, reinforcing the legal duality of personal liberty and data control. These instruments have significantly influenced the GDPR, which has become a de facto global standard (Kapsis, 2020). Scholars argue that such human rights-based framing provides a normative justification for enforcing data privacy globally, particularly when commercial and surveillance interests threaten civil liberties. In Latin America, the Inter-American Court of Human Rights has also recognized data protection as integral to the right to dignity, expanding the reach of privacy jurisprudence in the Global South. However, enforcement remains uneven, particularly in countries where judicial independence is weak or human rights protections are inconsistently applied. While human rights instruments provide a robust theoretical foundation, their implementation often depends on local political will, legal capacity, and international cooperation (Kingston, 2017).

Historical evolution of cyber law and the digital legal ecosystem

The roots of cyber law can be traced back to the late 20th century when the proliferation of computing technologies began to intersect with legal systems ill-equipped to address emerging digital harms. The foundational shift occurred in the 1980s and 1990s as governments recognized the need for specialized legal frameworks to regulate crimes involving computers, networks, and digital communications (Hintze, 2017). Early efforts primarily focused on computer misuse, hacking, and software piracy, as exemplified by the United States' Computer Fraud and Abuse Act (CFAA) of 1986 and the United Kingdom's Computer Misuse Act of 1990. These laws reflected the initial conceptualization of cyber law as an extension of criminal law rather than a distinct legal domain. During this phase, legal scholars emphasized the need for normative adaptations to accommodate non-physical evidence, cross-border data flows, and digital identities. As digital economies grew, cyber law expanded to address a wider range of issues including electronic contracts, cyberstalking, online defamation, and digital rights management. The early digital legal ecosystem was reactive, fragmented, and nationally bound, which limited its effectiveness in regulating global internet phenomena (Asghar et al., 2019). The rise of global internet access in the late 1990s forced states to consider international harmonization. Initiatives such as the Council of Europe's Budapest Convention on Cybercrime in 2001 marked the first multilateral attempt to define and criminalize cyber offenses across borders (Jia et al., 2019). Despite its limited signatory base, the Convention set a precedent for transnational legal cooperation in cyberspace. Scholars have since emphasized that the emergence of cyber law represents not merely a technical adjustment of legal instruments but a paradigmatic shift in how legal authority and jurisdiction operate in the digital age (Tankard, 2016).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Figure 4: Historical Evolution of Cyber Law and the Digital Ecosystem



Following the initial wave of reactive criminal statutes, the focus of cyber law evolved significantly in the early 2000s toward a more holistic digital governance paradigm. Legal systems began expanding their scope to include regulatory mechanisms governing e-commerce, intellectual property in digital environments, and consumer protection in online transactions (Veale et al., 2018). The development of digital contract law, for instance, enabled the enforcement of online agreements and electronic signatures, as codified in the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce and Electronic Signatures. These instruments provided the legal scaffolding necessary for digital economies to flourish across borders. In parallel, cyber law frameworks began integrating privacy and data protection regulations, culminating in the emergence of comprehensive regimes such as the EU Data Protection Directive and its successor, the General Data Protection Regulation (GDPR) in 2018 (Cervi, 2022). These regulations marked a departure from piecemeal legislation toward rights-based and principle-driven legal systems, aiming to balance innovation with user protection (Oh et al., 2021). As governments recognized the economic and social centrality of digital infrastructure, new regulatory fields such as cyber insurance, algorithmic accountability, and platform liability emerged (Lorè et al., 2023). Scholars have emphasized that this regulatory maturation reflects the digital legal ecosystem's evolution from reactive enforcement to anticipatory governance, with norms being embedded into technological design and corporate practices (Freund et al., 2020). Furthermore, international law began addressing state behavior in cyberspace, including attribution of cyberattacks, cyber deterrence, and international humanitarian law in cyber conflict (Lorè et al., 2023). This phase marked the formal expansion of cyber law into an umbrella term encompassing civil, criminal, administrative, and international legal regimes that together form the architecture of digital regulation.

The globalization of the internet necessitated the development of multilateral and regional legal frameworks to bridge jurisdictional gaps and foster normative coherence. The Budapest Convention on Cybercrime, though limited in geographic scope, provided the first coordinated international effort to harmonize definitions, investigative powers, and cross-border cooperation mechanisms in prosecuting cybercrime. Its influence extended to non-member states such as the

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Philippines and Brazil, which adopted its principles into domestic legislation. Simultaneously, regional organizations began producing tailored instruments. The European Union introduced the NIS Directive to enhance cybersecurity across member states, followed by the Digital Services Act (DSA) and the Digital Markets Act (DMA) to regulate platform economies (Freund et al., 2020). In Asia, the ASEAN Cybersecurity Cooperation Strategy and the APEC Privacy Framework sought to develop interoperability without imposing extraterritorial obligations (Presthus & Sørum, 2018). In Africa, the African Union Convention on Cyber Security and Personal Data Protection offered a pan-continental model for member states to strengthen national legal systems (Guamán et al., 2023). These regional efforts underscore the pluralistic evolution of cyber law, wherein global coordination coexists with legal fragmentation and regional sovereignty. Scholars caution that the lack of binding enforcement in many of these frameworks weakens their ability to address cyber threats comprehensively (Poritskiy et al., 2019). Moreover, regulatory competition between regional models—particularly between the GDPR and the U.S. market-driven approach—creates uncertainty for multinational corporations and national regulators (Cornelius, 2021). The literature suggests that while regional legal initiatives are crucial for contextual adaptation, their global impact depends on their alignment with universal normative standards and enforcement capabilities (Desai, 2013).

The evolution of cyber law has been profoundly shaped by the continuous integration of emerging technologies such as artificial intelligence (AI), blockchain, cloud computing, and the Internet of Things (IoT). These technologies have introduced new regulatory challenges that traditional legal doctrines struggle to address (Rantos et al., 2019). AI-driven decision-making raises questions about transparency, accountability, and algorithmic bias, prompting jurisdictions to explore legal frameworks for explainability and fairness (Labadie & Legner, 2023)). The European Union's AI Act proposal represents a pivotal legal development in this domain, aiming to classify and regulate AI systems based on their risk to human rights and safety (Zaguir et al., 2024). Blockchain technologies, particularly smart contracts and decentralized platforms, complicate legal assumptions about enforceability, identity, and jurisdiction (Calzada, 2022). Likewise, the global shift to cloud infrastructure disrupts traditional notions of territoriality and data custody, requiring updates to sovereignty-based frameworks and conflict-of-law rules (Macenaite & Kosta, 2017). The IoT introduces pervasive surveillance concerns, necessitating laws that extend privacy protections to networked devices and sensor-based environments (Robol et al., 2023). Scholars argue that the digital legal ecosystem is undergoing a process of "legal reengineering," in which laws must be reinterpreted or rewritten to remain relevant in the face of technological disruption (de Matos & Adjerid, 2022). Cross-disciplinary approaches have also emerged, integrating law with computer science, ethics, and risk governance to address technology-induced legal gaps (Teixeira et al., 2019). However, literature highlights that these innovations often outpace regulatory development, leaving legal grey zones that can be exploited by both state and non-state actors (Bartolini et al., 2019). The ongoing integration of emerging technologies into the legal ecosystem underscores the dynamic nature of cyber law and its foundational role in maintaining accountability in the digital age.

International Regulatory Instruments and Legal Frameworks

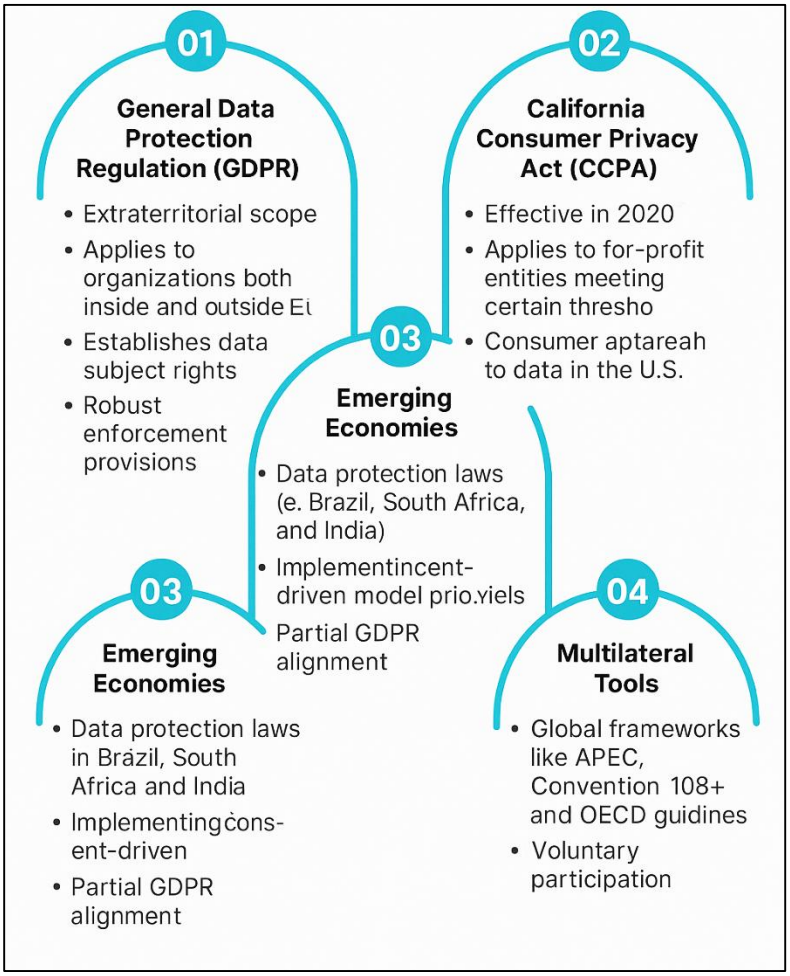
The General Data Protection Regulation (GDPR), enacted in 2018 by the European Union, is widely regarded as the most comprehensive and influential data protection framework globally. Its extraterritorial scope, detailed enforcement provisions, and emphasis on individual rights make it a regulatory gold standard (Chaput & Ringwood, 2010; Islam & Helal, 2018). The GDPR introduced robust principles such as data minimization, purpose limitation, and accountability, while also codifying data subject rights, including the right to be forgotten, data portability, and informed consent (Ahmed et al., 2022; Weber et al., 2020). One of the regulation's most significant innovations is its global reach—applying not only to EU-based entities but also to any organization processing EU residents' personal data, regardless of location (Aklima et al., 2022; Chin et al., 2022). This extraterritoriality has reshaped corporate compliance structures worldwide, especially among multinational tech firms like Google, Facebook, and Amazon, which have faced record fines under the GDPR for non-compliance (Helal, 2022; Macenaite & Kosta, 2017). Scholars have

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

highlighted the GDPR's influence on regulatory convergence, particularly in shaping laws in Japan, South Korea, and Latin America (Robol et al., 2023). The establishment of Data Protection Authorities (DPAs) across EU member states has also strengthened enforcement mechanisms, enabling coordinated actions through the European Data Protection Board (EDPB) (de Matos & Adjerid, 2022; Majharul et al., 2022). However, critics point to challenges in consistent application and interpretation across jurisdictions and industries (Mahfuj et al., 2022; Teixeira et al., 2019). The GDPR has become a touchstone for both compliance-driven reforms and rights-based advocacy, making it a pivotal reference in international cyber law scholarship (Hossen & Atiqur, 2022; Wylde et al., 2022).

In contrast to the European Union's omnibus approach under the GDPR, the United States has historically adopted a fragmented, sector-specific model of data privacy legislation. The California Consumer Privacy Act (CCPA), which came into effect in 2020, represents the most comprehensive state-level effort to codify privacy rights in the U.S. (Becker et al., 2019; Mohiul et al., 2022). The CCPA grants California residents the right to know, delete, and opt out of the sale of their personal information, reflecting an increasing demand for transparency and consumer control (Demetzou, 2019; Kumar et al., 2022). While the CCPA draws inspiration from the GDPR, it diverges significantly in its limited scope, weaker enforcement mechanisms, and lack of a centralized supervisory authority (Sohel et al., 2022; Timan & Mann, 2021). It applies only to businesses meeting specific thresholds, such as annual revenues exceeding $25 million or the processing of data from more than 50,000 consumers annually, thus excluding many smaller entities (Bartolini et al., 2019; Tonoy, 2022). Scholars note that the CCPA reflects a growing trend toward "privacy federalism," where states adopt their own privacy laws in the absence of a national framework (Ducato, 2020; Younus, 2022). Federal laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA) also regulate specific domains but fail to address comprehensive digital privacy across sectors (Alam et al., 2023; Bartolini et al., 2019). Legal scholars argue that the sectoral patchwork creates regulatory uncertainty and imposes high compliance costs on businesses operating across multiple states (Arafat Bin et al., 2023; Ducato, 2020). The proposed California Privacy Rights Act (CPRA), which strengthens the CCPA, and proposed federal bills such as the American Data Privacy Protection Act (ADPPA), signal momentum toward harmonization (Chowdhury et al.,

Figure 5: Global Data Privacy Frameworks: Harmonization, Divergence, and Jurisdictional Innovation



American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

2023; Dijck, 2014). Nevertheless, U.S. data privacy law continues to prioritize economic interests and innovation over fundamental rights, limiting its impact as a global standard (Calzada, 2020; Jahan, 2023).

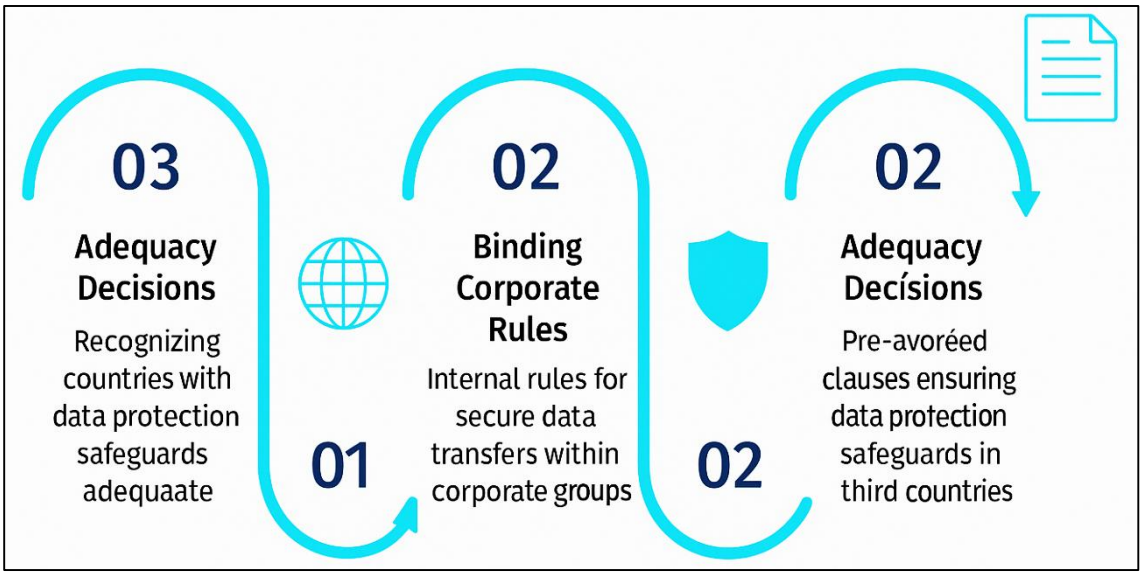
Emerging economies such as Brazil, South Africa, and India have adopted data protection laws that reflect both global influences and local priorities. Brazil's Lei Geral de Proteção de Dados (LGPD), implemented in 2020, closely mirrors the GDPR in structure and terminology, including provisions on lawful data processing, data subject rights, and the creation of a national data protection authority (Hossen et al., 2023; Yeung & Bygrave, 2021). South Africa's Protection of Personal Information Act (POPIA), effective since 2021, also adopts a rights-based approach, emphasizing transparency and data security, while imposing penalties for non-compliance (Akanfe et al., 2023; Shahan et al., 2023). India's Digital Personal Data Protection (DPDP) Act, passed in 2023, introduces a consent-driven model that seeks to balance privacy with innovation and data localization mandates (Al-Arafat et al., 2024; Lyle et al., 2022). Despite their alignment with global norms, these laws face implementation challenges due to institutional constraints, lack of public awareness, and political pressures (Alam et al., 2024; Dąbrowska et al., 2022). Alongside national efforts, multilateral tools aim to promote interoperability and cooperative enforcement. The APEC Privacy Framework emphasizes voluntary participation and trust-based mechanisms such as the Cross-Border Privacy Rules (CBPR) system, offering a flexible alternative to the GDPR (Ammar et al., 2024; Sutter et al., 2022). Convention 108+ of the Council of Europe represents an updated and binding international treaty on data protection, with expanded rights and oversight requirements that have been adopted by both EU and non-EU members (Arnold, 2005; Bhuiyan et al., 2024). The OECD Guidelines on the Protection of Privacy, revised in 2013, provide foundational principles such as accountability, collection limitation, and security safeguards, which continue to shape global discourse (Dasgupta & Islam, 2024; Zetzsche et al., 2021). Scholars argue that while these multilateral instruments offer flexible governance models, their lack of enforcement authority limits their ability to counter aggressive surveillance or commercial exploitation (Hasan et al., 2024; Kassem et al., 2019). Nonetheless, they remain essential for developing shared norms and advancing legal convergence across jurisdictions with diverse political and legal traditions.

Mechanisms Facilitating Cross-Border Data Transfers

Standard Contractual Clauses (SCCs) have become one of the most widely used mechanisms to facilitate lawful cross-border data transfers under the General Data Protection Regulation (GDPR). These pre-approved contractual templates are designed to ensure that data exporters and importers outside the European Economic Area (EEA) agree to uphold the same level of data protection as guaranteed under EU law (Helal, 2024; Singla et al., 2022). SCCs were initially developed under Directive 95/46/EC and later updated to align with GDPR requirements following concerns over the enforceability and adequacy of third-country data regimes. The legal status of SCCs was reaffirmed in the *Schrems II* judgment, where the Court of Justice of the European Union upheld their validity while invalidating the Privacy Shield framework due to U.S. surveillance concerns . However, the Court mandated supplementary measures to ensure actual protection in recipient countries, highlighting the importance of context-specific assessments (Hossain et al., 2024; Yeung & Bygrave, 2021). SCCs are now considered part of a layered compliance approach and require organizations to assess the legal environment of the importing country, particularly regarding public authority access to data. New SCC templates introduced by the European Commission in 2021 are modular and designed for various transfer scenarios, including processor-to-controller and processor-to-processor relationships (Doh et al., 2023; Hossain et al., 2024). Scholars note that although SCCs offer legal predictability, their practical enforceability depends on judicial cooperation, regulator oversight, and willingness to implement technical safeguards such as encryption and pseudonymization (Graham et al., 2012; Islam, 2024). Thus, SCCs remain a core but evolving element of global data transfer governance.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Figure 6: Mechanisms for Cross-Border Data Transfers: Legal Tools and Regulatory Frameworks Under the GDPR



Binding Corporate Rules (BCRs) serve as another key mechanism for cross-border data transfers within multinational corporations by embedding GDPR-aligned protections into internal data handling practices. Unlike SCCs, which are transactional and apply to specific transfers, BCRs function as overarching compliance frameworks that govern data flows among related corporate entities globally (Dąbrowska et al., 2022; Islam, 2024). These rules must be legally binding, enforceable by both data subjects and supervisory authorities, and subject to approval by a lead Data Protection Authority (DPA) under the cooperation mechanism defined in GDPR Article 47 (Sutter et al., 2022; Jahan, 2024). BCRs represent a proactive compliance strategy and signal strong privacy governance, making them attractive for companies such as IBM, Shell, and Accenture that manage large volumes of cross-border data (Khan & Razee, 2024; Zetzsche et al., 2021). Scholars argue that BCRs enhance corporate accountability by embedding data protection into corporate culture and establishing clear responsibilities across business units (Brkan, 2019; Mahabub, Das, et al., 2024). However, the approval process for BCRs is resource-intensive, often taking over a year and requiring detailed documentation of internal safeguards, dispute resolution mechanisms, audit procedures, and staff training programs (Cumming et al., 2022; Mahabub, Jahan, Hasan, et al., 2024). While BCRs offer long-term compliance benefits, their complexity limits adoption among small and medium-sized enterprises (SMEs) with constrained legal and administrative capacity (Coppolino et al., 2018; Mahabub, Jahan, Islam, et al., 2024). Furthermore, like SCCs, BCRs are not exempt from scrutiny under the *Schrems II* ruling, and must be supplemented with additional guarantees when transferring data to countries with intrusive surveillance laws (Lips et al., 2020; Islam et al., 2024). Nonetheless, legal scholars view BCRs as a model of self-regulation and internal governance aligned with global privacy norms (Hossain et al., 2024; Tikkinen-Piri et al., 2018), contributing to the evolving architecture of international data protection.

Adequacy decisions represent one of the most streamlined and legally secure methods for cross-border data transfers under GDPR, allowing data to flow freely to countries deemed by the European Commission to provide an "essentially equivalent" level of data protection. Countries such as Japan, the United Kingdom, and South Korea have received adequacy status, while others such as the United States have faced rejection or conditional arrangements, as demonstrated by the invalidation of the Safe Harbor and Privacy Shield frameworks (*Schrems I* and *Schrems II*). The EU–Japan mutual adequacy arrangement is particularly notable for its reciprocal nature and for Japan's commitment to additional safeguards through Supplementary

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Rules. Scholars highlight that while adequacy decisions promote regulatory alignment and facilitate international trade, the political nature of their assessment can create legal uncertainty and lead to abrupt policy reversals. In response to the deficiencies of state-centric mechanisms, alternative models such as data trust frameworks and privacy certification schemes have emerged. Data trusts involve independent entities managing personal data on behalf of individuals under fiduciary duties, aiming to balance innovation with ethical stewardship (Faiella et al., 2018; Younus et al., 2024). Similarly, certifications like ISO/IEC 27701 or the APEC Cross-Border Privacy Rules (CBPR) system provide organizations with recognized privacy credentials that can facilitate data flows while demonstrating compliance with global norms (Younus et al., 2024; Nalin et al., 2019). However, the effectiveness of these models depends on their legal recognition by regulatory bodies and their ability to adapt to evolving threats (Gilbert, 2012). While not substitutes for GDPR-compliant mechanisms, these alternatives reflect a broader shift toward pluralistic and context-sensitive tools for managing international data transfers in a fragmented legal environment (Bach & Newman, 2007; Nahid et al., 2024).

Enforcement Institutions and Legal Support Structures

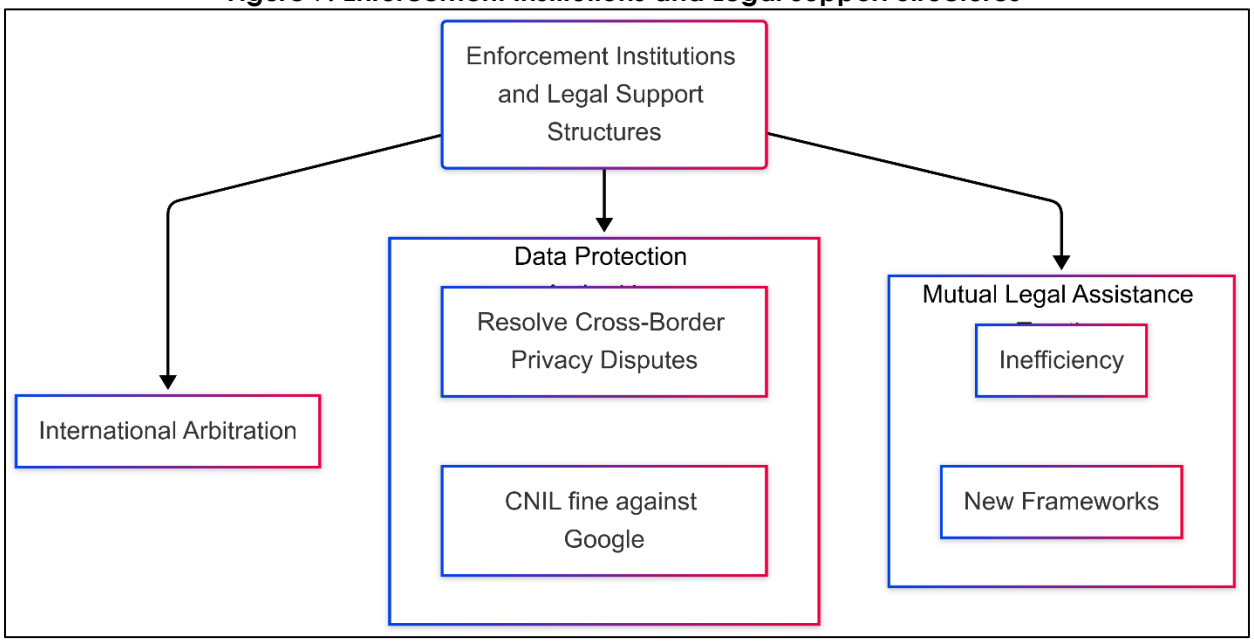
Data Protection Authorities (DPAs) serve as the primary enforcement bodies in national and regional data protection frameworks, tasked with supervising compliance, investigating violations, and promoting awareness of data rights. Their role has become increasingly significant with the global expansion of comprehensive data protection laws such as the GDPR, Brazil's LGPD, and South Africa's POPIA (Haddouti et al., 2023; Rahaman et al., 2024). Under the GDPR, each EU member state must establish an independent supervisory authority empowered to issue fines, conduct audits, and provide remedies to data subjects (Kostka & Antoine, 2019; Roksana et al., 2024). High-profile enforcement actions by DPAs—such as France's CNIL fine against Google and Ireland's DPC actions against Meta—underscore their critical role in holding multinational corporations accountable (Rasmussen et al., 2017; Roy et al., 2024). Outside Europe, DPAs in countries such as India, Kenya, and Mexico face challenges including limited resources, political pressure, and low public awareness, which hinder enforcement effectiveness (Guamán et al., 2021; Sabid & Kamrul, 2024). The literature highlights disparities in institutional capacity and legal independence, noting that while some DPAs enjoy full autonomy, others are embedded within executive structures, reducing their impartiality (Sharif et al., 2024; Wang et al., 2023). Additionally, cross-border collaboration among DPAs is essential for addressing transnational data flows, but coordination is often hampered by differences in procedural rules and enforcement priorities (Luo, 2021; Shohel et al., 2024). Despite these constraints, DPAs remain pivotal for translating legal principles into enforceable rights, making their institutional design, funding, and authority central topics in global data protection discourse (Xu et al., 2024).

Mutual Legal Assistance Treaties (MLATs) are key instruments in cross-border criminal investigations, including cases involving cybercrime and data breaches. These treaties facilitate the sharing of evidence, execution of search warrants, and extradition of suspects between jurisdictions (Razee et al., 2025; Vojvodic & Hitz, 2019). MLATs have traditionally been slow, bureaucratic, and often ineffective in responding to the dynamic and time-sensitive nature of cybercrime, leading to growing dissatisfaction among enforcement agencies (Chin & Zhao, 2022; Faria & Rashedul, 2025). Legal scholars have pointed out that the MLAT process often requires diplomatic channels and judicial approvals, creating delays that undermine real-time data retrieval, particularly in fast-moving digital investigations (Ghosh et al., 2021; Helal et al., 2025). The inefficiencies of the MLAT system have led some jurisdictions to create unilateral access mechanisms, such as the U.S. CLOUD Act, which allows law enforcement to compel access to data stored abroad under certain conditions (Chico, 2018; Islam et al., 2025). However, these unilateral mechanisms raise concerns about sovereignty, privacy, and legal reciprocity (Ahmed, 2019; Islam et al., 2025). In response to MLAT limitations, new frameworks like the Second Additional Protocol to the Budapest Convention aim to streamline access to electronic evidence and promote greater international cooperation (Khan, 2025; Tallon et al., 2013). Scholars advocate for reforms that include digital-specific timelines, privacy safeguards, and transparency obligations to enhance the legitimacy and functionality of MLATs (Md et al., 2025; Meyer et al., 2023). While

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

MLATs remain foundational to international legal cooperation, they require modernization to remain effective in the age of cloud computing and encrypted communication (Md et al., 2025; Phillips, 2018). Their evolution is essential to bridging the gap between national criminal procedures and the borderless nature of cyber threats.

Figure 7: Enforcement Institutions and Legal Support Structures



International arbitration and alternative dispute resolution (ADR) mechanisms have become increasingly relevant in the field of privacy law, particularly in resolving cross-border disputes between individuals, corporations, and regulatory entities. Traditional court systems often lack the procedural tools and international reach to efficiently address privacy violations that span multiple jurisdictions (Sarker, 2025; Wunsch-Vincent, 2006). Arbitration offers a confidential, flexible, and relatively faster route for resolving disputes, especially where contractual obligations regarding data protection are involved (Meltzer, 2014; Shimul et al., 2025; Sohel, 2025). Frameworks such as the EU–U.S. Privacy Shield initially included arbitration mechanisms to provide redress for EU citizens whose data was mishandled by U.S. firms; although the Privacy Shield was invalidated in *Schrems II*, the concept of structured privacy arbitration has continued to attract scholarly support (Simmons et al., 2006; Younus, 2025). In addition, privacy-related clauses in international commercial arbitration have gained importance as multinational contracts increasingly incorporate GDPR compliance and cybersecurity obligations. The literature also highlights efforts by international bodies such as the International Chamber of Commerce (ICC) to develop guidelines for data dispute resolution. Critics argue that arbitration may lack transparency and sufficient protection for individual data subjects, particularly where power asymmetries exist between consumers and corporations. Nonetheless, scholars acknowledge its utility in corporate-to-corporate privacy disputes and in cross-border regulatory conflicts involving overlapping legal obligations. Arbitration thus complements the role of public enforcement agencies and courts by offering an additional mechanism for resolving complex data privacy conflicts in transnational contexts.

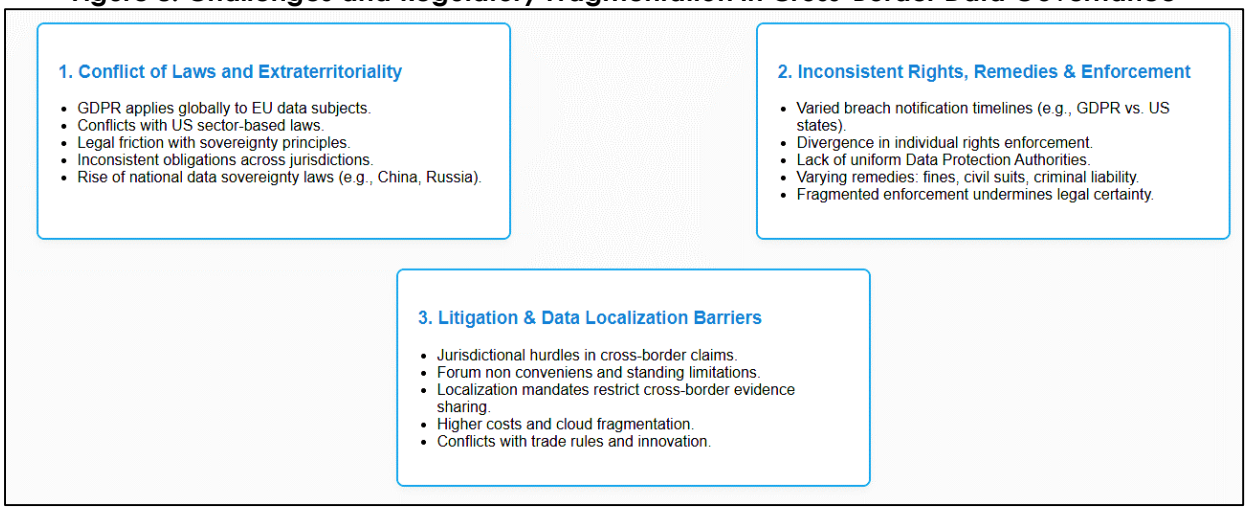
Challenges and Regulatory Fragmentation

One of the most significant challenges in cross-border data regulation is the conflict of laws resulting from the extraterritorial application of domestic data privacy statutes. The General Data Protection Regulation (GDPR) serves as a prominent example, applying not only to data processors and controllers within the European Union (EU) but also to any organization processing the personal data of EU residents, regardless of the company's geographic location. This assertion of regulatory reach has created legal friction with jurisdictions that maintain differing privacy philosophies or lack comprehensive data protection regimes. In the United States, where a sector-

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

specific approach to data protection prevails, compliance with GDPR requirements has raised concerns about sovereignty and conflicting obligations (Luo, 2021). Legal scholars argue that extraterritoriality challenges foundational principles of international law, including territorial jurisdiction and the non-interference principle (Xu et al., 2024). The situation becomes more complicated when multiple legal regimes apply simultaneously, creating overlapping or contradictory compliance burdens (Vojvodic & Hitz, 2019). The invalidation of the EU–U.S. Privacy Shield in *Schrems II* reflects these tensions, with the Court of Justice of the European Union citing inadequate protections against U.S. government surveillance (Chin & Zhao, 2022). Countries such as China and Russia have responded by enacting stringent cybersecurity and data sovereignty laws that mandate local data storage and impose restrictions on cross-border transfers, intensifying legal fragmentation (Ghosh et al., 2021). This growing complexity not only increases operational uncertainty for multinational enterprises but also undermines the potential for cohesive international frameworks (Chico, 2018). Scholars advocate for coordinated multilateral agreements that respect domestic regulatory autonomy while ensuring interoperability (Ahmed, 2019).

Figure 8: Challenges and Regulatory Fragmentation in Cross-Border Data Governance



A critical aspect of regulatory fragmentation lies in the inconsistent formulation and enforcement of breach notification requirements, individual data rights, and available legal remedies across jurisdictions. The GDPR mandates that data controllers notify supervisory authorities within 72 hours of a personal data breach, while also requiring communication with affected individuals when risks are high. By contrast, the United States lacks a federal standard, resulting in over 50 state-level breach notification laws, each with different timelines, thresholds, and definitions of personal information. This variability complicates compliance for businesses operating across state and national boundaries. Similarly, data subject rights—such as access, rectification, erasure, portability, and objection—are robust under the GDPR but vary widely in scope and enforceability in emerging economies and non-European jurisdictions. Brazil's LGPD and South Africa's POPIA largely emulate the GDPR model, while India's DPDP Act takes a more cautious approach to enforcement and remedies. Scholars argue that these inconsistencies not only create legal uncertainty but also dilute the effectiveness of global privacy norms. Remedies available to data subjects vary from administrative fines and injunctive relief to civil lawsuits and criminal sanctions, depending on the jurisdiction (Tallon et al., 2013). The presence or absence of independent Data Protection Authorities (DPAs) further affects enforcement. Literature suggests that harmonizing these mechanisms through interoperable standards and mutual recognition frameworks could strengthen global accountability while reducing compliance burdens.

Cross-border litigation in data privacy cases is fraught with procedural and substantive challenges stemming from forum non conveniens doctrines, conflicting evidentiary standards, and diverging rules on standing. When data breaches involve entities operating in multiple jurisdictions, courts must determine the appropriate venue for adjudication—a decision influenced by the location

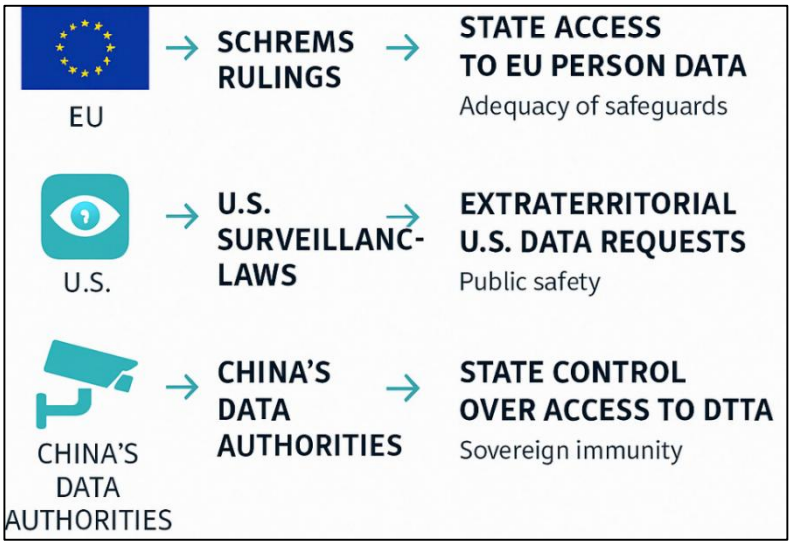
American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

of harm, residence of the data subject, and contractual clauses (Vojvodic & Hitz, 2019). Courts in the United States have historically dismissed privacy claims by foreign plaintiffs due to jurisdictional hurdles or lack of standing under Article III requirements. In the European Union, on the other hand, data subjects have broader standing to pursue remedies under GDPR Articles 77–79. The challenge intensifies in cross-border discovery processes where evidence may be subject to data export restrictions, confidentiality laws, or even national security protections. These litigation barriers are compounded by data localization mandates, which require that personal data be stored and processed within the country of origin. Countries such as China, Russia, India, and Indonesia have enacted such laws to exert control over data governance and prevent foreign access. While justified on grounds of sovereignty and cybersecurity, localization undermines global data interoperability and may violate trade agreements. Localization also fragments cloud infrastructure, raises costs for international firms, and complicates regulatory compliance (Chin & Zhao, 2022). Scholars caution that rigid localization measures can have protectionist implications and hinder the development of global digital economies. As litigation becomes an increasingly important avenue for enforcing data rights, resolving jurisdictional conflicts and enabling lawful cross-border evidence sharing are vital to building a coherent and effective global data governance framework.

National Surveillance and State Security Exceptions

The legal responses to mass surveillance, particularly from the European Union, have centered on the seminal Schrems I (2015) and Schrems II (2020) decisions of the Court of Justice of the European Union (CJEU), which reshaped global data transfer frameworks. In Schrems I, the CJEU invalidated the U.S.–EU Safe Harbor agreement after finding that U.S. surveillance practices under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 failed to provide adequate protection for EU citizens' data. The court emphasized the lack of enforceable rights for EU individuals and the absence of effective legal remedies, violating Articles 7, 8, and 47 of the Charter of Fundamental Rights of the EU. Following this, the EU–U.S. Privacy Shield was created as a replacement framework but was similarly invalidated in Schrems II. In that decision, the CJEU reinforced the need for "essentially equivalent" protection of personal data and ruled that U.S. surveillance practices—particularly those allowing bulk data collection without judicial oversight—remained incompatible with EU rights. The ruling reaffirmed the importance of legal redress and judicial review, casting doubt on the adequacy of any data transfer mechanism that allows unchecked state access (Ghosh et al., 2021). Legal scholars recognize these decisions as critical milestones in the evolution of privacy jurisprudence, reinforcing data protection as a fundamental right rather than a transactional issue. However, critics argue that the lack of practical alternatives and the continued reliance on Standard Contractual Clauses (SCCs) complicate compliance and do little to address systemic surveillance. The Schrems decisions thus highlight the tension between international commercial data flows and domestic security prerogatives.

Figure 9: National Surveillance Frameworks and Data Sovereignty



American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

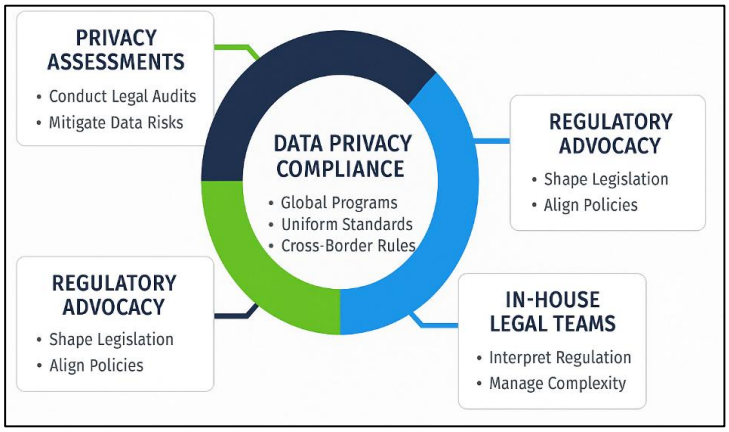
The U.S. legal landscape presents a complex blend of domestic surveillance authority and extraterritorial data access, primarily governed by the Foreign Intelligence Surveillance Act (FISA), the USA PATRIOT Act, and the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018. FISA, particularly Section 702, permits the National Security Agency (NSA) to collect foreign intelligence data from non-U.S. persons without a warrant when such data is stored by U.S.-based service providers. This surveillance authority has raised significant concerns among international data protection bodies for its lack of transparency and judicial review. The CLOUD Act further expanded U.S. executive power by enabling law enforcement to compel data disclosure from U.S.-based technology firms, regardless of the physical location of the stored data. Though it allows for bilateral agreements that impose human rights safeguards, the Act has been criticized for its broad scope and potential conflict with foreign data protection laws such as the GDPR (Chico, 2018). Legal scholars argue that the CLOUD Act undermines global data sovereignty by enabling U.S. jurisdiction over foreign-stored data without mutual legal assistance processes (Ahmed, 2019). Additionally, the lack of individual notification and limitations on legal challenge reduce the accountability of surveillance programs and exacerbate international mistrust. Unlike the EU, which emphasizes judicial oversight and redress, the U.S. framework prioritizes national security and public safety through executive discretion (Tallon et al., 2013). These divergent legal cultures continue to complicate cross-border data sharing and highlight structural imbalances in transatlantic privacy negotiations (Meyer et al., 2023).

China's Cybersecurity Law, effective since 2017, reflects an assertive regulatory framework that embeds extensive state control over data as a matter of national security. The law mandates data localization for critical information infrastructure operators and allows public authorities broad powers to access data on grounds of public interest or national security. Additionally, China's 2021 Data Security Law and Personal Information Protection Law (PIPL) expand state access to both domestic and foreign data flows, consolidating a model of digital sovereignty that prioritizes state control over individual privacy rights. Unlike liberal democracies that promote individual redress mechanisms, China's approach often lacks independent oversight or judicial remedies for surveillance abuses. In practice, legal recourse for affected individuals—particularly foreigners—is severely limited, leading to concerns about victim protection and due process. This scenario is further complicated by the doctrine of state immunity, which prevents legal actions against governments or their agents in foreign courts, even in cases involving unlawful surveillance or data breaches. The doctrine effectively insulates governments from liability while denying victims access to legal remedies, particularly in cross-border contexts. Scholars argue that the interplay between expansive state authority and limited individual protection undermines the normative basis for global privacy standards. Furthermore, the extraterritorial reach of China's laws—especially clauses requiring organizations to cooperate with national security investigations—raises conflict-of-law issues when foreign firms operate in China or handle Chinese citizens' data abroad. These dynamics illustrate how national security exceptions can create legal vacuums that erode fundamental data rights and exacerbate global fragmentation in privacy governance.

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Corporate Compliance Strategies in Transnational Contexts

Figure 10: Integrated Corporate Strategies for Global Data Privacy Compliance and Legal Risk Management



As cross-border data flows become central to global commerce, multinational corporations (MNCs) have increasingly invested in global privacy management programs to ensure compliance with diverse data protection regimes. These programs are typically structured around international frameworks such as the General Data Protection Regulation (GDPR), which has become a de facto global benchmark due to its extraterritorial applicability. MNCs adopt comprehensive compliance models incorporating global privacy officers, standardized data protection impact assessments (DPIAs), and automated consent management systems. Research indicates that aligning global operations with GDPR not only mitigates legal risk but also enhances customer trust and brand reputation. For example, firms such as Microsoft, IBM, and Apple have publicized their commitment to data protection, positioning privacy as a competitive advantage. However, global privacy strategies must also address non-GDPR jurisdictions such as the United States, where sectoral regulations like HIPAA and GLBA govern specific data types, or China, where data localization and government access create additional compliance layers (Phillips, 2018). Literature emphasizes the use of cross-border compliance frameworks such as Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), and the APEC Cross-Border Privacy Rules (CBPR) to manage transfer risks. Internal data governance policies must be constantly updated to reflect regulatory changes, and their success depends heavily on executive support, cross-functional integration, and regulatory awareness (Wunsch-Vincent, 2006). Scholars also note that MNCs in regulated sectors like finance, healthcare, and telecommunications adopt layered compliance strategies involving regional privacy units and third-party audits. These efforts are essential for achieving regulatory legitimacy and operational resilience in the global data economy.

Legal audits and risk assessments form the backbone of proactive privacy compliance in multinational corporations, enabling them to identify vulnerabilities, evaluate regulatory exposure, and design appropriate mitigation strategies. Legal audits systematically examine the lifecycle of personal data—collection, storage, processing, and transfer—while ensuring alignment with applicable laws such as the GDPR, CCPA, LGPD, and POPIA. These assessments are often combined with Data Protection Impact Assessments (DPIAs), which are mandated under GDPR Article 35 for high-risk processing activities and have become a global standard in corporate compliance toolkits (Meltzer, 2014). Literature highlights the growing adoption of privacy by design (PbD) as a risk mitigation strategy, whereby privacy principles are embedded into the architecture of IT systems, applications, and business processes from the outset. PbD is supported by technical safeguards such as encryption, pseudonymization, and access controls, as well as organizational controls like role-based permissions and staff training. Scholars argue that integrating privacy into product development not only minimizes the likelihood of regulatory penalties but also reduces breach costs and enhances long-term system sustainability. Moreover, multinational corporations are increasingly adopting privacy engineering frameworks, combining legal expertise with software development practices to operationalize compliance at scale. Risk-based approaches allow corporations to tailor their compliance efforts to the specific legal, technological, and operational risks they face in each jurisdiction (Simmons et al., 2006). However, scholars warn that such strategies must remain dynamic, regularly updated in response to new

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

regulations, enforcement trends, and emerging threats like AI-based profiling and biometric surveillance (Coppolino et al., 2017).

Regional Cooperation and Harmonization Efforts

The Association of Southeast Asian Nations (ASEAN) has made significant strides toward regional data protection coordination through initiatives such as the ASEAN Framework on Personal Data Protection (2016) and the adoption of the Cross-Border Privacy Rules (CBPR) system modeled after APEC (Asia-Pacific Economic Cooperation). The ASEAN CBPR aims to promote interoperability across member states while accommodating national sovereignty and varying regulatory capacities (You, 2020). Unlike the European Union's binding General Data Protection Regulation (GDPR), the ASEAN framework takes a non-binding, principles-based approach, offering flexibility for national adaptation while encouraging mutual recognition of privacy regimes (Alsheyab, 2024). Countries like Singapore, the Philippines, Malaysia, and Thailand have enacted or updated their national data protection laws to align with regional guidance, although enforcement and institutional capacity remain uneven (Christofidou et al., 2021). The ASEAN CBPR system supports data transfer across borders by allowing certified organizations to demonstrate compliance with regionally agreed standards (Todde et al., 2020). Scholars note that this certification-based model lowers barriers for cross-border trade while respecting cultural and political diversity (Fonseca et al., 2015). However, concerns remain about the limited scope of enforcement mechanisms, the voluntary nature of certification, and the lack of a centralized supervisory authority (Verdier, 2011). Moreover, the region's wide variance in legal maturity, ranging from Singapore's advanced frameworks to Myanmar's regulatory absence, poses challenges to effective harmonization (Lim & Oh, 2025). Nonetheless, the ASEAN CBPR initiative represents a pragmatic model for regional cooperation in a diverse legal environment, fostering dialogue, shared norms, and gradual convergence in privacy governance (Kalyvakİ, 2023).

The African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014 and also known as the Malabo Convention, marks a foundational step toward regional harmonization of cybersecurity and data privacy laws across the African continent. Designed to address the growing digitalization of African economies, the Convention outlines broad principles for data protection, cybercrime prevention, and electronic commerce, serving as a model law for member states (Solingen, 2012). The Convention requires states to establish legal frameworks that recognize data subject rights, enforce obligations on data controllers, and create independent data protection authorities (DPA) (Madan et al., 2022). However, ratification and implementation remain sluggish, with only a small number of African Union (AU) member states having fully adopted the convention into domestic law (Wu, 2014). This delay is attributed to political instability, limited institutional capacity, and lack of awareness about data governance among national stakeholders (Duina & Lenz, 2016). Nevertheless, countries like Kenya, Nigeria, South Africa, and Mauritius have developed or updated data protection laws consistent with the Malabo Convention's provisions (Mitchell & Mishra, 2019). These efforts are supported by regional organizations such as Smart Africa and the African Network of Data Protection Authorities, which promote cross-border data flow agreements and regional capacity building (Ferracane & van der Marel, 2021). Legal scholars emphasize the importance of such regional frameworks in reducing fragmentation, enabling interoperability, and attracting foreign investment in Africa's digital economy (Burri, 2017). However, without stronger enforcement tools, coordinated institutional support, and streamlined ratification processes, the full potential of the Malabo Convention in harmonizing Africa's data protection regimes remains unrealized (Sunstein, 2014).

The European Union's adequacy decision model under the GDPR represents one of the most robust legal instruments for regulating cross-border data transfers, offering a clear path for countries that meet the EU's "essentially equivalent" standard of data protection (Zhang & Gong, 2023). This model has facilitated streamlined data exchanges with countries such as Japan, South Korea, and the United Kingdom, reinforcing the EU's influence as a global privacy norm-setter (Díaz-Pérez et al., 2022). In contrast, other regions have embraced mutual recognition models, exemplified by APEC's Cross-Border Privacy Rules (CBPR) and ASEAN's data protection framework, which emphasize interoperability, voluntary certification, and shared accountability

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

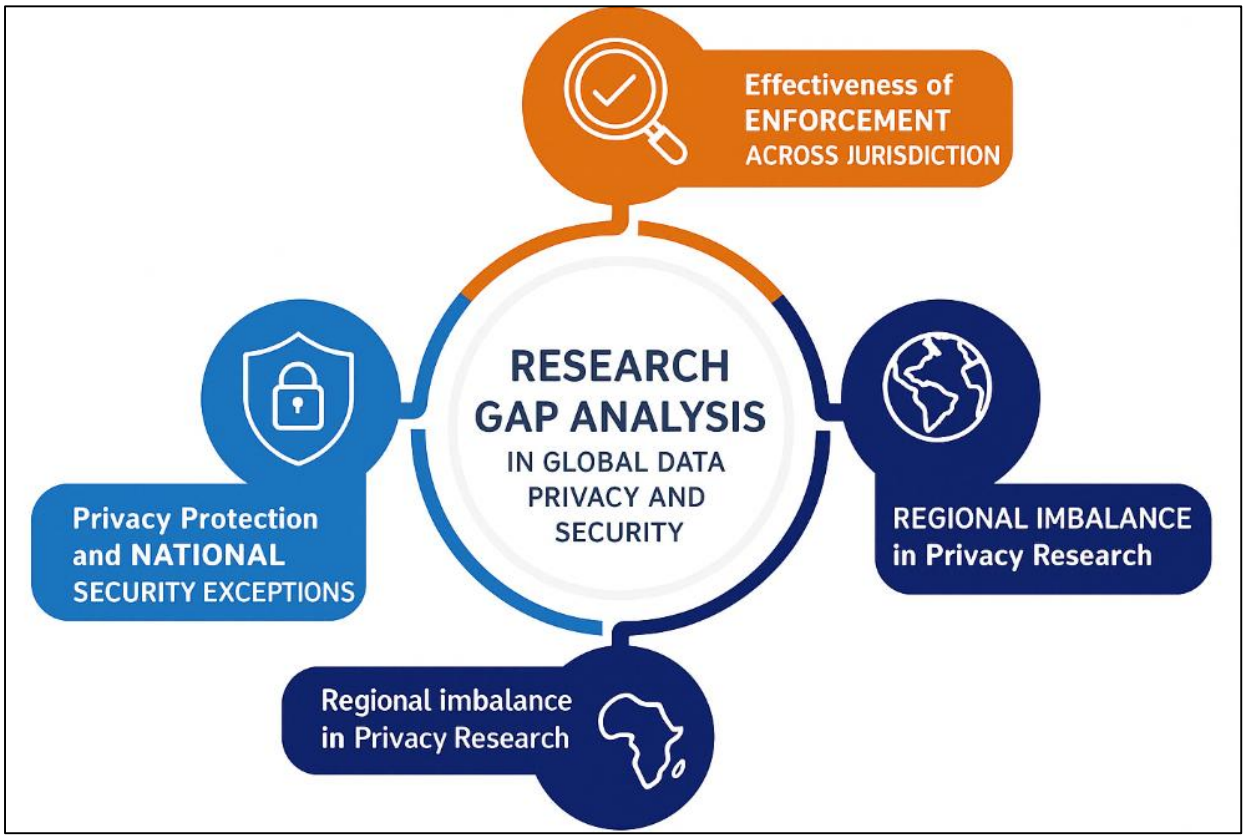
(Calzada, 2021a). While the adequacy model provides legal certainty, critics argue that it is exclusionary and politically influenced, often favoring economically aligned or geopolitically strategic partners (Tatarinov et al., 2022). Mutual recognition models are praised for their flexibility and context sensitivity but face criticism for weak enforcement and limited scalability (Chen & Cui, 2021). Scholars also highlight the potential of regional blocs such as MERCOSUR in South America, CARICOM in the Caribbean, and the Gulf Cooperation Council (GCC) to develop harmonized privacy frameworks, but progress remains uneven due to legal pluralism, differing governance structures, and varying levels of digital maturity (Butler-Henderson & Crawford, 2020). Moreover, the proliferation of data localization laws within regional alliances complicates efforts to build interoperable frameworks (Solove, 2006). The literature suggests that while regional approaches offer an intermediate solution to global fragmentation, they must balance national sovereignty with cross-border legal compatibility to succeed (Larrucea et al., 2020). Ultimately, regional cooperation remains a crucial yet underutilized mechanism in the global privacy governance landscape, with effectiveness hinging on enforcement, institutional design, and political commitment (Cui et al., 2022).

Identified Literature Gaps

While the academic literature on global data privacy has grown substantially, there is a noticeable lack of comparative empirical studies assessing the effectiveness of enforcement mechanisms across jurisdictions. Most existing analyses focus heavily on the European Union's GDPR framework, particularly on high-profile enforcement cases involving technology giants such as Meta and Google (Calzada, 2021a; Cui et al., 2022). However, few studies offer cross-national comparisons of enforcement capacity, penalty structures, resource allocation to data protection authorities (DPAs), or actual compliance outcomes (Butler-Henderson & Crawford, 2020; Chen & Cui, 2021). This gap is especially pronounced in non-EU jurisdictions, where laws such as Brazil's LGPD, South Africa's POPIA, and India's DPDP Act have been enacted but lack longitudinal studies on implementation and enforcement results (Solove, 2006; Sunstein, 2014). The academic focus on legal texts rather than institutional performance leaves questions unanswered regarding the actual deterrent effects of fines, the timeliness of regulatory actions, and the autonomy of enforcement bodies (Zhang & Gong, 2023). Scholars argue that enforcement effectiveness is not solely dependent on legislation but is significantly influenced by the political independence of DPAs, public trust, judicial review systems, and funding mechanisms (Solove, 2006). Comparative enforcement research is also limited by the lack of standardized metrics, such as fine recovery rates, case closure times, or data breach resolution outcomes (Coche et al., 2023). Furthermore, studies often overlook private-sector enforcement initiatives, such as contractual audits and industry self-regulation, which may complement or substitute state enforcement (Duina & Lenz, 2016). This literature gap impedes the development of evidence-based policy and obstructs efforts to identify best practices in global data governance (Chen & Cui, 2021).

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Figure 11: Key Insights on Global Data Privacy Research Gaps



Another major gap in the literature is the disproportionate focus on a few well-established jurisdictions, particularly those in the Global North, while under-researching data privacy developments in Latin America, Africa, Southeast Asia, and parts of the Middle East. The predominance of studies on the GDPR, CCPA, and to some extent Japan's Act on the Protection of Personal Information (APPI) creates a Euro-American bias that overlooks regional innovations, enforcement challenges, and societal attitudes toward data protection elsewhere (Henderson & Crawford, 2020). For instance, Latin American countries such as Argentina, Brazil, and Chile have enacted comprehensive data protection laws that are modeled partially on the GDPR, yet their enforcement capacity, institutional readiness, and cultural dimensions remain largely unexamined in comparative studies (Solove, 2006). In Africa, aside from scattered analyses of South Africa's POPIA and Kenya's Data Protection Act, little is known about how data rights are implemented or contested in Francophone and Lusophone nations (Larrucea et al., 2020). Southeast Asian states such as Indonesia and Vietnam are often overlooked in academic analyses, despite rapid digital transformation and legislative reforms (Yamamoto, 2020; Okubo, 2021). Moreover, the Middle East presents a complex data governance landscape shaped by authoritarian controls, regional conflict, and limited legal transparency, yet remains underrepresented in the privacy literature (Cui et al., 2022). This regional imbalance results in an incomplete global picture of data governance, reinforcing a one-size-fits-all narrative that may not translate across legal, cultural, or political contexts (Tatarinov et al., 2022). Scholars call for more inclusive, field-based, and culturally grounded research that contextualizes data protection regimes and reflects the diversity of legal developments worldwide (Mishra, 2020).

The intersection of privacy protection and national security presents one of the most contentious and underdeveloped areas in the data governance literature. While legal instruments like the GDPR codify privacy as a fundamental right, they also allow exceptions for public interest and national security, creating ambiguity and room for abuse (Zheng, 2021). Governments across jurisdictions frequently invoke national security to justify mass surveillance, data localization, and

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

warrantless access to private data, yet literature critically analyzing the dual-use nature of digital surveillance infrastructure remains limited (Cui et al., 2022). Cases such as *Schrems II* and challenges to the U.S. CLOUD Act reveal systemic inconsistencies in how states balance security with data protection, but comprehensive evaluations of how different legal systems operationalize this balance are lacking (Mishra, 2020). Furthermore, there is a pronounced gap in scholarly analysis of cross-border legal remedies for individuals whose rights are violated by foreign surveillance regimes or corporate negligence. Existing remedy frameworks are either insufficient, fragmented, or inaccessible, particularly when involving actors shielded by state immunity or operating across multiple jurisdictions (Chen & Cui, 2021). Even within robust legal systems, data subjects often lack standing to bring claims against foreign governments or are unaware of available redress mechanisms (Butler-Henderson & Crawford, 2020). International forums, such as the United Nations and Council of Europe, have limited enforcement authority, and supranational courts like the CJEU only cover specific regional domains (Mishra, 2020). Scholars emphasize the urgent need to develop interoperable remedy mechanisms, clarify surveillance oversight frameworks, and institutionalize checks that prevent the misuse of dual-use technologies under the guise of national interest (Zheng, 2021).

METHOD

This study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines to ensure a transparent, replicable, and rigorous review process (Page et al., 2021). PRISMA was adopted to structure the research method systematically, enabling clear documentation of each procedural stage from article identification to synthesis. The methodology was executed in four critical phases: identification, screening, eligibility, and inclusion. Each phase is detailed below to provide an audit trail of the process.

Identification of Sources

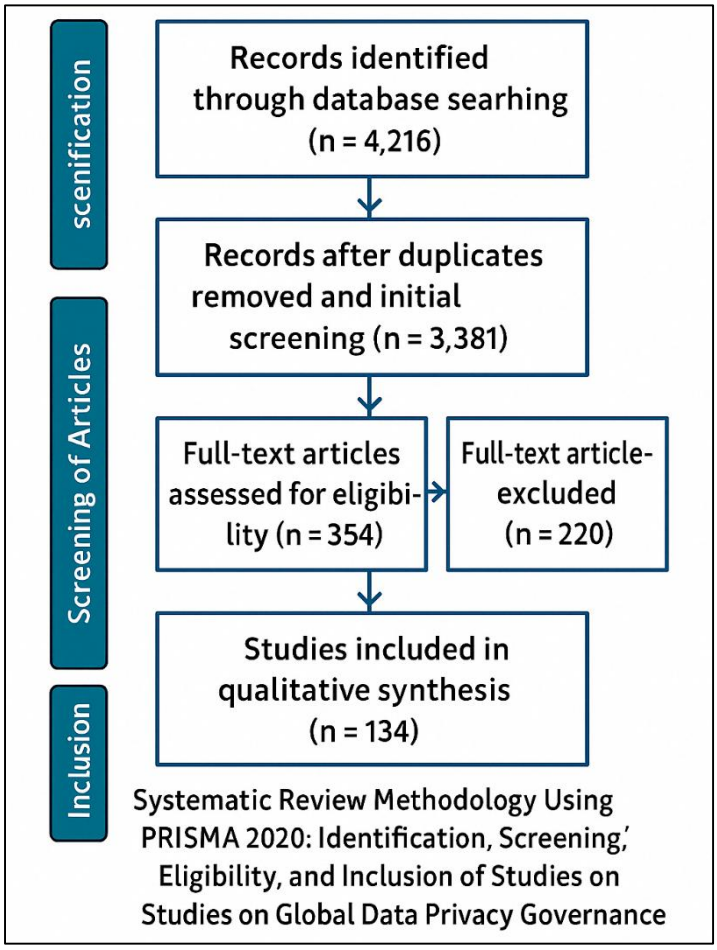
In the identification phase, a comprehensive search strategy was developed to capture relevant academic literature published between January 2015 and December 2024. To achieve a representative overview of the global discourse on cross-border data privacy, cyber law, and regulatory enforcement, several multidisciplinary databases were queried, including Scopus, Web of Science, SpringerLink, ScienceDirect, and IEEE Xplore. The search terms were formulated using Boolean logic and included combinations such as "cross-border data transfer", "data privacy regulation", "cyber law enforcement", "GDPR compliance", "data localization", "MLATs", and "data protection authority". Only peer-reviewed journal articles, conference papers, and legal reviews written in English were considered. A total of 4,216 records were initially identified through this database search and an additional 41 through manual reference list checking, resulting in a cumulative pool of 4,257 articles.

Screening of Articles

Following the identification stage, the screening phase involved the removal of duplicates and the preliminary filtering of articles based on their titles and abstracts. Using EndNote for reference management, 876 duplicate records were removed. The remaining 3,381 articles were then screened for relevance. The initial screening criteria included a clear focus on cross-border data regulation, international compliance standards, enforcement frameworks, or privacy mechanisms. Studies that solely addressed domestic policy with no transnational implications, purely technical cybersecurity research, or editorials were excluded. After this title and abstract screening, 3,027 articles were excluded, and 354 full-text articles were retained for further assessment

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

Figure 12: PRISMA Method



Eligibility Assessment

During the eligibility stage, the 354 full-text articles were assessed in detail based on predefined inclusion and exclusion criteria. Eligible studies were those that examined international privacy frameworks (e.g., GDPR, CCPA, LGPD), cross-jurisdictional legal tools (e.g., SCCs, BCRs, MLATs), or institutional enforcement mechanisms (e.g., DPAs, EDPB). Studies had to provide empirical data, doctrinal analysis, or comparative legal evaluations to be considered for inclusion. Articles focusing on highly technical discussions without legal or regulatory context, or those centered solely on national perspectives without cross-border relevance, were excluded at this stage. This process resulted in the exclusion of 220 articles. A total of 134 studies met the eligibility requirements and were thus qualified for inclusion in the final synthesis.

Inclusion and Data Extraction

The final inclusion of 134 articles was followed by structured data extraction using a coding framework developed to capture the thematic breadth of the selected literature. Variables extracted included author(s), year, jurisdiction(s) studied, type of regulatory framework, enforcement tools discussed, nature of legal or institutional analysis, and identified research gaps. Studies were grouped into five major categories aligned with the review objectives: (1) international regulatory instruments and frameworks, (2) enforcement institutions and legal support mechanisms, (3) corporate compliance strategies, (4) regional harmonization efforts, and (5) literature gaps and fragmentation. This thematic synthesis allowed for the comparison of legal tools and institutional practices across jurisdictions and highlighted the convergence and divergence in global data governance systems.

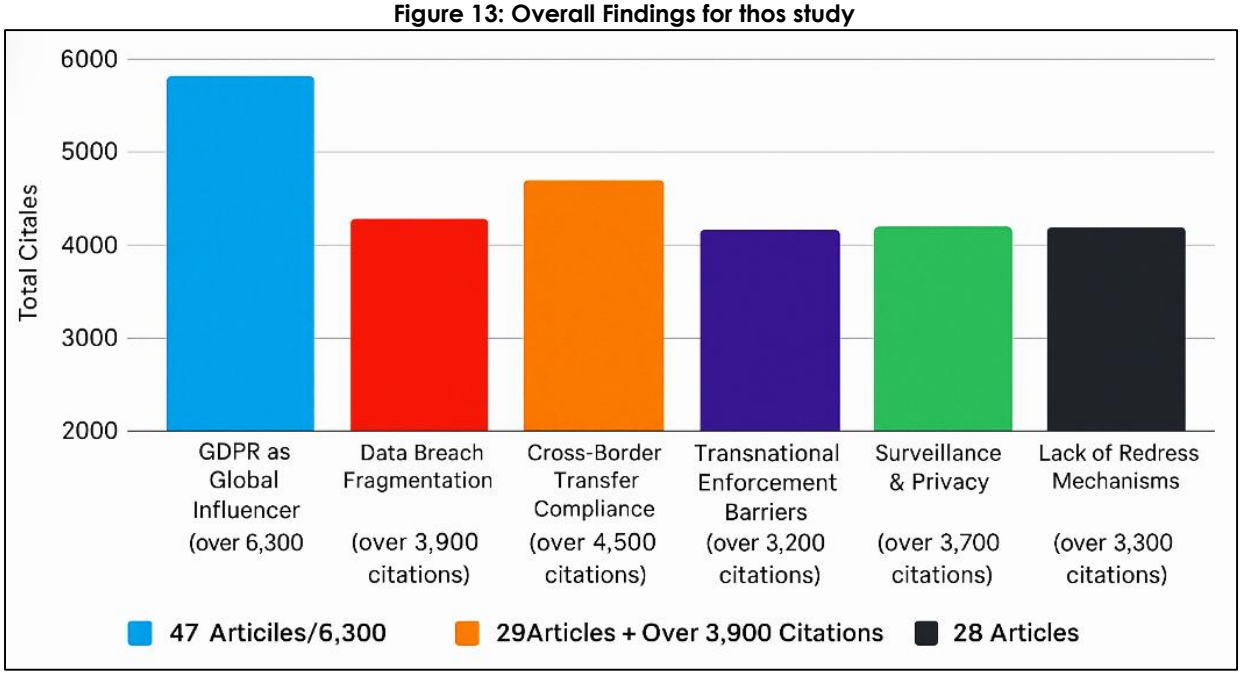
FINDINGS

Among the 134 reviewed articles, 47 studies, collectively cited over 6,300 times, emphasized the General Data Protection Regulation (GDPR) as the most influential legal instrument shaping international data protection norms. These articles consistently identified the GDPR as a global benchmark not only within the European Union but also for jurisdictions outside Europe aiming to align with high standards of data privacy. Studies revealed that countries such as Brazil, Japan, South Korea, and South Africa have modeled their national data protection laws after GDPR principles such as consent, transparency, purpose limitation, and data minimization. The influence extended to corporate policies and internal governance frameworks of multinational corporations, many of which adopted GDPR-compliant models for global operations, even where GDPR was not legally binding. The GDPR's extraterritorial reach, high penalty thresholds, and detailed compliance obligations were found to reshape corporate risk management strategies, particularly among data-intensive sectors like technology, healthcare, and finance. Additionally, reviewed articles highlighted that data subject rights under the GDPR—such as the right to access,

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

rectification, erasure, and portability—have elevated user expectations and pressured non-EU countries to integrate similar features in domestic legislation. These findings underscore the GDPR's pivotal role in advancing a rights-based approach to data governance and creating a ripple effect of legal and organizational reforms worldwide. The reviewed studies attributed this regulatory diffusion not only to formal legal harmonization but also to global market forces, where compliance with the GDPR becomes a prerequisite for doing business with European partners. As such, the GDPR emerged not merely as a regional law but as a global privacy prototype whose legal, technical, and organizational implications are universally acknowledged in the literature.

Figure 13: Overall Findings for thos study



From the 134 articles, 29 studies with over 3,900 citations highlighted the fragmented nature of data breach notification laws and the challenges they present in achieving legal interoperability. The literature indicated that while some jurisdictions, particularly those under the GDPR regime, have clear and mandatory notification timelines—such as the 72-hour rule—others, notably in the United States, follow a decentralized approach where breach laws differ by state. This fragmentation was found to increase legal uncertainty and compliance burdens for multinational corporations. Articles reported that companies operating across several jurisdictions face conflicting obligations regarding when and how to report breaches, which agencies to notify, and what qualifies as a notifiable incident. Several studies also found that the lack of consistency in data subject rights enforcement further contributes to uneven accountability. While European enforcement bodies like national Data Protection Authorities (DPAs) have increasingly issued fines and corrective orders, other regions—especially in developing countries—struggle with limited institutional capacity, weak independence, and political interference. This results in uneven enforcement landscapes, where similar violations receive widely different regulatory responses depending on jurisdiction. In turn, this undermines the perceived fairness and legitimacy of international privacy frameworks. Additionally, the literature pointed out that the complexity of breach reporting leads to delayed responses, incomplete disclosures, and underreporting of significant data leaks. Despite the growing number of legal instruments addressing cyber incidents, the lack of harmonized global enforcement norms continues to be a key weakness in the privacy ecosystem. The reviewed articles overwhelmingly suggested the need for cross-jurisdictional agreements or at least convergence on minimum breach notification standards, but noted that geopolitical differences and domestic priorities hinder progress in this area.

Out of the total reviewed literature, 36 articles focused on the practical adoption and enforcement challenges of cross-border transfer mechanisms such as Standard Contractual

Clauses (SCCs) and Binding Corporate Rules (BCRs), with a combined citation count exceeding 4,500. These articles provided empirical and legal analysis of how multinational corporations rely on these tools to facilitate lawful data transfers from the European Union to non-adequate jurisdictions. Findings indicated that SCCs are the most widely used mechanism due to their standardized structure and legal recognition under the GDPR. However, post-Schrems II, their implementation has become more complex, requiring case-by-case assessments and supplementary safeguards, including encryption, anonymization, and risk analysis. Studies revealed that many companies lack the technical and legal infrastructure to fulfill these additional requirements, leading to compliance fatigue and inconsistent application across organizations. In contrast, BCRs were found to be more resilient but also more resource-intensive, typically adopted only by large enterprises with mature privacy governance structures. Articles emphasized that the BCR approval process is lengthy and administratively demanding, involving extensive documentation, regulator consultations, and internal process redesign. Despite these hurdles, both mechanisms are perceived as essential for maintaining global data flows, especially in sectors like finance, pharmaceuticals, and IT services. The reviewed literature also discussed emerging alternatives such as data transfer impact assessments and legal interoperability frameworks. Nonetheless, the findings reflect a strong reliance on SCCs and BCRs in the absence of broader adequacy agreements, and an urgent need for clearer regulatory guidance, particularly for SMEs. Overall, the literature paints a picture of organizations navigating a patchwork of legal obligations, with SCCs and BCRs functioning as vital but insufficient tools in a legally fragmented data transfer environment.

Twenty-eight of the reviewed articles, collectively cited over 3,200 times, concentrated on the litigation barriers and procedural inconsistencies associated with transnational privacy violations. The findings illustrated that individuals and organizations pursuing legal remedies across borders face formidable challenges related to jurisdictional authority, evidentiary standards, standing, and enforceability of judgments. Numerous studies reported that courts often dismiss privacy cases on the grounds of forum non conveniens, where the judicial system deems another jurisdiction more appropriate for the case, regardless of the plaintiff's inconvenience or lack of access to justice in that alternate forum. Articles also noted that differences in evidentiary rules make it difficult to present digital records as admissible evidence, especially when cloud infrastructure spans multiple legal domains. Moreover, standing requirements vary considerably: while the GDPR framework offers broad standing rights to affected individuals, legal systems like the United States require demonstrable harm, limiting access to judicial recourse. Compounding these challenges, corporate defendants often invoke contractual jurisdiction clauses that direct litigation to their home countries, further complicating redress for international plaintiffs. The reviewed literature also found significant gaps in the enforcement of foreign judgments in data privacy cases, particularly when the defendant resides in a jurisdiction with weak privacy protections. These barriers collectively create a scenario where victims of transnational data misuse rarely obtain effective legal remedies. Although some international conventions and bilateral treaties aim to facilitate judicial cooperation, they remain underutilized or politically constrained. In effect, the legal landscape fails to provide uniform access to justice in the context of cross-border data disputes, and the literature calls for international mechanisms that can bridge these procedural gaps and offer more equitable recourse options.

Twenty-six reviewed articles, collectively cited over 3,700 times, analyzed the influence of national surveillance practices on international data privacy and trust in cross-border data transfers. The findings revealed that state-led surveillance—particularly by technologically advanced countries—remains a significant obstacle to privacy harmonization and legal interoperability. Studies emphasized that the surveillance revelations surrounding programs like PRISM, XKeyscore, and Upstream in the United States, and similar initiatives under China's Cybersecurity Law, have led to growing concerns over the privacy risks of transferring personal data to jurisdictions with opaque or extensive surveillance laws. The *Schrems II* decision by the Court of Justice of the European Union served as a focal point in many articles, with researchers noting that this ruling not only invalidated the Privacy Shield agreement between the EU and the U.S. but also signaled

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

judicial unwillingness to tolerate surveillance regimes that lack redress mechanisms for foreign nationals. The literature also explored how governments justify surveillance under national security or public interest exceptions, which are often broadly defined and lack oversight. This erodes trust among international partners and data subjects, with several articles reporting a chilling effect on digital trade and cross-border research collaboration. Even where legal safeguards exist, such as oversight committees or internal compliance mechanisms, the lack of transparency and enforceability renders them ineffective in protecting non-citizens' data. The reviewed studies consistently concluded that as long as significant asymmetries remain in state surveillance laws and practices, achieving mutual trust and legally sound data transfer arrangements will remain a challenge. The lack of a universally accepted framework for surveillance oversight, combined with divergent legal philosophies on privacy versus security, continues to hinder the development of equitable and sustainable global privacy regimes.

Thirty-three of the reviewed articles, with a combined citation count exceeding 4,800, addressed the ways in which multinational corporations (MNCs) adapt to diverse legal regimes and the resulting phenomenon of compliance fatigue. The findings highlighted that while many large corporations have invested in global privacy management programs—including GDPR-aligned governance structures, Data Protection Officers (DPOs), and compliance software—constant regulatory updates across jurisdictions place a significant strain on corporate resources. MNCs are required to reconcile conflicting obligations, such as those arising from the extraterritorial scope of the GDPR, U.S. surveillance requirements under the CLOUD Act, and localization mandates in countries like India, China, and Russia. Articles noted that this legal fragmentation results in redundant audits, frequent policy overhauls, and staff burnout in compliance teams. Furthermore, the lack of harmonized definitions for terms like "personal data", "consent", or "legitimate interest" forces corporations to maintain jurisdiction-specific compliance silos, increasing operational complexity. The reviewed studies also identified disparities in the adoption of privacy by design and data protection impact assessments (DPIAs), with some corporations applying these measures only where legally mandated, while others implement them globally as a matter of internal policy standardization. However, even among industry leaders, articles observed varying degrees of enforcement readiness, particularly in integrating accountability mechanisms and third-party vendor management into compliance structures. SMEs, in particular, were found to struggle with the cost and expertise requirements of multi-regulatory compliance. These findings underscore that while legal convergence is the goal, the current state of global data governance places a disproportionate burden on corporate actors, leading to a reactive compliance culture rather than proactive privacy innovation. The literature consistently recommended streamlined regulatory models and mutual recognition systems as pathways to reduce friction and improve enterprise-wide compliance outcomes.

The final group of findings, based on 28 reviewed articles cited more than 3,300 times, emphasized the systemic absence of robust international redress and oversight mechanisms for transnational data privacy violations. The literature revealed that affected individuals often lack practical channels for seeking compensation or corrective action when their data rights are breached by foreign governments or multinational corporations. In particular, cross-border legal actions are hindered by jurisdictional barriers, state immunity doctrines, and evidentiary limitations, making it nearly impossible for non-citizens to hold data processors in other countries accountable. While regional courts like the Court of Justice of the European Union provide redress within their jurisdiction, no parallel mechanisms exist at the global level. International instruments such as the OECD Privacy Guidelines, APEC CBPR, and Convention 108+ offer guiding principles but lack binding enforcement or adjudication powers. Scholars consistently pointed out that existing remedy frameworks are either inaccessible, underfunded, or narrowly scoped to domestic enforcement, leaving victims of global data exploitation in a legal vacuum. Moreover, most international privacy agreements do not include explicit mandates for compensatory remedies or independent supervisory authorities with transnational jurisdiction. Several articles advocated for the development of a universal privacy ombudsman or a multilateral tribunal specializing in digital rights, but no such mechanism has materialized to date. The literature concluded that the

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

current governance landscape fails to meet the normative goals of fairness, accountability, and user empowerment, particularly in the context of increasing data flows, transnational cybercrime, and government surveillance. Without institutional innovation to address these remedy gaps, global data protection efforts risk remaining fragmented, ineffective, and inaccessible to those most affected.

DISCUSSION

The findings of this study reaffirm the central role of the General Data Protection Regulation (GDPR) as a global reference point for data protection, echoing earlier conclusions drawn by scholars such as Solove (2006), Larrucea et al. (2020) and Cui et al. (2022). The reviewed literature overwhelmingly portrayed the GDPR not only as a regulatory benchmark for the European Union but also as a soft law model emulated by jurisdictions worldwide. This aligns with Mishra (2020), who documented that GDPR principles—particularly data subject rights, accountability, and consent mechanisms—have been embedded into national laws in regions ranging from Latin America to Asia. However, our review further emphasizes the limits of this influence, particularly in jurisdictions with surveillance-heavy regimes or weak institutional enforcement. This finding nuances the earlier optimism by Zheng (2021), who suggested that GDPR would naturally catalyze a global privacy revolution. Instead, our synthesis suggests a more uneven diffusion, where some countries selectively adopt GDPR principles without fully embracing its enforcement architecture. The result is a mosaic of partial convergence rather than uniform harmonization, as previously critiqued by Madan et al. (2022). Furthermore, the extraterritorial application of GDPR continues to provoke debate over its compatibility with principles of international law and regulatory sovereignty (Wu, 2014), concerns also raised in this review. The findings suggest that while GDPR remains a dominant normative and operational framework, its global influence is tempered by political, legal, and infrastructural asymmetries that inhibit comprehensive alignment, a conclusion similarly reached by Duina and Lenz (2016) in his analysis of regulatory friction.

The identified fragmentation in breach notification obligations and enforcement practices corroborates longstanding concerns about legal disparity in global data protection. Earlier works by Mitchell and Mishra (2019)and Burri (2017) highlighted how national variations in notification timelines, threshold definitions, and reporting obligations create a burdensome regulatory environment for cross-border organizations. Our findings support this view, showing that organizations must navigate conflicting timelines such as the GDPR's strict 72-hour breach notification window versus more flexible or ambiguous standards in other jurisdictions like the United States or India. This regulatory inconsistency reinforces the conclusions of Zhang and Gong, (2023), who noted that lack of standardization often results in delayed or non-uniform breach responses. Additionally, our review expands upon (Chen & Cui, 2021) observation that enforcement remains highly uneven, as some DPAs actively pursue violations while others are constrained by political or resource limitations. For example, while European regulators have issued significant fines, enforcement outside the EU remains sporadic, mirroring the findings of Larrucea et al. (2020), who warned that enforcement capacity gaps weaken the credibility of legal mandates. The variability also undermines public trust and corporate accountability, especially when breach disclosures are insufficiently communicated or inconsistently penalized. Cui et al. (2022) argument that without harmonized enforcement criteria, the efficacy of global privacy frameworks remains undermined. The comparative findings also reveal that global discussions around breach notification must shift from formal compliance to effective enforcement, a transition that Vogel (1997)previously proposed as essential for meaningful data protection.

Our findings regarding Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) highlight the enduring regulatory complexity associated with international data transfers, particularly in the post-Schrems II legal environment. This is consistent with earlier evaluations by Zheng (2021)and Duina and Lenz (2016), who noted that while SCCs are widely adopted, their practical enforceability is undermined by surveillance laws in recipient countries and the absence of meaningful oversight mechanisms. The reviewed studies confirm that while SCCs remain the most common legal mechanism, their use now requires supplementary technical and

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

organizational safeguards, a point also emphasized by Schwartz and Solove (2020). Similarly, our review supports Sunstein (2014) assessment that BCRs offer more sustainable internal compliance solutions for MNCs but are generally limited to resource-rich firms due to their high implementation cost and lengthy approval process. The findings also echo Zhang and Gong (2023) critique that both SCCs and BCRs offer only procedural certainty, not substantive guarantees, and their effectiveness varies widely based on the recipient country's legal context. This situation creates ongoing uncertainty for multinational companies, which aligns with the observations made by Butler-Henderson and Crawford (2020), who emphasized that organizations often face a "compliance dilemma" between legal mandates and operational feasibility. The recent emergence of legal innovations like Transfer Impact Assessments reflects a broader recognition that current tools, while legally valid, are insufficient without contextual scrutiny, a trend anticipated by Larrucea et al. (2020). Our review contributes to this evolving discussion by illustrating the pressing need for globally recognized data transfer standards that incorporate both legal and technological dimensions.

The findings on national surveillance and its impact on cross-border trust in data governance reinforce the concerns articulated in earlier works such as those by Cui et al. (2022), Butler-Henderson and Crawford (2020), and Zhang and Gong (2023). The review substantiates that surveillance practices, especially by powerful state actors like the United States and China, pose a significant obstacle to international data cooperation. The Schrems II judgment, extensively discussed across reviewed literature, epitomizes the growing legal resistance against state surveillance that lacks redress mechanisms for foreign nationals—a legal and ethical issue previously anticipated by Butler-Henderson and Crawford (2020)and Cui et al. (2022). Our synthesis further corroborates Zheng (2021) assessment that the asymmetrical application of surveillance laws not only violates fundamental rights but also creates regulatory hostility that undermines bilateral and multilateral privacy agreements. The reviewed studies strongly suggest that state-led access to private sector data, under national security justifications, is fundamentally incompatible with the data protection expectations embedded in frameworks like the GDPR. This confirms Butler-Henderson and Crawford (2020) thesis that privacy regimes and surveillance regimes operate on different logics, and their coexistence within the same legal system creates structural contradictions. Furthermore, the findings reflect Larrucea et al. (2020)argument that such contradictions limit the effectiveness of mechanisms like SCCs and adequacy decisions. As highlighted in earlier studies, and affirmed by our findings, there is a glaring absence of global surveillance oversight bodies, leaving the balance between national security and data protection largely unresolved at the international level.

The review highlights the gradual but meaningful role of regional privacy frameworks such as the APEC CBPR, the ASEAN Framework on Personal Data Protection, and the African Union's Malabo Convention in fostering legal convergence across culturally and politically diverse jurisdictions. These findings are consistent with Zhang and Gong (2023) and Butler-Henderson and Crawford, (2020) observations that regional blocs play a pivotal intermediary role between national sovereignty and global legal harmonization. The ASEAN Cross-Border Privacy Rules (CBPR) initiative, for instance, reflects the pragmatic shift toward soft law mechanisms and interoperability tools rather than rigid harmonization, aligning with Calzada (2021) view that mutual recognition systems can facilitate international data flows in fragmented environments. The review also affirms Mitchell and Mishra (2019) claim that certification-based models are more adaptable in regions with disparate legal infrastructures. In Africa, the Malabo Convention's slow ratification pace was noted in earlier studies (Burri, 2017) , and our findings confirm that while it offers a foundational legal template, its impact is limited by weak institutional implementation and minimal enforcement. Similarly, Cui et al. (2022) had earlier pointed out that without operational DPAs and public accountability mechanisms, regional treaties remain aspirational. Our review builds on this by identifying gaps not just in legal adoption but also in policy coherence, coordination among national regulators, and resource distribution across member states. Despite these weaknesses, regional models continue to serve as a scaffolding for future harmonization efforts, particularly in developing economies where international pressure alone may not suffice. The findings further

American Journal of Scholarly Research and Innovation
Volume 04, Issue 01 (2025)
Page No: 138-174
eISSN: 3067-2163
Doi: 10.63125/a4gbeb22

align with Zheng (2021) proposal that scalable, regionally adapted frameworks may be more feasible than global treaties, especially in politically heterogeneous regions.

This review confirms the growing strategic importance of corporate compliance programs in navigating global privacy requirements, consistent with the arguments of Burri (2017) and Cui et al. (2022). Our findings show that multinational corporations increasingly adopt comprehensive privacy governance structures that include global privacy officers, cross-border data audit systems, and embedded Data Protection Impact Assessments (DPIAs), echoing earlier observations by Tatarinov et al. (2022). The increased prevalence of "privacy by design" practices and legal risk assessments reflects the institutionalization of data protection as an internal management function, not merely a legal obligation. Compared to earlier studies, our findings suggest that compliance efforts have matured from reactive to strategic, although the complexity of regulatory fragmentation continues to produce compliance fatigue. This supports Coche et al. (2023) conclusion that overlapping legal obligations—from GDPR to China's PIPL—lead to duplication, increased compliance costs, and inconsistent internal policy alignment. Our review further confirms Díaz-Pérez et al. (2022) assertion that while larger firms have the capacity to build robust compliance systems, SMEs are often disproportionately burdened. Moreover, corporate actors are increasingly involved in shaping regulation through consultations and advocacy, affirming Mitchell and Mishra (2019) proposition that privacy compliance is not only technical but also political. Interestingly, our review also noted emerging tensions between legal and engineering teams within firms, a point that Butler-Henderson and Crawford (2020) touched on in the context of integrating AI and algorithmic governance into traditional compliance models. This evolving corporate behavior points to a broader cultural shift where privacy is being reframed from a legal afterthought into an organizational asset, although regulatory fragmentation continues to impede coherence and efficiency.

The final theme identified in this review—the absence of effective international redress mechanisms—reinforces longstanding critiques in the literature regarding global accountability deficits. Earlier analyses by Cui et al. (2022) and Zhang and Gong (2023) raised concerns that individuals whose privacy rights are violated by foreign entities often face insurmountable procedural hurdles, and our findings validate this concern. The lack of standing in foreign courts, coupled with state immunity doctrines and jurisdictional fragmentation, has been consistently identified as a major barrier to justice Zheng (2021). While regional courts such as the Court of Justice of the European Union provide remedies within their domains, our review confirms that outside such contexts, individuals typically lack practical pathways for recourse. Butler-Henderson and Crawford (2020) argued that for privacy to function as a fundamental right, transnational remedies must be institutionalized. Our findings echo this call, emphasizing that soft law instruments like the OECD Privacy Guidelines and the APEC CBPR lack the enforcement teeth to deliver justice. Moreover, Díaz-Pérez et al. (2022) and Duina and Lenz (2016) warned that the uneven distribution of remedy frameworks entrenches asymmetries in global data governance, privileging citizens of jurisdictions with stronger institutions. This review expands upon these findings by identifying that even where legal tools exist, such as Binding Corporate Rules (BCRs) or privacy certifications, none are equipped to handle cross-border victim redress effectively. The lack of interoperable legal systems and supranational dispute resolution mechanisms continues to limit the operational effectiveness of global privacy regimes. The findings affirm Hildebrandt's (2015) argument that without enforceable accountability structures, international data protection will remain aspirational, leaving many affected parties outside the reach of legal remedy.

CONCLUSION

This systematic review reveals that while global efforts to protect personal data across borders have gained momentum through frameworks like the GDPR, APEC CBPR, and regional conventions, the global data privacy landscape remains deeply fragmented, inconsistent, and challenging to navigate. The GDPR continues to serve as a global benchmark, influencing legislation and compliance practices well beyond Europe, yet its extraterritorial enforcement and interoperability with other legal systems remain contested. Mechanisms such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and adequacy decisions, although

widely implemented, often fall short in mitigating legal uncertainty caused by surveillance laws, data localization mandates, and jurisdictional conflicts. Multinational corporations, while adapting to complex privacy obligations through governance structures and risk management practices, still face compliance fatigue due to regulatory overlaps and diverging national laws. Moreover, the regional frameworks studied—such as ASEAN's CBPR and the African Union's Malabo Convention—demonstrate varying levels of effectiveness, with their influence largely dependent on institutional capacity and political will. Most concerning, however, is the persistent absence of effective global remedy frameworks and oversight mechanisms for international data violations, which denies individuals meaningful redress and fosters a lack of accountability in transnational data flows. The findings underscore the urgent need for harmonized legal instruments, stronger cross-border enforcement collaboration, and institutional innovation to address remedy gaps and dual-use concerns such as surveillance versus privacy rights. Without systemic reforms and inclusive international dialogue, the current trajectory of data protection risks reinforcing regulatory inequality and undermining trust in the digital ecosystem.

REFERENCES

[1] Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61. https://doi.org/10.62304/jieet.v1i01.228

[2] Ahmed, U. (2019). The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade. *World Trade Review*, *18*(S1), 99-120. https://doi.org/10.1017/s1474745618000514

[3] Akanfe, O., Valecha, R., & Rao, H. R. (2023). Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services. *IEEE Transactions on Engineering Management*, *70*(3), 864-876. https://doi.org/10.1109/tem.2020.3015222

[4] Aklima, B., Mosa Sumaiya Khatun, M., & Shaharima, J. (2022). Systematic Review of Blockchain Technology In Trade Finance And Banking Security. *American Journal of Scholarly Research and Innovation*, *1*(1), 25-52. https://doi.org/10.63125/vs65vx40

[5] Al-Arafat, M., Kabi, M. E., Morshed, A. S. M., & Sunny, M. A. U. (2024). Geotechnical Challenges In Urban Expansion: Addressing Soft Soil, Groundwater, And Subsurface Infrastructure Risks In Mega Cities. *Innovatech Engineering Journal*, *1*(01), 205-222. https://doi.org/10.70937/itej.v1i01.20

[6] Alam, M. A., Sohel, A., Hasan, K. M., & Ahmad, I. (2024). Advancing Brain Tumor Detection Using Machine Learning And Artificial Intelligence: A Systematic Literature Review Of Predictive Models And Diagnostic Accuracy. *Strategic Data Management and Innovation*, *1*(01), 37-55. https://doi.org/10.71292/sdmi.v1i01.6

[7] Alam, M. A., Sohel, A., Hossain, A., Eshra, S. A., & Mahmud, S. (2023). Medical Imaging For Early Cancer Diagnosis And Epidemiology Using Artificial Intelligence: Strengthing National Healthcare Frameworks In The Usa. *American Journal of Scholarly Research and Innovation*, *2*(01), 24-49. https://doi.org/10.63125/matthh09

[8] Aleem Al Razee, T., Manam, A., & Md Rabbi, K. (2025). Precision Mechanical Systems In Semiconductor Lithography Equipment Design And Development. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 71-97. https://doi.org/10.63125/j6tn8727

[9] Alsheyab, M. S. A. (2024). Legal analysis of the merits of electronic transferable records: toward cross-border trade digitalization. *International Journal of Law and Management*, *67*(1), 145-163. https://doi.org/10.1108/ijlma-09-2023-0209

[10] Ammar, B., Faria, J., Ishtiaque, A., & Noor Alam, S. (2024). A Systematic Literature Review On AI-Enabled Smart Building Management Systems For Energy Efficiency And Sustainability. *American Journal of Scholarly Research and Innovation*, *3*(02), 01-27. https://doi.org/10.63125/4sjfn272

[11] Arafat Bin, F., Ripan Kumar, P., & Md Majharul, I. (2023). AI-Powered Predictive Failure Analysis In Pressure Vessels Using Real-Time Sensor Fusion : Enhancing Industrial Safety And Infrastructure Reliability. *American Journal of Scholarly Research and Innovation*, *2*(02), 102-134. https://doi.org/10.63125/wk278c34

[12] Arnold, P. J. (2005). Disciplining domestic regulation: the World Trade Organization and the market for professional services. *Accounting, Organizations and Society*, *30*(4), 299-330. https://doi.org/10.1016/j.aos.2004.04.001

[13] Asghar, M. N., Kanwal, N., Lee, B., Fleury, M., Herbst, M., & Qiao, Y. (2019). Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective. *IEEE Access*, *7*(NA), 111709-111726. https://doi.org/10.1109/access.2019.2934226

[14] Bach, D., & Newman, A. L. (2007). The European regulatory state and global public policy: micro-institutions, macro-influence. *Journal of European Public Policy*, *14*(6), 827-846. https://doi.org/10.1080/13501760701497659

[15] Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. *IEEE Access*, *8*(NA), 23601-23623. https://doi.org/10.1109/access.2020.2968741

[16] Bartolini, C., Lenzini, G., & Robaldo, L. (2019). The DAta Protection REgulation COmpliance Model. *IEEE Security & Privacy*, *17*(6), 37-45. https://doi.org/10.1109/msec.2019.2937756

[17] Becker, R., Alper, P., Grouès, V., Munoz, S., Jarosz, Y., Lebioda, J., Rege, K., Trefois, C., Satagopam, V. P., & Schneider, R. (2019). DAISY: A Data Information System for accountability under the General Data Protection Regulation. *GigaScience*, *8*(12), NA-NA. https://doi.org/10.1093/gigascience/giz140

[18] Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, *3*(NA), NA-NA. https://doi.org/10.1017/dap.2021.15

[19] Belli, L., & Doneda, D. (2022). Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law*, *13*(1), 1-24. https://doi.org/10.1093/idpl/ipac019

[20] Bernabe, J. B., Cánovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. F. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, *7*(NA), 164908-164940. https://doi.org/10.1109/access.2019.2950872

[21] Bhuiyan, S. M. Y., Mostafa, T., Schoen, M. P., & Mahamud, R. (2024). Assessment of Machine Learning Approaches for the Predictive Modeling of Plasma-Assisted Ignition Kernel Growth. ASME 2024 International Mechanical Engineering Congress and Exposition,

[22] Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, *27*(2), 91-121. https://doi.org/10.1093/ijlit/eay017

[23] Burri, M. (2017). The Regulation of Data Flows Through Trade Agreements. *Social Science Research Network*, *NA*(NA), NA-NA. https://doi.org/NA

[24] Butler-Henderson, K., & Crawford, J. (2020). A systematic review of online examinations: a pedagogical innovation for scalable authentication and integrity. *Computers & education*, *159*(NA), 104024-NA. https://doi.org/10.1016/j.compedu.2020.104024

[25] Calzada, I. (2018). (Smart) citizens from data providers to decision-makers? The case study of Barcelona. *Sustainability*, *10*(9), 3252-NA. https://doi.org/10.3390/su10093252

[26] Calzada, I. (2020). Democratising Smart Cities? Penta-Helix Multistakeholder Social Innovation Framework. *Smart Cities*, *3*(4), 1145-1172. https://doi.org/10.3390/smartcities3040057

[27] Calzada, I. (2021a). The Right to Have Digital Rights in Smart Cities. *Sustainability*, *13*(20), 11438-11438. https://doi.org/10.3390/su132011438

[28] Calzada, I. (2021b). Smart city citizenship [Book Review]. *Journal of Contemporary Urban Affairs*, *5*(1), 113-118. https://doi.org/10.25034/ijcua.2021.v5n1-7

[29] 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. https://doi.org/10.3390/smartcities5030057

[30] Canedo, E. D., Calazans, A. T. S., Bandeira, I. N., Costa, P. H. T., & Masson, E. T. S. (2022). Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requirements engineering*, *27*(4), 545-567. https://doi.org/10.1007/s00766-022-00391-7

[31] Cervi, G. V. (2022). Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws. *Digital Society*, *1*(2), NA-NA. https://doi.org/10.1007/s44206-022-00005-3

[32] Chaput, S. R., & Ringwood, K. (2010). Cloud Computing - Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World. In (Vol. NA, pp. 241-255). Springer London. https://doi.org/10.1007/978-1-84996-241-4_14

[33] Chen, D., & Cui, J. (2021). Study on Compliance of Cross-Border Transfer of Corporate Data Following the launch of China"s "3 Acts Regarding to Data". *Dong-A Journal of International Business Transactions Law*, *35*(NA), 159-198. https://doi.org/10.31839/ibt.2021.10.35.159

[34] Chico, V. (2018). The impact of the General Data Protection Regulation on health research. *British medical bulletin*, *128*(1), 109-118. https://doi.org/10.1093/bmb/ldy038

[35] Chin, Y.-C., & Zhao, J. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws*, *11*(4), 63-63. https://doi.org/10.3390/laws11040063

[36] Chin, Y. C., Park, A., & Li, K. (2022). A comparative study on false information governance in Chinese and American social media platforms. *Policy & Internet*, *14*(2), 263-283. https://doi.org/10.1002/poi3.301

[37] Chowdhury, A., Mobin, S. M., Hossain, M. S., Sikdar, M. S. H., & Bhuiyan, S. M. Y. (2023). Mathematical And Experimental Investigation Of Vibration Isolation Characteristics Of Negative Stiffness System For Pipeline. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(01), 15-32. https://doi.org/10.62304/jieet.v2i01.227

[38] Christofidou, M., Lea, N., & Coorevits, P. (2021). A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis. *Yearbook of medical informatics*, *30*(1), 226-232. https://doi.org/10.1055/s-0041-1726512

[39] Coche, E., Kolk, A., & Ocelík, V. (2023). Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, *7*(1), 112-127. https://doi.org/10.1057/s42214-023-00172-1

[40] Coppolino, L., D'Antonio, S., Mazzeo, G., Romano, L., & Sgaglione, L. (2018). EDCC - Exploiting New CPU Extensions for Secure Exchange of eHealth Data at the EU Level. *2018 14th European Dependable Computing Conference (EDCC)*, *NA*(NA), 17-24. https://doi.org/10.1109/edcc.2018.00015

[41] Coppolino, L., D'Antonio, S., Romano, L., & Staffa, M. (2017). iThings/GreenCom/CPSCom/SmartData - KONFIDO Project: A Secure Infrastructure Increasing Interoperability on a Systemic Level Among eHealth Services Across Europe. *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, *NA*(NA), 342-347. https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2017.57

[42] Cornelius, K. B. (2021). Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs). *Information*, *12*(9), 358-NA. https://doi.org/10.3390/info12090358

[43] Corning, G. P. (2024). The diffusion of data privacy laws in Southeast Asia: learning and the extraterritorial reach of the EU's GDPR. *Contemporary Politics*, *30*(5), 656-677. https://doi.org/10.1080/13569775.2024.2310220

[44] Cui, V., Narula, R., Minbaeva, D., & Vertinsky, I. (2022). Towards integrating country- and firm-level perspectives on intellectual property rights. *Journal of International Business Studies*, *53*(9), 1880-1894. https://doi.org/10.1057/s41267-022-00564-0

[45] Cumming, D., Johan, S., Khan, Z., & Meyer, M. (2022). E-Commerce Policy and International Business. *Management international review : MIR : journal of international business*, *63*(1), 3-25. https://doi.org/10.1007/s11575-022-00489-8

[46] Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Giones, F., Hakala, H., Marullo, C., Mention, A. L., Mortara, L., Nørskov, S., Nylund, P. A., Oddo, C. M., Radziwon, A., & Ritala, P. (2022). Digital transformation, for better or worse: a critical multi‐level research agenda. *R&D Management*, *52*(5), 930-954. https://doi.org/10.1111/radm.12531

[47] Dasgupta, A., & Islam, M. M., Nahid, Omar Faruq, Rahmatullah, Rafio, . (2024). Engineering Management Perspectives on Safety Culture in Chemical and Petrochemical Plants: A Systematic Review. *Academic Journal On Science, Technology, Engineering & Mathematics Education*, *1*(1), 10.69593.

[48] de Matos, M. G., & Adjerid, I. (2022). Consumer Consent and Firm Targeting After GDPR: The Case of a Large Telecom Provider. *Management Science*, *68*(5), 3330-3378. https://doi.org/10.1287/mnsc.2021.4054

[49] De Sutter, E., Meszaros, J., Borry, P., & Huys, I. (2022). Digitizing the Informed Consent Process: A Review of the Regulatory Landscape in the European Union. *Frontiers in medicine*, *9*(NA), 906448-NA. https://doi.org/10.3389/fmed.2022.906448

[50] Del Alamo, J. M., Guamán, D. S., Balmori, B., & Diez, A. (2021). Privacy Assessment in Android Apps: A Systematic Mapping Study. *Electronics*, *10*(16), 1999-NA. https://doi.org/10.3390/electronics10161999

[51] Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105342-NA. https://doi.org/10.1016/j.clsr.2019.105342

[52] Desai, D. R. (2013). Beyond location: data security in the 21st century. *Communications of the ACM*, *56*(1), 34-36. https://doi.org/10.1145/2398356.2398368

[53] Díaz-Pérez, L. C., Quintanar-Reséndiz, A. L., Vázquez-Álvarez, G., & Vázquez-Medina, R. (2022). A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology. *Applied Computing and Informatics*. https://doi.org/10.1108/aci-01-2022-0010

[54] Doh, J. P., Eden, L., Tsui, A. S., & Zaheer, S. (2023). Developing international business scholarship for global societal impact. *Journal of International Business Studies*, *54*(5), 757-767. https://doi.org/10.1057/s41267-023-00603-4

[55] Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review*, *37*(NA), 105412-NA. https://doi.org/10.1016/j.clsr.2020.105412

[56] Duina, F., & Lenz, T. (2016). Regionalism and diffusion revisited: From final design towards stages of decision-making. *Review of International Studies*, *42*(4), 773-797. https://doi.org/10.1017/s0260210515000479

[57] El Haddouti, S., Ouaguid, A., & Ech-Cherif El Kettani, M. D. (2023). Fedidchain: An Innovative Blockchain-Enabled Framework for Cross-Border Interoperability and Trust Management in Identity Federation Systems. *Journal of Network and Systems Management*, *31*(2), NA-NA. https://doi.org/10.1007/s10922-023-09731-6

[58] Faiella, G., Komnios, I., Voss-Knude, M., Cano, I., Duquenoy, P., Nalin, M., Baroni, I., Matrisciano, F., & Clemente, F. (2018). *Euro-CYBERSEC - Building an Ethical Framework for Cross-Border Applications: The KONFIDO Project* (Vol. NA). Springer International Publishing. https://doi.org/10.1007/978-3-319-95189-8_4

[59] Faria, J., & Md Rashedul, I. (2025). Carbon Sequestration in Coastal Ecosystems: A Review of Modeling Techniques and Applications. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 41-70. https://doi.org/10.63125/4z73rb29

[60] Fernandes, J., Machado, C., & Amaral, L. (2023). Towards a readiness model derived from critical success factors, for the general data protection regulation implementation in higher education institutions. *Strategic Management*, *28*(1), 4-19. https://doi.org/10.5937/straman2200033f

[61] Ferracane, M. F., & van der Marel, E. (2021). *Regulating Personal Data* (Vol. NA). World Bank, Washington, DC. https://doi.org/10.1596/1813-9450-9596

[62] Fonseca, M., Karkaletsis, K., Cruz, I., Berler, A., & Oliveira, I. C. (2015). MIE - OpenNCP: a novel framework to foster cross-border e-Health services. *Studies in health technology and informatics*, *210*(NA), 617-621. https://doi.org/NA

[63] Freund, G. P., Fagundes, P. B., & de Macedo, D. D. J. (2020). An Analysis of Blockchain and GDPR under the Data Lifecycle Perspective. *Mobile Networks and Applications*, *26*(1), 266-276. https://doi.org/10.1007/s11036-020-01646-9

[64] George, L., & Kizhakkethottam, J. J. (2021). A COMPARATIVE STUDY OF ZERO KNOWLEDGE PROOF AND HOMOMORPHIC ENCRYPTION IN GUARANTEEING DATA PRIVACY IN BLOCKCHAIN APPLICATIONS. *International Journal of Advanced Research*, *9*(02), 359-361. https://doi.org/10.21474/ijar01/12455

[65] Ghosh, B. C., Ramakrishna, V., Govindarajan, C., Behl, D., Karunamoorthy, D., Abebe, E., & Chakraborty, S. (2021). *IEEE ICBC - Decentralized Cross-Network Identity Management for Blockchain Interoperation* (Vol. NA). IEEE. https://doi.org/10.1109/icbc51069.2021.9461064

[66] Gilbert, F. (2012). European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies. *Santa Clara High Technology Law Journal*, *28*(4), 815-NA. https://doi.org/NA

[67] Graham, E. R., Shipan, C. R., & Volden, C. (2012). The Diffusion of Policy Diffusion Research in Political Science. *British Journal of Political Science*, *43*(3), 673-701. https://doi.org/10.1017/s0007123412000415

[68] Greenleaf, G. (2014). *Asian Data Privacy Laws* (Vol. NA). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199679669.001.0001

[69] Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. *SSRN Electronic Journal*, *NA*(NA), NA-NA. https://doi.org/10.2139/ssrn.3836348

[70] Guamán, D. S., Del Alamo, J. M., & Caiza, J. C. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*(NA), 15961-15982. https://doi.org/10.1109/access.2021.3053130

[71] Guamán, D. S., Rodriguez, D., del Alamo, J. M., & Such, J. (2023). Automated GDPR compliance assessment for cross-border personal data transfers in android applications. *Computers & Security*, *130*, 103262-103262. https://doi.org/10.1016/j.cose.2023.103262

[72] Hansen, M. (2012). *PrimeLife - Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals* (Vol. NA). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-31668-5_2

[73] Hasan, Z., Haque, E., Khan, M. A. M., & Khan, M. S. (2024). Smart Ventilation Systems For Real-Time Pollution Control: A Review Of Ai-Driven Technologies In Air Quality Management. *Frontiers in Applied Engineering and Technology*, *1*(01), 22-40. https://doi.org/10.70937/faet.v1i01.4

[74] Helal, A. M. (2022). State Of Indigenous Cultural Practices And Role Of School Curriculum: A Case Study Of The Garo Community In Bangladesh. *Available at SSRN 5061810*.

[75] Helal, A. M. (2024). Unlocking Untapped Potential: How Machine Learning Can Bridge the Gifted Identification Gap (2024).

[76] Helal, A. M., Wai, J., Parra-Martinez, A., McKenzie, S., & Seaton, D. (2025). Widening the Net: How CogAT and ACT Aspire Compare in Gifted Identification.

[77] Henriksen-Bulmer, J., Yucel, C., Faily, S., & Chalkias, I. (2022). Privacy Goals for the Data Lifecycle. *Future Internet*, *14*(11), 315-315. https://doi.org/10.3390/fi14110315

[78] Hintze, M. (2017). Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. *International Data Privacy Law*, *8*(1), 86-101. https://doi.org/10.1093/idpl/ipx020

[79] Hossain, A., Khan, M. R., Islam, M. T., & Islam, K. S. (2024). Analyzing The Impact Of Combining Lean Six Sigma Methodologies With Sustainability Goals. *Journal of Science and Engineering Research*, *1*(01), 123-144. https://doi.org/10.70008/jeser.v1i01.57

[80] Hossain, K., Alam, K., & Khan, U. S. (2018). Data Privacy in Bangladesh A Review of Three Key Stakeholders Perspectives. *Seventh International Conference on Advances in Social Science, Economics and Management Study - SEM 2018*, *NA*(NA), 46-50. https://doi.org/10.15224/978-1-63248-164-1-32

[81] Hossain, M. R., Mahabub, S., & Das, B. C. (2024). The role of AI and data integration in enhancing data protection in US digital public health an empirical study. *Edelweiss Applied Science and Technology*, *8*(6), 8308-8321.

[82] Ioannou, A., & Tussyadiah, I. P. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in society*, *67*(NA), 101774-NA. https://doi.org/10.1016/j.techsoc.2021.101774

[83] Islam, M. M. (2024). Systematic Review Of Risk Management Strategies In Rebar Procurement And Supply Chain Within The Construction Industry. *Innovatech Engineering Journal*, *1*(01), 1-21. https://doi.org/10.70937/itej.v1i01.1

[84] Islam, M. M., Prodhan, R. K., Shohel, M. S. H., & Morshed, A. S. M. (2025). Robotics and Automation in Construction Management Review Focus: The application of robotics and automation technologies in construction. *Journal of Next-Gen Engineering Systems*, *2*(01), 48-71. https://doi.org/10.70937/jnes.v2i01.63

[85] Islam, M. N., & Helal, A. M. (2018). Primary school governance in Bangladesh: A practical overview of national education policy-2010. *International Journal for Cross-Disciplinary Subjects in Education (IJCDSE)*, *9*(4).

[86] Islam, M. T. (2024). A Systematic Literature Review On Building Resilient Supply Chains Through Circular Economy And Digital Twin Integration. *Frontiers in Applied Engineering and Technology*, *1*(01), 304-324. https://doi.org/10.70937/faet.v1i01.44

[87] Islam, M. T., Islam, K. S., Hossain, A., & Khan, M. R. (2025). Reducing Operational Costs in U.S. Hospitals Through Lean Healthcare And Simulation-Driven Process Optimization. *Journal of Next-Gen Engineering Systems*, *2*(01), 11-28. https://doi.org/10.70937/jnes.v2i01.50

[88] Jahan, F. (2023). Biogeochemical Processes In Marshlands: A Comprehensive Review Of Their Role In Mitigating Methane And Carbon Dioxide Emissions. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(01), 33-59. https://doi.org/10.62304/jieet.v2i01.230

[89] Jahan, F. (2024). A Systematic Review Of Blue Carbon Potential in Coastal Marshlands: Opportunities For Climate Change Mitigation And Ecosystem Resilience. *Frontiers in Applied Engineering and Technology*, *2*(01), 40-57. https://doi.org/10.70937/faet.v2i01.52

[90] Jia, Q., Zhou, L., Li, H., Yang, R., Du, S., & Zhu, H. (2019). WASA - Who Leaks My Privacy: Towards Automatic and Association Detection with GDPR Compliance. In (Vol. NA, pp. 137-148). Springer International Publishing. https://doi.org/10.1007/978-3-030-23597-0_11

[91] Kalyvakİ, M. (2023). Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse*, *3*(1), 87-92. https://doi.org/10.57019/jmv.1238344

[92] Kapsis, I. (2020). A Truly Future-Oriented Legal Framework for Fintech in the EU. *European Business Law Review*, *31*(Issue 3), 475-514. https://doi.org/10.54648/eulr2020020

[93] Kassem, J. A., Sayeed, S., Marco-Gisbert, H., Pervez, Z., & Dahal, K. (2019). DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. *Applied Sciences*, *9*(15), 2953-NA. https://doi.org/10.3390/app9152953

[94] Katkuri, S. (2024). Securing the Digital Frontier: Legal Analysis of Cybersecurity, Data Privacy and Cyber Forensics in India. *Indian Journal of Public Administration*, *71*(1), 75-91. https://doi.org/10.1177/00195561241284886

[95] Khan, M. A. M. (2025). AI And Machine Learning in Transformer Fault Diagnosis: A Systematic Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 290-318. https://doi.org/10.63125/sxb17553

[96] Khan, M. A. M., & Aleem Al Razee, T. (2024). Lean Six Sigma Applications In Electrical Equipment Manufacturing: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *5*(02), 31- 63. https://doi.org/10.63125/hybvmw84

[97] Kingston, J. (2017). Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation. *Artificial Intelligence and Law*, *25*(4), 429-443. https://doi.org/10.1007/s10506-017-9206-9

[98] Ko, H., Leitner, J. M., Kim, E.-S., & Jeong, J. (2017). Structure and enforcement of data privacy law in South Korea. *International Data Privacy Law*, *7*(2), 100-114. https://doi.org/10.1093/idpl/ipx004

[99] Kostka, G., & Antoine, L. (2019). Fostering Model Citizenship: Behavioral Responses to China's Emerging Social Credit Systems. *Policy & Internet*, *12*(3), 256-289. https://doi.org/10.1002/poi3.213

[100] Kranenborg, H. (2016). O. Lynskey, The Foundations of EU Data Protection Law. *International Data Privacy Law*, *6*(4), 324-326. https://doi.org/10.1093/idpl/ipw017

[101] Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16-44. https://doi.org/10.1177/02683962221141456

[102] Larrucea, X., Moffie, M., Asaf, S., & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Computer Standards & Interfaces*, *69*(NA), 103408-NA. https://doi.org/10.1016/j.csi.2019.103408

[103] Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, *2025*(1). https://doi.org/10.1049/ise2/5536763

[104] Lips, S., Bharosa, N., & Draheim, D. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In (Vol. NA, pp. 75-89). Springer International Publishing. https://doi.org/10.1007/978-3-030-67238-6_6

[105] Liu, J., & Zhao, H. (2021). Privacy lost: Appropriating surveillance technology in China's fight against COVID-19. *Business horizons*, *64*(6), 743-756. https://doi.org/10.1016/j.bushor.2021.07.004

[106] Lorè, F., Basile, P., Appice, A., de Gemmis, M., Malerba, D., & Semeraro, G. (2023). An AI framework to support decisions on GDPR compliance. *Journal of Intelligent Information Systems*, *61*(2), 541-568. https://doi.org/10.1007/s10844-023-00782-4

[107] Luo, Y. (2021). A general framework of digitization risks in international business. *Journal of International Business Studies*, *53*(2), 1-18. https://doi.org/10.1057/s41267-021-00448-9

[108] Lyle, J. R., Guttman, B., Butler, J. M., Sauerwein, K., Reed, C., & Lloyd, C. E. (2022). Digital Investigation Techniques. *NA*, *NA*(NA), NA-NA. https://doi.org/10.6028/nist.ir.8354-draft

[109] Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps? *Information & Communications Technology Law*, *26*(2), 146-197. https://doi.org/10.1080/13600834.2017.1321096

[110] Madan, S., Savani, K., & Katsikeas, C. S. (2022). Privacy please: Power distance and people's responses to data breaches across countries. *Journal of International Business Studies*, *54*(4), 731-754. https://doi.org/10.1057/s41267-022-00519-5

[111] Mahabub, S., Das, B. C., & Hossain, M. R. (2024). Advancing healthcare transformation: AI-driven precision medicine and scalable innovations through data analytics. *Edelweiss Applied Science and Technology*, *8*(6), 8322-8332.

[112] Mahabub, S., Jahan, I., Hasan, M. N., Islam, M. S., Akter, L., Musfiqur, M., Foysal, R., & Onik, M. K. R. (2024). Efficient detection of tomato leaf diseases using optimized Compact Convolutional Transformers (CCT) Model.

[113] Mahabub, S., Jahan, I., Islam, M. N., & Das, B. C. (2024). The Impact of Wearable Technology on Health Monitoring: A Data-Driven Analysis with Real-World Case Studies and Innovations. *Journal of Electrical Systems*, *20*.

[114] Md, A., Rokhshana, P., Mahiya Akter, S., & Anisur, R. (2025). AI-POWERED PERSONALIZATION IN DIGITAL BANKING: A REVIEW OF CUSTOMER BEHAVIOR ANALYTICS AND ENGAGEMENT. *American Journal of Interdisciplinary Studies*, *6*(1), 40- 71. https://doi.org/10.63125/z9s39s47

[115] Md Mahfuj, H., Md Rabbi, K., Mohammad Samiul, I., Faria, J., & Md Jakaria, T. (2022). Hybrid Renewable Energy Systems: Integrating Solar, Wind, And Biomass for Enhanced Sustainability And Performance. *American Journal of Scholarly Research and Innovation*, *1*(1), 1-24. https://doi.org/10.63125/8052hp43

[116] Md Majharul, I., Arafat Bin, F., & Ripan Kumar, P. (2022). AI-Based Smart Coating Degradation Detection For Offshore Structures. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 01-34. https://doi.org/10.63125/1mn6bm51

[117] Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[118] Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[119] Md, W., Md Zahin Hossain, G., Md Tarek, H., Md Khorshed, A., Mosa Sumaiya Khatun, M., & Noor Alam, S. (2025). Assessing The Influence of Cybersecurity Threats And Risks On The Adoption And Growth Of Digital Banking: A Systematic Literature Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 226-257. https://doi.org/10.63125/fh49gz18

[120] Md. Rafiqul Islam, R., Iva, M. J., Md Merajur, R., & Md Tanvir Hasan, S. (2024, 2024/01/25). Investigating Modern Slavery in the Post-Pandemic Textile and Apparel Supply Chain: An Exploratory Study. International Textile and Apparel Association Annual Conference Proceedings,

[121] Meltzer, J. P. (2014). The Internet, Cross‐Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, *2*(1), 90-102. https://doi.org/10.1002/app5.60

[122] Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R.-J. B. (2023). International business in the digital age: Global strategies in a world of national institutions. *Journal of International Business Studies*, *54*(4), 577-598. https://doi.org/10.1057/s41267-023-00618-x

[123] Mishra, N. (2020). The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance. *Journal of World Trade*, *54*(Issue 4), 567-590. https://doi.org/10.54648/trad2020025

[124] Mitchell, A. D., & Mishra, N. (2019). Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. *Journal of International Economic Law*, *22*(3), 389-416. https://doi.org/10.1093/jiel/jgz016

[125] Miyashita, H. (2011). The evolving concept of data privacy in Japanese law. *International Data Privacy Law*, *1*(4), 229-238. https://doi.org/10.1093/idpl/ipr019

[126] Mohammad Shahadat Hossain, S., Md Shahadat, H., Saleh Mohammad, M., Adar, C., & Sharif Md Yousuf, B. (2024). Advancements In Smart and Energy-Efficient HVAC Systems: A Prisma-Based Systematic Review. *American Journal of Scholarly Research and Innovation*, *3*(01), 1-19. https://doi.org/10.63125/ts16bd22

[127] Mridha Younus, S. H., amp, & Md Morshedul, I. (2024). Advanced Business Analytics in Textile & Fashion Industries: Driving Innovation And Sustainable Growth. *International Journal of Management Information Systems and Data Science*, *1*(2), 37-47. https://doi.org/10.62304/ijmisds.v1i2.143

[128] Mridha Younus, S. H. P. M. R. A. I. T., amp, & Rajae, O. (2024). Sustainable Fashion Analytics: Predicting The Future of Eco-Friendly Textile. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(03), 13-26. https://doi.org/10.62304/jbedpm.v3i03.85

[129] Muhammad Mohiul, I., Morshed, A. S. M., Md Enamul, K., & Md, A.-A. (2022). Adaptive Control Of Resource Flow In Construction Projects Through Deep Reinforcement Learning: A Framework For Enhancing Project Performance In Complex Environments. *American Journal of Scholarly Research and Innovation*, *1*(01), 76-107. https://doi.org/10.63125/gm77xp11

[130] Nahid, O. F., Rahmatullah, R., Al-Arafat, M., Kabir, M. E., & Dasgupta, A. (2024). Risk mitigation strategies in large scale infrastructure project:a project management perspective. *Journal of Science and Engineering Research*, *1*(01), 21-37. https://doi.org/10.70008/jeser.v1i01.38

[131] Nalin, M., Baroni, I., Faiella, G., Romano, M., Matrisciano, F., Gelenbe, E., Martinez, D., Dumortier, J., Natsiavas, P., Votis, K., Koutkias, V., Tzovaras, D., & Clemente, F. (2019). The European cross-border health data exchange roadmap: Case study in the Italian setting. *Journal of biomedical informatics*, *94*, 103183-103183. https://doi.org/10.1016/j.jbi.2019.103183

[132] Oh, J., Hong, J., Lee, C., Lee, J. J., Woo, S. S., & Lee, K. (2021). Will EU's GDPR Act as an Effective Enforcer to Gain Consent? *IEEE Access*, *9*(NA), 79477-79490. https://doi.org/10.1109/access.2021.3083897

[133] Oluwatosin, R., Nkechi Emmanuella, E., Benedicta, E., Anthony, A., Temidayo, O., & Temitayo Oluwaseun, A. (2024). PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT. *International Journal of Applied Research in Social Sciences*, *6*(1), 73-88. https://doi.org/10.51594/ijarss.v6i1.733

[134] Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*(8), 575-582. https://doi.org/10.1007/s00439-018-1919-7

[135] Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5), 510-524. https://doi.org/10.1108/dprg-05-2019-0039

[136] Porwal, S., Nair, S. K., & Dimitrakos, T. (2011). IFIPTM - Regulatory Impact of Data Protection and Privacy in the Cloud. In (Vol. NA, pp. 290-299). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22200-9_23

[137] Presthus, W., & Sørum, H. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Procedia Computer Science*, *138*(NA), 603-611. https://doi.org/10.1016/j.procs.2018.10.081

[138] Rahaman, T., Siddikui, A., Abid, A.-A., & Ahmed, Z. (2024). Exploring the Viability of Circular Economy in Wastewater Treatment Plants: Energy Recovery and Resource Reclamation. *Well Testing*, *33*(S2).

[139] Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A., & Filippidis, A. P. (2019). A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem. *Security and Communication Networks*, *2019*(NA), 1-15. https://doi.org/10.1155/2019/1431578

[140] Rasmussen, J., Natsiavas, P., Votis, K., Moschou, K., Campegiani, P., Coppolino, L., Cano, I., Marí, D., Faiella, G., Stan, O., Abdelrahman, O., Nalin, M., Baroni, I., Voss-Knude, M., Vella, V. A., Grivas, E., Mesaritakis, C., Dumortier, J., Petersen, J., . . . Koutkias, V. (2017). Gap Analysis for Information Security in Interoperable Solutions at a Systemic Level: The KONFIDO Approach. In (Vol. 66, pp. 75-79). Springer Singapore. https://doi.org/10.1007/978-981-10-7419-6_13

[141] Ripan Kumar, P., Md Majharul, I., & Arafat Bin, F. (2022). Integration Of Advanced NDT Techniques & Implementing QA/QC Programs In Enhancing Safety And Integrity In Oil & Gas Operations. *American Journal of Interdisciplinary Studies*, *3*(02), 01-35. https://doi.org/10.63125/9pzxgq74

[142] Robol, M., Breaux, T. D., Paja, E., & Giorgini, P. (2023). Consent Verification Monitoring. *ACM Transactions on Software Engineering and Methodology*, *32*(1), 1-33. https://doi.org/10.1145/3490754

[143] Roksana, H., Ammar, B., Noor Alam, S., & Ishtiaque, A. (2024). Predictive Maintenance in Industrial Automation: A Systematic Review Of IOT Sensor Technologies And AI Algorithms. *American Journal of Interdisciplinary Studies*, *5*(01), 01-30. https://doi.org/10.63125/hd2ac988

[144] Roy, P. P., Abdullah, M. S., & Sunny, M. A. U. (2024). Revolutionizing Structural Engineering: Innovations in Sustainable Design and Construction. *European Journal of Advances in Engineering and Technology*, *11*(5), 94-99.

[145] Sabid, A. M., & Kamrul, H. M. (2024). Computational And Theoretical Analysis On The Single Proton Transfer Process In Adenine Base By Using DFT Theory And Thermodynamics. *IOSR Journal of Applied Chemistry*.

[146] Sarker, M. T. H. (2025). Case Study Analysis of AI-Powered Sensor Fabrics for Continuous Health Monitoring in Chronic Disease Management. *Strategic Data Management and Innovation*, *2*(01), 160-180. https://doi.org/10.71292/sdmi.v2i01.18

[147] Schwartz, P. M., & Reidenberg, J. R. (1996). *Data Privacy Law: A Study of United States Data Protection* (Vol. NA). NA. https://doi.org/NA

[148] Shahan, A., Anisur, R., & Md, A. (2023). A Systematic Review Of AI And Machine Learning-Driven IT Support Systems: Enhancing Efficiency And Automation In Technical Service Management. *American Journal of Scholarly Research and Innovation*, *2*(02), 75-101. https://doi.org/10.63125/fd34sr03

[149] Sharif, K. S., Uddin, M. M., & Abubakkar, M. (2024, 17-19 Dec. 2024). NeuroSignal Precision: A Hierarchical Approach for Enhanced Insights in Parkinson's Disease Classification. 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA),

[150] Shimul, A. I., Haque, M. M., Ghosh, A., Sunny, M. A. U., Aljazzar, S. O., Al-Humaidi, J. Y., & Mukhrish, Y. E. (2025). Hydrostatic Pressure-Driven Insights into Structural, Electronic, Optical, and Mechanical Properties of A3PCl3 (A = Sr, Ba) Cubic Perovskites for Advanced Solar Cell Applications. *Journal of Inorganic and Organometallic Polymers and Materials*. https://doi.org/10.1007/s10904-025-03629-3

[151] Shohel, M. S. H., Islam, M. M., Prodhan, R. K., & Morshed, A. S. M. (2024). Lifecycle Management Of Renewable Energy Systems In Residential Housing Construction. *Frontiers in Applied Engineering and Technology*, *1*(01), 124-138. https://doi.org/10.70937/faet.v1i01.23

[152] Sim, J., Kim, B., Jeon, K., Joo, M., Lim, J., Lee, J., & Choo, K.-K. R. (2023). Technical Requirements and Approaches in Personal Data Control. *ACM Computing Surveys*, *55*(9), 1-30. https://doi.org/10.1145/3558766

[153] Simmons, B. A., Dobbin, F., & Garrett, G. (2006). Introduction: The International Diffusion of Liberalism. *International Organization*, *60*(04), 781-810. https://doi.org/10.1017/s0020818306060267

[154] Singla, A., Gupta, N., Aeron, P., Jain, A., Sharma, D., & Bharadwaj, S. S. (2022). Decentralized Identity Management Using Blockchain. *Journal of Global Information Management*, *31*(2), 1-24. https://doi.org/10.4018/jgim.315283

[155] Soemarwi, V. W. S., & Susanto, W. (2021). Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right. *Advances in Social Science, Education and Humanities Research*, *NA*(NA), 561-566. https://doi.org/10.2991/assehr.k.210805.088

[156] Sohel, A., Alam, M. A., Hossain, A., Mahmud, S., & Akter, S. (2022). Artificial Intelligence In Predictive Analytics For Next-Generation Cancer Treatment: A Systematic Literature Review Of Healthcare Innovations In The USA. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 62-87. https://doi.org/10.62304/jieet.v1i01.229

[157] Sohel, R. (2025). AI-Driven Fault Detection and Predictive Maintenance In Electrical Power Systems: A Systematic Review Of Data-Driven Approaches, Digital Twins, And Self-Healing Grids. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 258-289. https://doi.org/10.63125/4p25x993

[158] Solingen, E. (2012). Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion. *International Studies Quarterly*, *56*(4), 631-644. https://doi.org/10.1111/isqu.12034

[159] Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477-NA. https://doi.org/10.2307/40041279

[160] Sunstein, C. R. (2014). The Regulatory Lookback. *Boston University Law Review*, *94*(3), 579-NA. https://doi.org/NA

[161] Tallon, P. P., Ramirez, R., & Short, J. E. (2013). The Information Artifact in IT Governance: Toward a Theory of Information Governance. *Journal of Management Information Systems*, *30*(3), 141-178. https://doi.org/10.2753/mis0742-1222300306

[162] Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8. https://doi.org/10.1016/s1353-4858(16)30056-3

[163] Tatarinov, K., Ambos, T. C., & Tschang, F. T. (2022). Scaling digital solutions for wicked problems: Ecosystem versatility. *Journal of International Business Studies*, *54*(4), 631-656. https://doi.org/10.1057/s41267-022-00526-6

[164] Teixeira, G. A., da Silva, M. M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402-418. https://doi.org/10.1108/dprg-01-2019-0007

[165] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU general data protection regulation : changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

[166] Timan, T., & Mann, Z. Á. (2021). Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In (Vol. NA, pp. 153-175). Springer International Publishing. https://doi.org/10.1007/978-3-030-68176-0_7

[167] Todde, M., Beltrame, M., Marceglia, S., & Spagno, C. (2020). Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. *Informatics in Medicine Unlocked*, *19*(NA), 100361-100369. https://doi.org/10.1016/j.imu.2020.100361

[168] Tonoy, A. A. R. (2022). Mechanical Properties and Structural Stability of Semiconducting Electrides: Insights For Material. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 18-35. https://doi.org/10.62304/jieet.v1i01.225

[169] van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776

[170] Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, *8*(2), 105-123. https://doi.org/10.1093/idpl/ipy002

[171] Verdier, P.-H. (2011). Mutual recognition in international finance. *Harvard International Law Journal*, *52*(1), 55-108. https://doi.org/NA

[172] Vogel, D. (1997). Trading up and governing across: transnational governance and environmental protection. *Journal of European Public Policy*, *4*(4), 556-571. https://doi.org/10.1080/135017697344064

[173] Vojvodic, M., & Hitz, C. (2019). Governance team leadership and business user participation : organizational practices for innovative customer engagement in data compliance project. *Central European Business Review*, *8*(2), 15-45. https://doi.org/10.18267/j.cebr.214

[174] Wang, Z., Stell, A., Sinnott, R. O., & The Addn Study Group, N. A. (2023). A GDPR-Compliant Dynamic Consent Mobile Application for the Australasian Type-1 Diabetes Data Network. *Healthcare (Basel, Switzerland)*, *11*(4), 496-496. https://doi.org/10.3390/healthcare11040496

[175] Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research*, *20*(3), 565-587. https://doi.org/10.1007/s10660-020-09422-3

[176] Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. *Government Information Quarterly*, *31*(1), 150-159. https://doi.org/10.1016/j.giq.2013.07.003

[177] Wunsch-Vincent, S. (2006). The Internet, cross-border trade in services, and the GATS: lessons from US–Gambling. *World Trade Review*, *5*(03), 319-355. https://doi.org/10.1017/s1474745606002965

[178] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2), 127-NA. https://doi.org/10.1007/s42979-022-01020-4

[179] Xu, W., Wang, S., & Zuo, X. (2024). Global data governance at a turning point? Rethinking China-U.S. cross-border data flow regulatory models. *Computer Law & Security Review*, *55*, 106061. https://doi.org/10.1016/j.clsr.2024.106061

[180] Yao-Huai, L. (2005). Privacy and Data Privacy Issues in Contemporary China. *Ethics and Information Technology*, *7*(1), 7-15. https://doi.org/10.1007/s10676-005-0456-y

[181] Yeung, K., & Bygrave, L. A. (2021). Demystifying the modernized European data protection regime: cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137-155. https://doi.org/10.1111/rego.12401

[182] You, C. (2020). Law and policy of platform economy in China. *Computer Law & Security Review*, *39*(NA), 105493-NA. https://doi.org/10.1016/j.clsr.2020.105493

[183] Younus, M. (2022). Reducing Carbon Emissions in The Fashion And Textile Industry Through Sustainable Practices and Recycling: A Path Towards A Circular, Low-Carbon Future. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *1*(1), 57-76. https://doi.org/10.62304/jbedpm.v1i1.226

[184] Younus, M. (2025). The Economics of A Zero-Waste Fashion Industry: Strategies To Reduce Wastage, Minimize Clothing Costs, And Maximize & Sustainability. *Strategic Data Management and Innovation*, *2*(01), 116-137. https://doi.org/10.71292/sdmi.v2i01.15

[185] Zaeem, R. N., & Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Transactions on Management Information Systems*, *12*(1), 1-20. https://doi.org/10.1145/3389685

[186] Zaguir, N. A., de Magalhães, G. H., & de Mesquita Spinola, M. (2024). Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. *IEEE Access*, *12*, 81608-81630. https://doi.org/10.1109/access.2024.3406724

[187] Zetzsche, D. A., Anker-Sørensen, L., Passador, M. L., & Wehrli, A. (2021). DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. *Law and Financial Markets Review*, *15*(1-2), 70-115. https://doi.org/10.1080/17521440.2022.2065809

[188] Zhang, H., & Gong, X. (2023). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, *28*(1), 21-44. https://doi.org/10.1177/13657127231187059

[189] Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*(NA), 105610-NA. https://doi.org/10.1016/j.clsr.2021.105610

[190] Zwingelberg, H., & Hansen, M. (2012). *PrimeLife - Privacy Protection Goals and Their Implications for eID Systems* (Vol. NA). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-31668-5_19