Page 3014 - 3026 **DOI:** *https://doij.org/10.10000/IJLMH.119402*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

India's Domestic Violence Laws Legal Challenges and Prospects

SIDHIDA VARMA S[1]

ABSTRACT

Today, personal data in the hands of various actors has become a highly sought-after commodity in the global digital economy. When something is desired, it is also essential to have regulatory laws to collect, process, and transfer personal data. In essence, these laws govern data fiduciaries or data controllers, who are considered to be the ones with a duty of care towards the personal data of data subjects. This paper aims to analyze the history of data fiduciary obligations in the context of a comparison of some significant and influential regimes in the protection of personal data in the European Union's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act (DPDPA), China's Personal Information Protection Law (PIPL), and several laws from states in the United States, including the California Consumer Privacy Act (CCPA) and the Utah Consumer Privacy Act (UCPA).

Essentially, the study seeks to outline the basic definitions, legal responsibilities, and standards of accountability required by data fiduciaries operating within such jurisdictions. It also elucidates crucial tenets like grounds for lawful processing, consent models (opt-in versus opt-out), minimization of data, transparency obligations, security measures, the appointment of Data Protection Officers, and the rights of data subjects. Added to that, the paper further describes the areas of disagreement over the differences of scope and extraterritoriality of the laws, with a particular focus on cross-border data flows."

The study further proceeds to examine the impact of the tension created by the rights-centered approaches that define GDPR and PIPL against the commercial-mindedness of U.S.-state law, which indicates some areas of convergence and divergence within international privacy standards. This then provides a solid anchor for global businesses, regulators, and policymakers to navigate the complexities of data protection around the world, underlining the need for harmonization in defining personal liability and transparency and protecting individual rights within the framework of our interlinked digital ecosystem.

I. INTRODUCTION

The personal data of individuals has gone through a metamorphosis and is one of the most

[1] Author is LL.M. Student at Hindustan University, TamilNadu, India.

 [ISSN 2581-5369]

sought-after possessions, or better, the "new oil" of the global economy, pulling governments, MNCs, and digital platforms into the direct processing of tremendous personal data almost each day. Therefore, it will be a concern on any regulatory agenda requiring such protection. The increasing dependence on the "data fiduciary" being somewhat equated with data controllers and data processors is gradually gathering attention in different jurisdictions.

The degree of variation between the divergent national data protection regimes, therefore, makes the obligations imposed upon them almost unrecognizably different, hence giving rise to various compliance challenges. To put things in perspective, there exists a high global bar under the GDPR; while CCPA slightly differs from everything the sphere China creates under the Personal Information Protection Law (PIPL), India under DPDP, [2]and Utah under CPA introduces several different approaches, definitions, and compliance mechanisms. All of these combined create a large grey space within which global organizations and data fiduciaries grapple to navigate.

This paper compares and contrasts the diverse roles and obligations of data fiduciaries across these major jurisdictions in an effort toward analysis. Their legal duties, their accountability standards, their obligations of care to data subjects, and their consequences of noncompliance are brought under scrutiny. This study thus stands to benefit not only global corporations that seek to carry on business legally but also regulators and academics in pursuit of convergence in privacy standards and the protection of individual rights in an increasingly digitally connected world.

II. DEFINITION AND CONCEPT OF DATA FIDUCIARIES

The concept of the data fiduciary may be considered the key pillar in data protection frameworks, though interpretations differ among jurisdictions. In essence, however, the term comprises the concepts of accountability, trust, and ethical responsibility. [3]

- The key actors under the European Union's General Data Protection Regulation (GDPR) are the data controller and the data processor. The controller is to be understood as that body which determines the purposes and means of processing personal data, whereas the processor is that body that processes data on behalf of the controller.[4] The

[2] Calzada, Igor. "Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL)." Smart Cities 5.3 (2022): 1129-1150.
[3] McDermott, Yvonne. "Conceptualising the right to data protection in an era of Big Data." *Big Data & Society* 4.1 (2017): 2053951716686994.
[4] Manis, Maria Luisa. "The processing of personal data in the context of scientific research. The new regime under the EU-GDPR." *BioLaw Journal-Rivista di BioDiritto* 3 (2017): 325-354.

 [ISSN 2581-5369]

GDPR establishes essential obligations on the controller while the processor is obliged to act under the instructions of the controller and ensure confidentiality and security thereof.

- In India, the introduction of the term data fiduciary under the Digital Personal Data Protection Act (DPDPA) would imply that a data fiduciary is in a position of trust about the individual (data principal) and the entity undertaking the data processing[5]. A fiduciary, under DPDPA, is liable for its data processing activities to be lawful, for obtaining the data subject's consent, and for ensuring the data subject's rights. Other obligations have also been cast upon those considered Significant Data Fiduciaries.
- Under the California Consumer Privacy Act (CCPA) and the Utah Consumer Privacy Act, businesses and service providers are the terms used therein. [6]Those refer mainly to commercial actors who collect, share, or sell consumer data. Though the CCPA arguably imposes some duties, particularly in terms of transparency and opt-out rights, it seems to be largely business-centric and lacking a fiduciary tone.
- China's Personal Information Protection Law (PIPL) internationally rules the processing of personal information by both the data controller[7] and data processor in function. Basically, such processors bear legal obligations to get consent, restrict the use of data for legal purposes, and secure storage and transfer.

What underlies this spectrum of frameworks stipulates that the entity in charge of personal data is in a position of trust and responsibility. That fiduciary position, whether framed legally or morally, implies accountability, transparency, and a duty to act in the best interest of the data subject.

III. EXTENT, SCOPE, AND APPLICABILITY OF LAWS

The varying scope and applicability of data protection laws denote the different ways jurisdictions grapple with the globalization of data processing. To assess the legal dynamics of data fiduciaries across borderlines, it is pertinent to investigate the covered entities, the jurisdictional reach, and the structural approach, whether sectoral or omnibus.

This has made the European Union's General Data Protection Regulation (GDPR) a prime example of an omnibus law because its extra-territorial reach is much too comprehensive. The

[5] Sundara, Karishma, and Nikhil Narendran. "The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection." Computer Law Review International 24.5 (2023): 129-141.
[6] Bukaty, Preston. *The california consumer privacy act (ccpa): An implementation guide*. IT Governance Ltd, 2019.
[7] Calzada, Igor. "Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL)." Smart Cities 5.3 (2022): 1129-1150.

 [ISSN 2581-5369]

Regulation is not only concerned with organizations in the EU; it also includes entities abroad dealing with goods or services in the EU or monitoring the behavior of residents in the EU. They apply to data controllers and processors together and impose extensive compliance on those entities irrespective of their physical presence. This extraterritorial aspect significantly affects global entities dealing with the personal data of EU residents.

Much like the GDPR, China has thrown the borderless concept onto the playing field with its Personal Information Protection Law (PIPL). It applies to personal data processes conducted outside China if the focal point of such processing is to provide products or services to individuals in China or to analyze or assess their behavior. Thus, the PIPL shares large portions of global applicability with the GDPR in that both expressly endorse national data sovereignty in the protection of citizen data internationally.

The Digital Personal Data Protection Act (DPDPA) passed by India also contains provisions that make it extraterritorial, applied to processing outside India if it involves offering goods or services to data principals within India. The operation and application of the DPDPA are still evolving, but it reflects the strong intent of lawmakers behind the international regulation of data flows affecting Indian citizens.

The California Consumer Privacy Act (CCPA) and the Utah Consumer Privacy Act, oriented around the threshold, work primarily from a business perspective. These laws apply to businesses meeting certain revenue or data volume thresholds, for instance, a certain gross annual revenue or processing personal data of some minimum number of consumers. Their reach is limited to for-profit entities, exempting smaller businesses as well as certain sectors from compliance.

Structurally, the CCPA and Utah's Act examine consumer data, while other U.S. laws touch on humanitarian and financial matters separately [8]ly via HIPAA and GLBA; therefore, we see a sectoral distinction for data protection. Meanwhile, GDPR, PIPL, and DPDPA are considered omnibus laws designed to regulate all sectors under one umbrella.

The divergences in scope, threshold, and structure foster complications for multinational corporations. The multinational firms must grapple with the differences in applicability criteria for each of the laws, discern whether their data practices fall within the ambit of foreign legislation, and then find ways of seizing the day and conducting business to avoid those various sets of rules coming into conflict with one another concerning liability and regulations.

[8] Newell, Bryce Clayton, et al. "Regulating the Data Market: The Material Scope of American Consumer Data Privacy Law." U. Pa. J. Int'l L. 45 (2023): 1055.

 [ISSN 2581-5369]

IV. RESPONSIBILITIES OF DATA FIDUCIARIES OR CONTROLLERS

The responsibilities of fiduciaries or data controllers are the absolute bedrock upon which the framework for enforcing privacy rights rests. Although the terminology may differ in various regimes, the fundamental aspects generally emphasize the legitimate processing of data, transparency surrounding data processing, protection of the data, and accountability.

A. Legal Bases for Processing of Personal Data

Article 6 of the GDPR lays down six independent legal bases that will permit data processing, namely: consent, contract, legal obligation, vital interests, public task, and legitimate interests.[9]

Correspondingly, Section 4 of India's Digital Personal Data Protection Act, 2023 (DPDPA) gives effect to processing in furtherance of a lawful purpose with either consent of the individual concerned or as per the definition of legitimate use envisaged within Section 7. [10]

Article 13 of China's Personal Information Protection Law, in keeping with the understanding, speaks of information processing based on clear legal grounds, with informed consent being an overriding condition for that purpose.[11]

Unlike others, CCPA and UCPA are opt-out in nature, whereby consent is presumed unless an individual opts out of the particular use, e.g., selling data (CCPA, Section 1798.120).[12]

B. The Models of Opt-in and Opt-out

The GDPR, PIPL, and DPDPA have all opted for an opt-in model - that is, a model that requires affirmative and informed consent before any data can be collected. The alternative to that would be the CCPA and UCPA, which are opt-out laws that require the individual to act in order to prevent certain uses of his or her information, primarily for commercial purposes.

C. Data Minimization and Purpose Limitation

Article 5(1)(b) and (c) of the GDPR speak of data collection for clear, specific, and legitimate purposes, while PIPL Article 6 and DPDPA Section 6 require that data processing be necessary and lawful with respect to relevance and non-excessiveness.

D. Accountability and transparency

The GDPR is an exceedingly strong accountability regime laid down by Articles 5(2) and 24, which require controllers to demonstrate their compliance with records and checks. Herein, we

[9] European Parliament and Council. General Data Protection Regulation. 2016.
[10] India. Digital Personal Data Protection Act. 2023.
[11] China. *Personal Information Protection Law*.
[12] *California Consumer Privacy Act*.

 [ISSN 2581-5369]

see a semblance of notice to data principals in Section 10 of the DPDPA. Transparency has been included in Article 7 of the PIPL.

E. Appointment of DPO

A DPO is mandated under GDPR (Articles 37-39) for public authorities or entities involved in large-scale processing. PIPL Article 52 imposes similar obligations. The DPDPA Section 10(2) empowers the Central Government to frame rules requiring DPOs in certain circumstances. In neither CCPA nor UCPA is there such a requirement.

F. Security Safeguards and Risk Mitigation.

Thus, Article 32 of GDPR, Article 51 of PIPL, and Section 8 of DPDPA all expressly stipulate the need for taking appropriate technical and organizational measures to protect personal data, like encryption or pseudonymization, as well as for having breach response mechanisms in place. CCPA has general security obligations regarding this point but lacks prescriptive technical requirements.

V. RIGHTS OF DATA SUBJECTS AND FIDELITY OBLIGATIONS

The protection of personal data rests upon a set of individual rights and corresponding duties of data fiduciaries or controllers for the realization of these rights, thereby enabling an individual to exercise control over the personal data with respect to its collection, processing, and sharing by other persons.

- Articles 12 through 23 of the General Data Protection Regulation contain the catalog of rights from the right of access to personal data, the rectification of inaccuracies, the erasure of data (Right to be Forgotten - Article 17), restrictions on processing, objections to processing (Article 21), and data portability (Article 20). Data controllers are thus obliged by law to submit these rights to a user in a clear manner and within a specified timeframe- usually one month.
- Similarly, the Digital Personal Data Protection Act, 2023 (DPDPA) of India recognizes data principals' rights granted within Sections 11 to 14, e.g., the right to access, the right to correction, and the right to erasure. The data fiduciaries, therefore, have a legal obligation to address the requests of data principals in accordance with the time and manner prescribed.
- The People's Republic of China Personal Information Protection Law (PIPL) was passed similarly and provides for these rights under Articles 44 to 49 for those who assert them

and obligates other handlers of personal information to this extent. Withdrawing consent and giving the right to know are essential tenets under PIPL.

- The California Consumer Privacy Act (CCPA) has provisions on access to and deletion of personal data (Section 1798.105) and opting out of its sale. However, rights to correction were added much later by the passage of the California Privacy Rights Act of 2020 (CPRA). Although the Utah Consumer Privacy Act (UCPA) provided for some rights regarding access and deletion, it did not include any provisions for a right of correction.

Thus, enforcement mechanisms and fiduciary duties vary widely, with the more stringent norms imposed under the GDPR and PIPL diverging from the more business-friendly U.S. models. Nevertheless, all data fiduciaries must have validated processes for rights request processing.

VI. CROSS-BORDER DATA TRANSFER RESPONSIBILITIES

A defining characteristic of the cross-border data transfer within the globalized digital economy is the jurisdictional, accountability, and protectionist dimensions. This suggests that the onus for cross-border transfers lies with data fiduciaries and controllers as personal data leaves the boundary of origin.

- International transfers fall under Chapter V of the General Data Protection Regulation (GDPR), which comprises Articles 44 to 50. To transfer data to a third country at all, however, the Commission of the European Union must have determined positively that the country of destination applies sufficient levels of protection equivalent to that of the EU. In the absence of such an adequacy decision, controllers must refer to standard contractual clauses (SCCs), binding corporate rules (BCRs), or any other legal instruments providing for adequate safeguard measures.
- Articles 38-43 of China's Personal Information Protection Law (PIPL) certifies or does an event assessment from the information processors for the transfer of data outside the territory by requiring a security assessment event by the Cyberspace Administration of China (CAC) or certified organizations. Moreover, this law requires data handlers to inform individuals that their data will be transferred beforehand and collect affirmative consent.
- Section 16 of the Digital Personal Data Protection Act, 2023 of India (DPDPA) provides that personal data may be transferred outside India but only to those countries at the time specified by the Central Government. Unlike the other two frameworks, there is no

adequacy criterion mentioned here, as such would be open to general discretion as to who might be a worthy recipient of this designation.

- Both the California Consumer Privacy Act (CCPA) and the Utah Consumer Privacy Act (UCPA) pretty much cut down the bureaucratic tape for cross-border transfers to the bare minimum. Here, there is neither a requirement of adequacy nor formal mechanisms but an obligation on businesses to ensure that they comply with general data security and the rights of consumers.

This is why it has become necessary for a data fiduciary to scan its legal environment and develop contractual safeguards for the ongoing protection of personal data across borders. However, the scrutiny is heavier from regimes in the EU and China, whereas US state legislatures go to a business-light approach.

VII. ENFORCEMENT MECHANISMS AND PENALTIES FOR FIDUCIARIES

Enforcement laws are required to ensure compliance from any data fiduciaries or data controllers. Each jurisdiction provides some regulatory authority that also prescribes penalties for breaching the established personal data laws.

The supervisory authorities under the General Data Protection Regulation (GDPR) are the Data Protection Authorities (DPAs).[13] These authorities are conferred powers under Articles 51-59, which are to be utilized to monitor the states of compliance, to conduct inquiries, and to sanction. Article 83 states that the fine shall be above a tiered structure and may reach €20 million or 4% of the worldwide annual turnover, whichever figure provides higher deterrence. The DPA may also issue warnings or reprimands or may put a stop to the processing activities for a period of time.

Under the PIPL, China as Central Administration CAC will exercise the primary supervisory authority over China. Penalties, per Articles 66 to 70, can amount to RMB 50 million or 5 percent of annual turnover for very serious offenses committed against an entity. Besides imposing such penalties, the CAC may also suspend operation licenses or blacklist companies in the case of repeated violations. [14]

In India, the Digital Personal Data Protection Act, 2023 (DPDPA) contains provisions for the establishment of a Data Protection Board under Section 18, which will hear all matters relating

[13] Schütz, Philip. "Data protection authorities under the EU General Data Protection Regulation-a new global benchmark." Handbook of Regulatory Authorities. Edward Elgar Publishing, 2022. 128-145.
[14] Clementi, Davide. "Between digital surveillance and individual protection: a juridical and comparative history of the Cyberspace Administration of China." Rivista di Digital Politics 4.2 (2024): 343-370.

to non-compliance under this Act. A finer grading of penalties is to be worked out by way of rules; however, Schedule 1 provides for penalties up to ₹250 crore, depending on the nature and gravity of the breach.

Further, the CCPA gives teeth to the California attorney general for administrative enforcement, which entails fines of $2,500 for every unintentional violation and $7,500 per intentional violation, as articulated in Section 1798.155. The stitching of this pattern shall, therefore, be extended to the even worst-resourced UCPA, that pertaining directly to Utah, which is paralyzed by the absence of any private right of action.

These are all liabilities that solidly encumber fiduciaries for what is largely a slip in compliance, varying either by their actions against reputation or by exposure. Apart from contrasts in enforcement and a far-reaching domain, the GDPR and PIPL are still the torchbearers in their regulatory rigor.

VIII. CASE STUDIES AND REAL-WORLD EFFECTS

Entirely speaking, the earth enforcement speaks to the extent of seriousness afforded to data fiduciary duties across the globe concerning data protection laws. A case that provided a landmark in the subject was Meta (Facebook), fined €1.2bn by the Irish Data Protection Commission under GDPR in regard to payment for data transfer across borders according to Article 46. This fine, dated May 2023, so far the heaviest under the GDPR, increasingly points to an increased scrutiny of the data flow from the EU to the USA, especially due to the fall of the Privacy Shield framework. [15]

Amazon was fined €746 million by the National Commission for Data Protection of Luxembourg (CNPD) for breaching numerous principles of the GDPR as regards data processing and consent. Amazon contested it on substantive grounds, nevertheless, it only further illustrated how the global tech companies expose themselves to the financial or reputational risk resulting from their violation of the lawful bases for processing of data prescribed by Articles 5 and 6 of the GDPR. [16]

The UK Information Commissioner's Office has opened inquiries into TikTok, Reddit, and Imgur concerning their approaches to children's personal information and ways of verifying ages. The focus is on TikTok's algorithms recommending content to teens. The probe comes in

[15] Euronews. "US Tech Giant Meta Fined a Record €1.2 Billion in Europe." Euronews, 22 May 2023, https://www.euronews.com/next/2023/05/22/us-tech-giant-meta-fined-a-record-12-billion-in-europe.

[16] Reuters. "Amazon Hit with $886 Million EU Data Privacy Fine." Reuters, 30 July 2021, https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/.

 [ISSN 2581-5369]

the wake of a penalty slapped on TikTok for flouting rules for younger kids in a similar manner.[17]

In the United States, under the California Privacy Rights Act, which also amends the CCPA and has extended enforcement powers as far back as January 2023, the newly activated California Privacy Protection Agency (CPPA) has continued to issue notices of noncompliance to companies as well as investigate companies breaching opt-out rights and privacy notices.[18]

Although not yet fully operational in India, the Digital Personal Data Protection Act, 2023, enjoins extra data governance frameworks upon companies. The uncertainty as to the precise shape of the procedural rules and the constitution of the Data Protection Board raises that concern or something else. Once implemented and put to work, an aspirant is to see this aligned with GDPR.

IX. EMERGING TRENDS AND GLOBAL CONVERGENCE

With worldwide connected economies and data still driving them, nations have been enacting new laws that shape the new realities of privacy and sovereignty, and also of creativity. One of the instances of this trend under the dominant theme is data sovereignty mandates in which nations were seeking to enforce requirements that data be stored or processed nationally before acceptance of transnational data flow. Such is the case given India's Data Protection Bill 2023 Section 16 that empowers the government to impose prohibitions against cross-border flow for certain countries. [19]China's Personal Information Protection Law demands a security assessment and a Cyber Administration of China approval for data transferring out of its borders, much more so for critical or sensitive data.

The increasing clamor for a federal data protection law has found resonance in the US, which is still struggling with un-anarchic regulation due to state-law-sought approaches such as CCPA, CPRA, and Utah's Consumer Privacy Act. The trend is manifested in bills such as the American Data Privacy and Protection Act, which aims to bring practices closer to EU standards, e.g., that of the GDPR.

Countries are thus pushed to collaborate on interoperable privacy frameworks that will have flexibility in standards incorporated into the national privacy regulations while still allowing

[17] Reuters. “UK Launches Investigation into TikTok, Reddit over Children's Personal Data.” Reuters, 3 Mar. 2025, https://www.reuters.com/world/uk/uk-launches-investigation-into-tiktok-reddit-over-childrens-personal-data-2025-03-03/.

[18] Reuters. “New Era of Privacy Laws Takes Shape in United States.” Reuters, 15 Nov. 2023, https://www.reuters.com/legal/legalindustry/new-era-privacy-laws-takes-shape-united-states-2023-11-15/.

[19] Panchal, Sumit. "Cross-Border Data Protection Laws in India and European Union: A Critical Analysis of the Complexities and the Legal Challenges." (2024).

seamless transfer of data. The 2022 - OECD Declaration on Government Access to Personal Data Held by Private Sector Entities is yet another step in restoring trust in the data that run across borders.

As practices of data continue to accommodate AI, fresh challenges in privacy emerge. There's a whirlwind of speculation over a whole new bunch of 'fiduciary principles' in algorithmic decision-making that are now being termed principles such as openness, bias mitigation, and accountability. The argument goes that this calls for being placed within the broader context of data governance for AI as pure regulation of its own within the mega-regulatory frameworks of privacy while data fiduciaries are re-created in an automated environment.

X. CONCLUSION

As data drives the global digital economy, nations are amending their legal structures to meet new realities regarding privacy, sovereignty, and innovation. The biggest development is perhaps the emergence of the data-localization mandates, whereby nations require personal data to be stored or processed within their territories. India's DPDPA, 2023, in Section 16, allows the government to restrict cross-border data transfer to certain countries. Similarly, the PIPL in China requires an assessment of security and approval by the CAC for outbound transfer of data, especially with regard to critical or sensitive data.

Increasing momentum is building in the U.S. for a comprehensive federal data protection law that would harmonize the current patchwork of state-level laws, such as the CCPA, the CPRA, and Utah's Consumer Privacy Act. Proposed laws, such as the American Data Privacy and Protection Act (ADPPA), also represent this push, with the intention of further aligning the practices in the U.S. with global standards such as the GDPR.

Global bodies such as the OECD and G20 have also called for the creation of interoperable privacy frameworks that allow unobstructed data flows, albeit with the understanding that differing national standards for privacy will be upheld. One such step in the restoration of trust in international data flows is the OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities 2022.

AI integration into data processing, in its most nascent state, has germinated a mad set of privacy concerns. A fiduciary orientation is increasingly being demanded for algorithmic decision-making, ranging from transparency, bias mitigation, and accountability. This has led to calls for AI-specific data protection standards to be developed within existing privacy regimes, drawing attention to the changing role of data fiduciaries in an automated world.

 [ISSN 2581-5369]

XI. REFERENCES

1. European Parliament and Council. General Data Protection Regulation. 2016. (Referenced throughout the text regarding GDPR articles and concepts.)

2. India. Digital Personal Data Protection Act. 2023. (Referenced throughout the text regarding DPDPA sections and concepts.)

3. China. Personal Information Protection Law. (Referenced throughout the text regarding PIPL articles and concepts.)

4. California. California Consumer Privacy Act. (Referenced throughout the text regarding CCPA sections and concepts.)

5. Utah. Utah Consumer Privacy Act. (Referenced throughout the text regarding UCPA concepts.)

6. European Parliament and Council. General Data Protection Regulation, Articles 12-23, 44-50, 51-59, 83. 2016. (Referenced for data subject rights, cross-border transfers, and enforcement mechanisms.)

7. India. Digital Personal Data Protection Act, 2023, Sections 11-14, 16, 18, Schedule 1. (Referenced for data principal rights, cross-border transfers, and the Data Protection Board and penalties.)

8. China. Personal Information Protection Law, Articles 38-43, 44-49, 66-70. (Referenced for cross-border transfers, data subject rights, and enforcement mechanisms.)

9. California. California Consumer Privacy Act, Section 1798.105, 1798.155. (Referenced for data subject rights and enforcement mechanisms.)

10. Utah. Utah Consumer Privacy Act. (Referenced for data subject rights and the absence of a private right of action.)

11. Irish Data Protection Commission (DPC). (Referenced as the supervisory authority that issued the significant GDPR fine against Meta (Facebook) for cross-border data transfer violations.)

12. National Commission for Data Protection of Luxembourg (CNPD). (Referenced as the supervisory authority that issued the substantial GDPR fine against Amazon for breaches related to data processing and consent.)

 [ISSN 2581-5369]

13. UK Information Commissioner's Office (ICO). (Referenced for launching investigations into TikTok, Reddit, and Imgur concerning children's personal data practices and age verification.)

14. California Privacy Protection Agency (CPPA). (Referenced as the newly activated agency in California responsible for enforcing the CPRA and issuing notices of noncompliance).

15. Organisation for Economic Co-operation and Development (OECD). OECD Declaration on Government Access to Personal Data Held by Private Sector Entities. 2022. (Referenced as an example of a global effort towards creating interoperable privacy frameworks and restoring trust in cross-border data flows.)

*****

 [ISSN 2581-5369]