IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comparative Analysis Of Global Data Protection Regulations

[1]Srinath Muralinathan

[1]University of North Carolina at Charlotte

Abstract: The study is mainly focusing on global data protection regulations such as GDPR, CCPA, PDPA, LGPD, and PIPL that protect individual identities in the new digital age. It examines their legal scope, Rights of Data Subjects, Compliance Requirements, Enforcement Mechanism, and Regulations on Cross-border Data Transfer. It shows variations in enforcement strategies, penalties, and applicability while these regulations share the same principles like transparency, user control, and accountability. The paper also discusses the challenges that businesses have to face in compliance across various jurisdictions, the effectiveness of those regulations concerning consumer rights, and the influence of emerging technologies like artificial intelligence and big data. The study ends with proposals towards greater international harmonization in data protection laws along with recommendations to policymakers, organizations as well, and researchers.

Index Terms - Data Protection, GDPR, CCPA, Privacy Regulations, Global Compliance, Cross-Border Data Transfers, Digital Rights.

I. INTRODUCTION

With the advent of the new millennium, data became the most precious element in fuelling the economies, businesses, and governments all around the world. The invention and vigorous development of modern digital technologies; artificial intelligence, cloud computing, and the Internet of Things (IoT), have ushered in an unrelenting generation and collection of personal data on an absolute scale. This digital transformation has improved efficiency, accessibility, and connectivity but has severely exposed individuals to massive privacy risks, including data breaches, unauthorized surveillance, and even identity theft.

Relevance and Significance of the Topic

Thus, regulations have been instituted by governments and regulatory bodies that seal the rights and control an individual would have over personal information [3]. How scope varies widely across jurisdictions in regard to mechanisms of enforcement and compliance requirements is positivelly the broadest angle of concern. The European Union's General Data Protection Regulation (GDPR), on the one hand, is popularly viewed as the gold standard of data protection by virtue of its stringent provisions and extraterritorial applicability [4]; on the other, the California Consumer Privacy Act emphasizes consumer rights within a business-friendly framework. PIPL, China's Personal Information Protection Law, takes a government-centric perspective of data governance, echoing national security concerns that are wider and deeper in scope [5].

With these, a full comparative and contrastive analysis can be instrumental in understanding the effectiveness of data protection and its challenges along with global trends. This can help policymakers, businesses, and researchers design a harmonized approach toward data privacy regarding individual rights, innovation, and economic interests with the knowledge of strengths and weaknesses in regulatory frameworks.

Objective of the Study

This study aims to conduct a comparative analysis of major global data protection regulations to identify commonalities, differences, and potential areas for harmonization. The key objectives include:

- Comparing Legal Frameworks: Analyzing key provisions, enforcement mechanisms, and compliance obligations in major data protection laws.
- Assessing Effectiveness: Evaluating how well different regulations protect individuals' data rights and mitigate privacy risks.
- Identifying Gaps & Challenges: Highlighting inconsistencies, regulatory loopholes, and challenges businesses face in compliance.
- Exploring Cross-Border Data Governance: Examining how different laws handle international data transfers and their implications for global trade.
- Providing Policy Recommendations: Offering insights for governments, businesses, and policymakers to improve data protection frameworks.

By addressing these objectives, the study contributes to the broader discourse on data sovereignty, privacy rights, and regulatory convergence in the digital economy.

Research Questions

To achieve these objectives, the study is guided by the following key research questions:

1. How do major data protection regulations (e.g., GDPR, CCPA, LGPD, PIPL) compare in terms of legal scope, principles, and enforcement?
2. What are the similarities and differences in how these laws define data subject rights, obligations for businesses, and enforcement mechanisms?
3. How effective are these regulations in preventing data breaches, ensuring compliance, and empowering individuals with control over their personal data?
4. What challenges do businesses face in complying with multiple regulations, and how do they navigate cross-border data transfer restrictions?
5. Are there existing trends toward global harmonization of data protection laws, and what role do international organizations play in this process?

II. Overview of Major Data Protection Regulations

With the increasing use of digital platforms for communication, commerce, and governance, there have arisen the demands for strong data protection laws in different jurisdictions. There are some principles that link these sets of regulations, such as transparency, accountability, and rights of the consumers; however, important variations remain in their scope, enforcement mechanisms, and compliance [6]. This section will then proceed to analyze and provide insights into some of the prominent data protection laws across the world, outlining the legal framework applicable to these laws, as well as the implications upon businesses and individuals.

General Data Protection Regulation (GDPR) – European Union

The General Data Protection Regulation (GDPR) is one of the broadest frameworks for data protection around the world, put in force from May 25, 2018. The GDPR is applicable to all those persons who process personal data of living individuals within the European Union (EU) and European Economic Area (EEA), even if they are neither incorporated nor established in the territory of an EU member state [8]. The regulation has established minimum conditions governing the collection, processing and transfer of personal data, ensuring people are informed about, and entitled to control, the use of their information [9]. Processing must be legally authorized on the basis of one or more of the conditions outlined in the GDPR such as: user consent, requirement of a contract, legal obligation, or legitimate interest. The rights granted to data subjects are broad and include the right to access, rectify and erase their data, the right to data portability, and the right to object to processing [10]. Privacy by Design and Default it principles must also be applied, in which protection should be there from the beginning stage of business fractions. Other than that, GDPR enforces a very strict regulation regarding data breach notifications, where organizations report a breach of personal data to the appropriate supervisory authority within 72 hours. Failure to adhere to GDPR can bring severe penalties, including fines of up to €20 million or 4% of the annual global turnover

of the company-in whichever is higher [11]. Indeed, the enforcement of GDPR has had a dramatic effect on data protection frameworks around the world, and many nations have copied similar principles [12].

California Consumer Privacy Act (CCPA) – United States

Among the various data privacy laws in the United States, the California Consumer Privacy Act (CCPA) is arguably one of the strictest. CCPA is not a law that entitles citizens of the EU to bring claims against all entities that handle personal data. Instead, it restricts itself to a business that does not operate in California, but conducts business within California or collects data from California residents. The law applies to any business that meets at least one of three criteria: $25 million or more in gross annual revenue; processes personal data of 50,000 or more consumers; and derives 50% or more of its annual revenue from selling consumer data [14]. The California Consumer Privacy Act offers rights similar to those under GDPR to residents of California, such as the right to know what data is collected, the right to request deletion of personal data, and the right to opt out of selling personal data to third parties. It differs from GDPR in that it does not require businesses to have a legal basis under which data can be processed, but rather focuses solely on giving consumers transparency and control over their data. The enforcement of this presumption is chiefly handled by the California Attorney General. The penalties for violations are set at $7,500 for each intentional violation. And $2,500 for unintentional violations [15]. CCPA, however, is thinner in scope than GDPR and does not have stringent principles of data processing such as purpose limitation and data minimization.

Personal Data Protection Act (PDPA) – Singapore

The Personal Data Protection Act (PDPA), introduced in 2012 and amended in 2020, serves to safeguard the collection, use, and disclosure of personal data by private entities in Singapore. The PDPA is a consent-based law in that it requires organizations to obtain explicit consent before any collection or processing of that data [16]. Contrary to the GDPR and CCPA, the PDPA lays emphasis on the alignment of business interests and the protection of consumer privacy. What sets it apart is the Do Not Call (DNC) Registry that prohibits unsolicited marketing messages to registered numbers [17]. It also provides a right to portability, allowing a person to switch data between service providers. Organizations must implement reasonable measures to secure personal data against unauthorized access. While any violation of PDPA may subject an organization to a penalty of up to SGD 1 million (~USD 750,000), in the event of a data breach, the company is obliged to notify the appropriate authorities within three calendar days [18]. The administration of PDPA enforcement has made Singapore a role model for data protection in the Asia-Pacific region.

Protection of Personal Information Act (POPIA) – South Africa

In essence, South Africa's principal legislation for data protection is the Protection of Personal Information Act, also known as POPIA, which became operational on 1 July 2021. POPIA is therefore based on international data and privacy concepts but is localized to South Africa's own legal and economic traditions [19]. The law covers both sectors, private and public, which handle personal data. In so doing, the act lays down the principle of lawfulness, accountability, and security safeguards [20]. The organizations should implement measures that are reasonable and technically feasible and designed to protect such information from security breaches. With its various legal bases for processing, the GDPR is very different from POPIA, which relies mainly on the consent of the data subject as its key processing ground to protect personal information [20], [21]. The body's enforcement mechanism, the Information Regulator of South Africa, has fine-imposing powers in an amount not exceeding ZAR 10 million (~USD 500,000) for an infringement, and in aggravated circumstances, a fine may go with imprisonment of up to 10 years. There are also stringent rules regarding cross-border data transfer under POPIA; for instance, organizations transferring data should ensure that countries of data receipt have comparable data protection standards.

Brazilian General Data Protection Law (LGPD) – Brazil

The Lei Geral de Proteção de Dados (LGPD) is a comprehensive data protection law analyzed after GDPR in Brazil, and it was established in September 2020. LGPD addresses any entity processing personal data from Brazilian residents, no matter where the organization may be located. Similar to GDPR, the LGPD establishes ten legal bases for data processing, including consent, contractual necessity, and compliance with a legal obligation. The regulation further introduces a new body for national enforcement, the National Data Protection Authority (ANPD), which is accountable for oversight and compliance [21]. Noncompliance with LGPD may lead to fines amounting to 2% of annual gross revenue of the offending organization capped at 50 million BRL (approximately 10 million USD) per infraction. Emphasized in the

LGPD is the appreciation for accountability and transparency through the implementation of privacy policies, as well as the appointment of data protection officers by organizations to oversee organizational compliance [22]. The Act is of huge significance for multinational companies doing business in Brazil as reconciliation of data processing activities with the LGPD will be mandatory.

China's Personal Information Protection Law (PIPL) – China

The Personal Information Protection Law (PIPL) of China has been implemented as from November 1, 2021. This law was established to be China's first general data protection law. PIPL is targeted to all entities, both private and public, and sets strict limits on cross-border data transfer by mandating security assessments from the relevant government authorities upon its departure with such data from China [24]. Unlike the General Data Protection Regulation, which permits several legal bases for processing data, PIPL is a strong advocate of obtaining independent consent for the processing of sensitive personal data [24][25]. There are fines up to 5% of a business' total annual revenue or CNY 50 million (~USD 7 million) for non-compliance with PIPL [26]. Enforcement under PIPL reflects China's approach to state-controlled data governance, which is significantly different from Western privacy law [27]. Most data protection laws around the world have an underlying foundation that is generally built on some fundamental principles toward guaranteeing data privacy, security, and accountability [28]. Among those are the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Data Protection Act (PDPA), Protection of Personal Information Act (POPIA), Brazilian General Data Protection Law (LGPD), and the Personal Information Protection Law (PIPL) of China, all of which had some common principles even if the implementation differed, with some containing lawfulness of processing, rights of data subjects, transparency, breach notification, and enforcement mechanisms [29]. The table 01 below shows the key similarities between these rules.

Table 1. Similarities & Harmonization Efforts Across Major Data Protection Regulations

PRINCIPLE	GDPR	CCPA	PDPA	POPIA	LGPD	PIPL
Lawfulness of Processing	Required legal basis	No specific basis required	Consent-based	Consent-based	10 legal bases, including consent & legal obligations	Primarily consent-based, strict rules for sensitive data
Data Subject Rights	Access, rectification, erasure, portability, objection	Access, deletion, opt-out of data sale	Access, correction, withdrawal of consent	Access, correction, erasure, restriction	Access, rectification, portability, objection	Access, correction, erasure, portability, right to explanation
Transparency & Notice	Privacy policies & explicit notices required	Businesses must disclose data collection practices	Clear notice to users required	Mandatory privacy policies	Transparency requirements for data collection	Users must be informed of processing activities
Breach Notification	Must notify regulator & individuals within 72 hours	No specific timeframe, but penalties for failure to disclose	Must notify regulator within 3 calendar days	Must notify regulator & affected individuals	Breach notification to ANPD required	Must notify authorities & individuals immediately
Enforcement Authority	Data Protection Authorities (DPAs) in each EU	California Attorney General, CPPA	Personal Data Protection Commiss	Information Regulator	National Data Protection Authority (ANPD)	Cyberspace Administration of China (CAC)

	member state		ion (PDPC)			

While many data protection frameworks share common principles, significant differences exist in legal definitions, obligations, and penalties. The key divergences include the definition of personal data, legal bases for processing, cross-border data transfer rules, enforcement mechanisms, and financial penalties for non-compliance. The table 02 below highlights these key differences.

Table 2. Key Differences & Divergences in Data Protection Regulations

ASPECT	GDPR (EU)	CCPA (USA)	PDPA (SINGAPORE)	POPIA (SOUTH AFRICA)	LGPD (BRAZIL)	PIPL (CHINA)
Definition of Personal Data	Broad, includes IP addresses, online identifiers	Broad, but mainly focused on identifiers & consumer data	Covers all identifiable personal data	Covers personal and special data	Covers identifiable personal data	Expansive, includes biometric & sensitive data
Legal Basis for Processing	Requires consent, contract, legal obligation, vital interest, public task, legitimate interest	No legal basis required, but opt-out is allowed	Primarily consent-based, some exceptions	Primarily consent-based	10 legal bases, including consent & legal obligations	Strict consent rules, especially for sensitive data
Cross-Border Data Transfers	Allowed with safeguards (adequacy decision, SCCs, BCRs)	No specific regulation	Allowed with safeguards & user consent	Only allowed to countries with equivalent protection	Allowed with safeguards or adequacy measures	Highly restricted, government security assessments required
Penalties for Non-Compliance	Up to 4% of global revenue or €20 million	$7,500 per intentional violation, $2,500 per unintentional	Up to SGD 1 million	Up to ZAR 10 million	Up to 2% of revenue, capped at 50M BRL	Up to 5% of revenue or CNY 50 million
Right to be Forgotten	Yes	No	Limited	Yes	Yes	Yes
Automated Decision-Making	Right to object & request human intervention	No specific provisions	No strict regulation	No explicit rules	Must provide explanation & allow challenge	Strict rules, requires separate consent
Data Localization	No, but must comply with transfer safeguards	No	No	No	No explicit localization requirement	Yes, strict data localization mandates

Despite strong legal frameworks, enforcement of data protection laws remains a significant challenge. Some regulations, like GDPR and PIPL, have imposed heavy fines, whereas others, such as PDPA and POPIA, face challenges in enforcement due to limited resources. The table 03 below presents case studies of major enforcement actions.

Table 3. Effectiveness & Enforcement Challenges in Global Data Protection Laws

CASE STUDY	REGULATION VIOLATED	VIOLATION TYPE	PENALTY/OUTCOME
Meta (Facebook) – 2023	GDPR (EU)	Unlawful data transfers to the U.S.	€1.2 billion fine
Google Analytics – 2022	GDPR (EU)	Illegal data transfers outside the EU	Fined by multiple European DPAs
Sephora – 2022	CCPA (USA)	Failure to honor opt-out requests	$1.2 million fine
SingHealth Data Breach – 2018	PDPA (Singapore)	Unauthorized access to healthcare data	SGD 1 million fine
Dis-Chem – 2022	POPIA (South Africa)	Insufficient security safeguards	Under investigation
Banco Pan – 2021	LGPD (Brazil)	Unlawful sharing of financial data	Fined R$8.5 million
Didi Global – 2022	PIPL (China)	Mishandling of user data & national security concerns	$1.2 billion fine

As new technologies like AI, IoT, blockchain, and big data evolve, data protection laws must adapt to new risks and challenges. The table 04 below compares how different regulations address these emerging technologies.

Table 4. Adaptability of Data Protection Laws to Emerging Technologies

TECHNOLOGY	GDPR (EU)	CCPA (USA)	PDPA (SINGAPORE)	POPIA (SOUTH AFRICA)	LGPD (BRAZIL)	PIPL (CHINA)
Artificial Intelligence (AI)	Strict regulations on AI profiling & automated decision-making	No AI-specific rules, but businesses must disclose AI use	AI guidelines under development	No specific AI laws	AI use under discussion	Requires transparency & user consent for AI processing
Internet of Things (IoT)	Requires privacy-by-design for IoT devices	No direct IoT regulation	Security safeguards required for IoT data	Weak IoT protections	Requires privacy safeguards for IoT devices	Requires government review of IoT data
Blockchain	Right to erasure conflicts with immutability of blockchain	No direct regulations on blockchain	No direct blockchain regulation	No blockchain-specific rules	No blockchain-specific rules	Blockchain scrutinized under national security laws

Big Data & Analytics	Requires explicit user consent for profiling & analytics	Businesses must disclose big data processing	Must balance data usage with privacy	Organizations must minimize unnecessary data collection	Requires transparency in data analytics	Requires government oversight of big data usage

.

III. Implications & Challenges in Global Data Protection Regulations

There's a lot of interest in how data privacy law may evolve to affect differently governments and regulatory authorities, businesses and organizations, and consumers and data subjects. Privacy regulations extend to the various stakeholder concerns about standardization, compliance burdens, enforcement, and user rights. Trends also indicate a shift toward greater global harmonization while there are still hurdles to overcome towards achieving an altogether unified framework for data protection. This section examines some of those salient points of concern.

Implications for Governments & Regulators: Standardization & Interoperability

The governments and regulatory bodies play a role in establishing data protection policies for both the national security and international cooperation. Standardization and interoperability among jurisdictions, however, pose several challenges, as they have to consider the local laws, economy, and culture [30]. Figure 01 illustrates "Balancing Sovereignty and Innovation in Regulatory Complications," which shows the challenge of aligning global regulation with national interest. GDPR is a step toward harmonization in laws, with countries like Brazil, China, and India considering GDPR-inspired frameworks as well [31]. Within that, however, different regions still have variances on rules regarding data localization, cross-border transfers, and mechanisms of enforcement [32]. Regulatory fragmentation is yet another challenge, where different legal requirements from different countries complicate global compliance [33]. For instance, a major country such as the U.S. does not have federal law on data protection, and this leads to state-level laws like CCPA, creating more complications in the compliance pathways [33], [34].

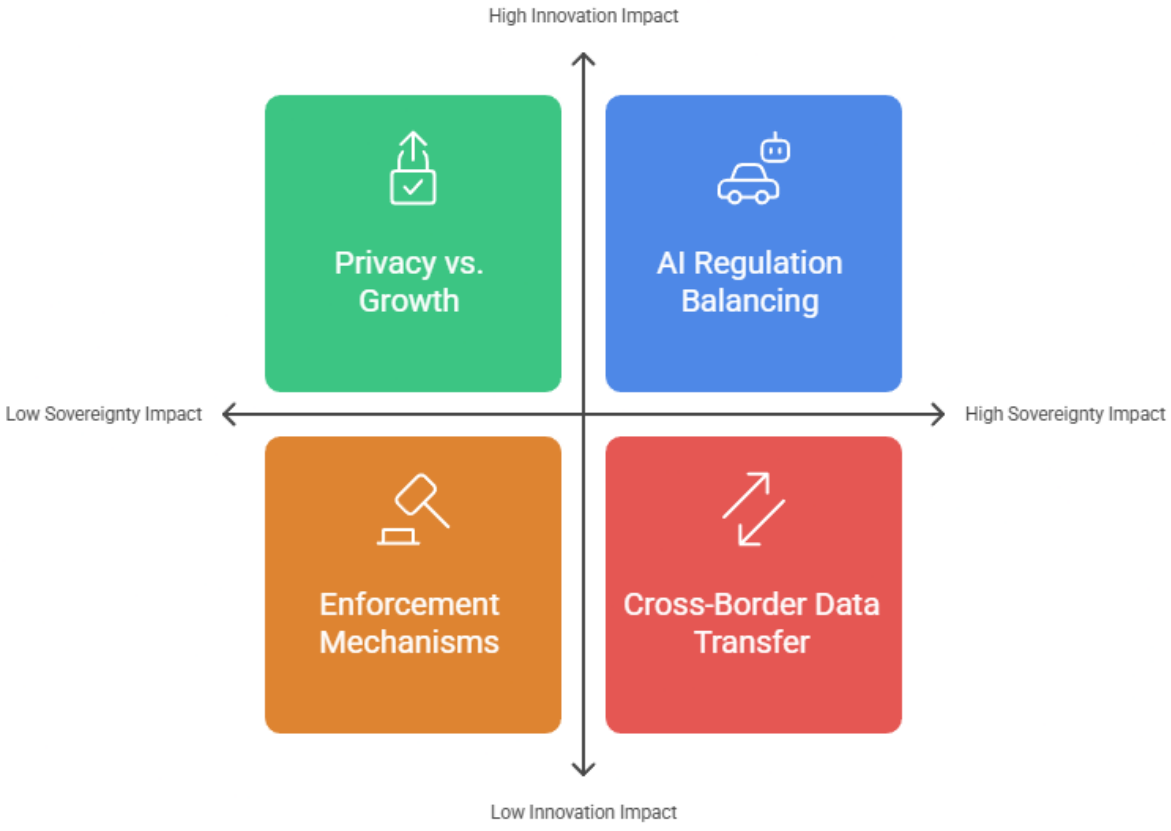

Figure 1: Balancing Sovereignty and Innovation in Regulatory Challenges

Implications for Businesses & Organizations: Compliance Burden & Legal Risks

The very stringent requirements of data protection laws become a huge operational and financial burden for businesses and organizations [35]. Figure 02 Prioritizing Business Challenges indicates most of the problems experienced by businesses in terms of compliance with changing regulatory requirements. Investment in legal specialists and monitoring requires high levels of advanced data governance policies to prevent high penalties from non-compliance [36]. One of the biggest issues facing many multinationals is compliance with the multitude of different regulatory frameworks under which they operate at the same time [37]. It is also expensive to comply, and many find themselves struggling with privacy-by-design, data impact assessments, and record maintenance-related compliance issues. Compliance with SMEs add another additional burden usually making it difficult for them to compete against larger corporations that usually have to dedicate teams for compliance. Legal harms could come in the form of hefty fines, reputational damage, and loss of consumer trust. Prominent examples include the €1.2 billion GDPR fine of Meta and the CCPA fine of US $1.2 million against Sephora [38].

Figure 2: Prioritizing Business Challenges

Implications for Consumers & Data Subjects: Awareness & Exercising Rights

Data protection legislation, including GDPR, LGPD, and PIPL, has enhanced consumer control over personal data but there is little awareness among consumers on how to effectively exercise that right. Figure 03 illustrates the process of Navigating Consumer Challenges in Data Privacy and Trust, which shows individual difficulties in understanding and acting on their data rights. Low consumer awareness, especially in newly introduced privacy law regions, can be cited as the most significant problem [39]. Studies conducted in 2022 suggest that 60% of U.S. consumers were unaware of the provisions of the CCPA, which limited their option to opt out of selling their data [40], [41]. Further, the exercise of these rights is also made problematic due to the absence of user-friendly/applicable procedures for requesting such exercises for many organizations. Companies also tend to unobtrusively apply dark design elements to make this process difficult for the individual who seeks to opt-out or requests the deletion of their data. Data breaches and misuse of personal data erode yet more consumer trust in corporations, raising questions as to corporate accountability for the enforcement of privacy laws and the effectiveness of the regulatory framework [42].

Figure 3: Navigating Consumer Challenges in Data Privacy and Trust

Global Trends & Future Directions: Toward a Unified Global Framework?

Increasingly, countries around the world are investing more in data protection, urging calls for a single, interoperable privacy framework [43]. The key trends and challenges are depicted in Figure 04 because they reflect the nature of the concern that making globally standardized data protection will require. The GDPR has inspired other new laws regarding privacy, such as the LGPD, PIPL and India's DPDP, which collectively converge towards common standards [44]. However, differences such as geopolitical issues, national security concerns and economic priorities all make true global standardization impossible [45]. The EU puts the priority on consumer rights and privacy, while through PIPL, the emphasis is on state control over data in China. In the US, absence of a federal privacy law prevents the alignment from being made globally [46]. It is then expected that the increasing regulation of emerging technologies such as AI, IoT, and big data will put in place stronger AI governance, better consumer rights and stricter corporate accountability enforcement.

Figure 4: Key Trends and Challenges

IV. Future Directions in Global Data Protection Regulations

Factors that shape data protection in the future include digitization of personal data, technological advancement, and the collective push for tougher privacy laws. While huge steps have been taken toward putting in place regulatory frameworks like Gdpr, Ccpa, Pipil, and Lgpd, several challenges are still unresolved. Among these are regulatory fragmentation, cross-border data transfer conflict, enforcement inconsistency, and the need for governance for AI and emerging technologies [47], [48]. In the future, data protection regulations will mostly be driven by international cooperation and standardization initiatives. OECD Guides on Privacy and APEC Cross-Border Privacy Rules provide an impetus to harmonized global frameworks. AI, IoT, and blockchain will need particular regulatory responses for responsible data processing [49]. Such a framework will require business establishments to invest greatly in privacy-centric infrastructures while increasing consumers' ability to understand rights and be equipped with better enforcement mechanisms.

Table 5. Key Concerns & Future Implementation Strategies

MAJOR CONCERN	CURRENT CHALLENGE	
Regulatory Fragmentation	Lack of global standardization	Establishment of an international data privacy treaty or interoperable frameworks like CBPR
Cross-Border Data Transfers	Conflicting regional policies (GDPR, PIPL, etc.)	Mutual adequacy agreements and secure transfer mechanisms
AI & Automated Decision-Making	Insufficient regulations for AI-driven profiling	Introduction of AI-specific privacy laws requiring explainability & accountability
Enforcement Gaps	Uneven application of penalties across regions	Strengthening global cooperation in enforcement & increased regulator funding
Consumer Awareness & Rights	Low understanding of privacy rights	Standardized consumer education campaigns & user-friendly opt-out mechanisms
Business Compliance Burden	High costs & complexity for multinational organizations	Simplified regulatory frameworks with common compliance mechanisms
Big Data & IoT Privacy Risks	Large-scale, unregulated data collection	Sector-specific guidelines for IoT, big data, and real-time tracking technologies
Data Localization & National Security Conflicts	Governments imposing data localization mandates	Balanced policies allowing data flows with security safeguards

With time and continuous evolution in the area of data privacy, it is incumbent upon governments, businesses, and individuals to come together to shape the regulatory framework for tomorrow. Though a worldwide standard load is remote at this juncture, it could be better facilitated by mediation, bolstering AI governance, and program enforcement over the next ten years. After all, companies will have to insist on the governance of compliance, while the regulators must make sure that, in all circumstances, privacy frameworks remain highly relevant to modern technologies. The very future lies in balancing privacy rights, innovation, and security, albeit with an edge leaning on the digital world that envelopes all of us.

V. Conclusion

The global analysis of data protection laws has revealed common principles, but different legal definitions, compliance requirements, and enforcement mechanisms in the research study. It highlights the confusion and complexity that has resulted due to the introduction of AI, IoT, big data, and blockchains into the regulatory framework. It calls for increasing international cooperation on issues like cross-border data transfer, harmonization of enforcement, and new AI-specific privacy laws. Businesses need to invest in privacy-by-design frameworks and adaptive legal strategies to meet complex compliance demands. Consumers still have restrictions in the areas of awareness and control of data. On an international level, the global trend towards

standardization and interoperability does indicate progress toward alignment. The balance between privacy, innovation, and security will be the challenge for the regulators but will have to be built toward a sustainable and adaptive model of data governance in a digitalized world.

.

REFERENCES

[1] Xia, L., Baghaie, S., & Sajadi, S. M. (2023). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. Ain Shams Engineering Journal, 15(2), 102411. https://doi.org/10.1016/j.asej.2023.102411

[2] Thavorn, J., Gowanit, C., Muangsin, V., & Muangsin, N. (2021). Collaboration Network and Trends of Global coronavirus Disease Research: A Scientometric analysis. IEEE Access, 9, 45001–45016. https://doi.org/10.1109/access.2021.3066450

[3] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2017). 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

[4] Bholasing, J. (2022). How Technological Advances in the Big Data Era Make it Impossible to Define the 'Personal' in GDPR's 'Personal Data.' European Data Protection Law Review, 8(3), 346–361. https://doi.org/10.21552/edpl/2022/3/5

[5] Janeček, V. (2022). Rethinking Law, Regulation, and Technology by Roger Brownsword. International Journal of Law and Information Technology, 30(4), 512–514. https://doi.org/10.1093/ijlit/eaad003

[6] Rommetveit, K., Tanas, A., & Van Dijk, N. (2018). Data protection by Design: promises and perils in crossing the rubicon between aw and engineering. In IFIP advances in information and communication technology (pp. 25–37). https://doi.org/10.1007/978-3-319-92925-5_3

[7] Urquhart, L., Lodge, T., & Crabtree, A. (2018). Demonstrably doing accountability in the Internet of Things. International Journal of Law and Information Technology, 27(1), 1–27. https://doi.org/10.1093/ijlit/eay015

[8] Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

[9] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2017b). 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

[10] Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law. https://doi.org/10.1093/idpl/ipz014

[11] Parker, O., Mui, R., & Titus, V. (2019). Unwelcome voices: The gender bias-mitigating potential of unconventionality. Strategic Management Journal, 41(4), 738–757. https://doi.org/10.1002/smj.3104

[12] Edwards, L., & Veale, M. (2018). Enslaving the algorithm: from a "Right to an explanation" to a "Right to better decisions"? IEEE Security & Privacy, 16(3), 46–54. https://doi.org/10.1109/msp.2018.2701152

[13] Khilnani, A., Schulz, J., & Robinson, L. (2020). The COVID-19 pandemic: new concerns and connections between eHealth and digital inequalities. Journal of Information Communication and Ethics in Society, 18(3), 393–403. https://doi.org/10.1108/jices-04-2020-0052

[14] Issue information. (2021). Security and Privacy, 4(1). https://doi.org/10.1002/spy2.113

[15] Xiao, L. Y. (2020). PEOPLE'S REPUBLIC OF CHINA LEGAL UPDATE: SUPREME PEOPLE'S COURT'S GUIDING OPINION ON REFUND REQUESTS RELATING TO UNAUTHORIZED ONLINE VIDEO GAMING TRANSACTIONS PAID FOR BY MINORS (PUBLISHED MAY 15, 2020). Gaming Law Review, 24(7), 476–479. https://doi.org/10.1089/glr2.2020.0014

[16] Michael, K. (2018). Sylvia Mercado Kierkegaard (1953–2015). Computer Law & Security Review, 34(4), 671–676. https://doi.org/10.1016/j.clsr.2018.05.003

[17] Ramlan, N. L. M., Abdullah, N. A., Karkonasasi, K., & Mousavi, S. A. (2019). A study on the impact of Crowd-Sourced rating on tweets for the credibility of information spreading. In Advances in intelligent systems and computing (pp. 66–78). https://doi.org/10.1007/978-3-030-33582-3_7

[18] Van De Waerdt, P. J. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review, 38, 105436. https://doi.org/10.1016/j.clsr.2020.105436

[19] Wong, B. (2021). Problems with controller-based responsibility in EU data protection law. International Data Privacy Law, 11(4), 375–387. https://doi.org/10.1093/idpl/ipab014

[20] Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. The African Journal of Information and Communication (AJIC), 28. https://doi.org/10.23962/10539/32213

[21] Drechsler, L. (2020). Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. International Data Privacy Law, 11(2), 182–195. https://doi.org/10.1093/idpl/ipaa019
[22] 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
[23] Zheng, G., & Shu, J. (2024). In the name of protection—A critical analysis of China's legal framework of children's personal information protection in the digital era. Computer Law & Security Review, 53, 105979. https://doi.org/10.1016/j.clsr.2024.105979
[24] 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
[25] Yin, D., Li, X., Liu, R., Zhang, L., & Zhan, Q. (2022). China's Personal Information Protection Law. BMJ, e072619. https://doi.org/10.1136/bmj-2022-072619
[26] Understanding China's Personal Information Protection Law (China PIPL). (n.d.). https://www.bitraser.com/article/understanding-china-personal-information-protection-law-pipl.php
[27] Feng, Y. (2019). The future of China's personal data protection law: challenges and prospects. Asia Pacific Law Review, 27(1), 62–82. https://doi.org/10.1080/10192557.2019.1646015
[28] Greenleaf, G. (2021). Global convergence of data privacy standards and laws: Speaking notes for the European Commission events on the launch of the General Data Protection Regulation in Brussels & New Delhi. European Data Protection Law Review, 7(2), 287-300. https://doi.org/10.21552/edpl/2021/2/17
[29] Mondschein, C. F., & Monda, C. (2018). The EU's General Data Protection Regulation (GDPR) in a research context. In Springer eBooks (pp. 55–71). https://doi.org/10.1007/978-3-319-99713-1_5
[30] 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
[31] Ryngaert, C., & Taylor, M. (2020). The GDPR as global Data protection regulation? AJIL Unbound, 114, 5–9. https://doi.org/10.1017/aju.2019.80
[32] De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2017). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review, 34(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003
[33] Eskhita, R., & Stamhuis, E. (2024). The influence of the Brussels effect on the interpretation of data protection laws in the Gulf. Global Journal of Comparative Law, 13(2), 261–278. https://doi.org/10.1163/2211906x-13020007
[34] Chauhan, P. S., & Kshetri, N. (2021). 2021 State of the Practice in Data Privacy and Security. Computer, 54(8), 125–132. https://doi.org/10.1109/mc.2021.3083916
[35] Lakshmi, K., Gupta, H., & Ranjan, J. (2020). Analysis of general data protection regulation compliance requirements and mobile banking application security challenges. 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1028–1032. https://doi.org/10.1109/icrito48877.2020.9197954
[36] Adebayo, N. V. I., Ige, N. a. B., Idemudia, N. C., & Eyieyien, N. O. G. (2024). Ensuring compliance with regulatory and legal requirements through robust data governance structures. Open Access Research Journal of Multidisciplinary Studies, 8(1), 036–044. https://doi.org/10.53022/oarjms.2024.8.1.0043
[37] Udo, N. a. A. (2024). REGULATORY COMPLIANCE AND ACCESS TO FINANCE: IMPLICATIONS FOR BUSINESS GROWTH IN DEVELOPING ECONOMIES. Deleted Journal, 1(2), 8–23. https://doi.org/10.62536/sjehss.2023.v1.i2.pp8-23
[38] 1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board. (n.d.). https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en
[39] Prastyanti, R. A., & Sharma, R. (2024). Establishing consumer trust through data protection law as a competitive advantage in Indonesia and India. Journal of Human Rights Culture and Legal System, 4(2), 354–390. https://doi.org/10.53955/jhcls.v4i2.200
[40] IAB. (2022, October 24). Interactive Advertising Bureau | CCPA Benchmark Survey. https://www.iab.com/insights/iab-ccpa-benchmark-survey/
[41] Baik, J. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). Telematics and Informatics, 52, 101431. https://doi.org/10.1016/j.tele.2020.101431

[42] Andrew, J., Baker, M., & Huang, C. (2021). Data breaches in the age of surveillance capitalism: Do disclosures have a new role to play? Critical Perspectives on Accounting, 90, 102396. https://doi.org/10.1016/j.cpa.2021.102396

[43] EU-US Data Privacy Framework: A brief history. (n.d.). Blog | OneTrust. https://www.onetrust.com/blog/eu-us-data-privacy-framework-a-brief-history/

[44] EU-US Data Privacy Framework: A brief history. (n.d.). Blog | OneTrust. https://www.onetrust.com/blog/eu-us-data-privacy-framework-a-brief-history/

[45] De Gregorio, G. (2022). The transnational dimension of data protection. The Italian Review of International and Comparative Law, 1(2), 335–359. https://doi.org/10.1163/27725650-01020006

[46] Purcell, C., & Zhan, J. (2007). Adapting US privacy laws to the internet: Is patching enough? International Conference on Machine Learning and Cybernetics, 3000–3005. https://doi.org/10.1109/icmlc.2007.4370662

[47] H. Agarwal, "International Data Privacy: A Look at Future and Challenges," UniSense Advisory, 2023. [Online]. Available: https://unisenseadvisory.com/international-data-privacy-future-challenges/ UNISENSEADVISORY

[48] "The Global State of Data Protection – Data Protection Day," 2023. [Online]. Available: https://dataprotection.day/the-global-state-of-data-protection/dataprotection.day

[49] S. Finck, "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways," Journal of Cybersecurity, vol. 11, no. 1, 2023. [Online]. Available: https://academic.oup.com/cybersecurity/article/11/1/tyaf002/8024082