Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Qualitative Analysis of Data Protection Laws: A shield for Personal Data Protection concerning California, European Union, China, and India

Nupur Pandey[1*], Angrish Agarwal[2] and Arun Kumar Tripathi[3]
[1]Invertis Institute of Management Studies, Invertis University Bareilly, Bareilly 243001, India; mailtonupurtripathi@gmail.com
[2]Invertis Institute of Management Studies, Invertis University Bareilly, Bareilly 243001, India; angrish.a@invertis.org
[3]Department of Computer Science, Noida Institute of Engineering and Technology, Greater Noida 201306, India; mailtoaruntripathi@gmail.com
***Corresponding Author:** Nupur Pandey
*Invertis Institute of Management Studies, Invertis University Bareilly, Bareilly 243001, India; mailtonupurtripathi@gmail.com

ARTICLE INFO
Received: 25 Dec 2024
Revised: 15 Feb 2025
Accepted: 25 Feb 2025

ABSTRACT
In the past decades, technological innovation and globalization have created a borderless digital space where digital devices continuously generate enormous amounts of data, referred as "Big Data". Almost every organisation utilizes this data to predict consumer behaviour, future requirements, and trends legally or illegally. This situation prompted government authorities to establish a framework that defines data privacy boundaries before processing consumers' data.
The European Union (EU) announced the General Data Protection Regulation (GDPR) 2018 as a standardized data protection law to address privacy concerns. Subsequently, the California Consumer Privacy Act (CCPA), Personal Information Protection Law (PIPL), and Personal Data Protection Bill (PDPB) were proposed in California, China, and India, respectively. These laws represent significant improvements in consumer data protection.
This paper briefly outlines the need for data protection laws and examines the most prominent data protection regulations worldwide, including their key features. It provides a comparative study of privacy protection laws on various parameters of personal data protection. The paper intends to exhibit a typical pattern in all data privacy laws while emphasizing their significant differences. It will provide a deep understanding of 'rights' for consumers and personal data protection under the mentioned privacy regulations.

Index Terms— *GDPR, CCPA, PIPL, PDPB, Data Privacy, Consumers' Personal Data.*

I. INTRODUCTION

HE electronics and communication industries have emerged as our society's central pillars in the last two decades. These provide ubiquitous services to the numerous industrial segments such as banking, healthcare, agriculture, education, financial sectors, etc. In these sectors, electronic gadgets such as smartphones, tablets, laptops, etc., are used as an interface for hoarding and retrieving data to and from. It led to the generation and warehousing of enormous data in the cloud. The generated data includes vital personal information related to consumers such as name, date of birth (DoB), Unique Identification Number (UIDN), , biometric information, likes, dislikes, lifestyles, behavioral patterns, phone number, personal health record, etc. Most organisations utilise the listed personal information as a source of intelligence for establishing a new business model or refining the existing one. Leakage of personal data knowingly or unknowingly without the customer's permission causes privacy [1-17] issues and may affect the life of a specific customer or its family members. The government-imposed Data Protection Regulations (DPR) [18-19] were introduced to address customer privacy issues.
Section 2 of the paper introduces the most popular data protection acts. Section 3 briefly describes the evolution of data protection acts worldwide, as specified in Section 2. Section 4 describes the world's most prevalent Data Protection Acts (DPA) and their principles and rights. Section 5 provides a comparative qualitative analysis of data protection acts discussed in Section 6. At last, section 6 concludes the paper.

II. DATA PROTECTION ACTS (DPA)

Individual privacy is one of the topmost concerns, especially in the digital era. Data breaches expose individual

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

personal data and seriously affect them through identity theft, blackmailing, etc. Organizations face financial risks and loss of trust from society, investors, and customers. Almost all countries have proposed their Data Protection Act (DPA) [19] to deal with privacy breaches. For any individual, the data protection acts are their fundamental right [10]. The primary goal of data protection acts is to safeguard individual information against its misuse, and it can only processed after the individual's prior consent. Furthermore, every individual is entitled to be informed about why and how their personal data is being processed [13]. These laws have defined a set of procedural safeguards in processing personal data. More particularly, the laws have three sets of unified goals as follows:

- Protection of an individual's privacy and social values related to it.
- Increases the accountability of organizations storing individuals' personal information.
- Improves efficiency and security of the decision-making process on personal data.

III. EVOLUTION OF DATA PROTECTION ACTS (DPA)

Data protection acts provide a legal framework to obtain, use, and store individual data. Every society has different definitions, features, and boundaries regarding privacy based on other cultures and disciplines. As a result, several privacy laws have been proposed worldwide to protect individuals' rights. These laws include the right to get details for what data is stored, for which specific purpose it is collected, and to delete stored data once the specified purpose is completed.

Officially, for the first time in 1890, two United States (US) lawyers published an article to define "The Right to Privacy". "The article examines the 'right to be left alone,' presenting it as a definition of privacy. Authors analyzed data privacy as 'inviolate personality' and 'man's spiritual nature, of his feelings and intellect'. In the meantime, individual researchers propose several privacy articles. In 1948, the United Nations successfully drafted a momentous document in the history of "human rights" and published it as the Universal Declaration of Human Rights (UDHR). Article 12 [20] defines the "Right to privacy", and as per the definition ", No one has the right to interfere with the privacy of anyone, i.e., everyone has the right to protect his/her honor and reputation".

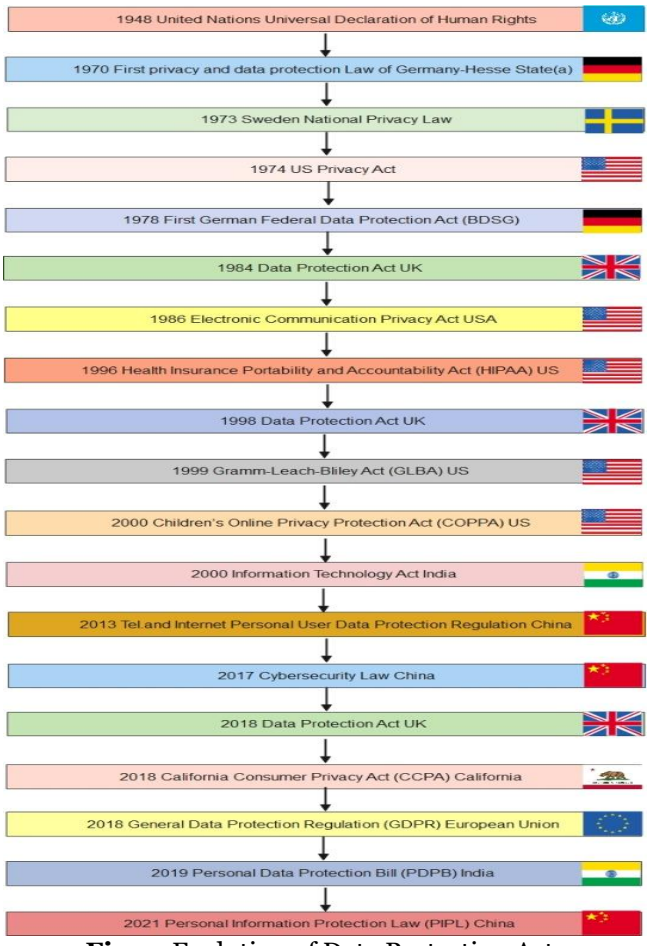

Fig. 1. Evolution of Data Protection Acts

In 1970, the German federal state of Hesse introduced the country's first data protection law. In 1971, the first

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

draft of it, with the title “Federal Data Protection Act” [21], was submitted for consideration and published in 1978 with a series of amendments to the draft. In 1973, Sweden also proposed its first national privacy law to deal with data larceny. It allows consumers to demand and review the personal information stored by an organization. It also complies with privacy rights, marking a significant step in developing data protection frameworks. The Swedish Data Act was revised several times and published in 1989. Figure 1 shows the evolution of the most popular data protection acts worldwide from 1948 to 2021. "Several data protection drafts were proposed after 2021 but were not included in this review."

The United States (US) is a group of more than 50 states, and no single data protection legislation can be implemented in all states. Each state has its data protection regulations. In 1974 the United States proposed “The United States Privacy Act”. It acts as a safeguard for collecting individual personal data such as name, mobile number, DoB, UIDN, etc., along with storage, processing, and disposal of individual records. Later, several privacy acts were proposed by individual states, and the most popular privacy acts in the US are the California Consumer Privacy Act (CCPA) [22], California Privacy Rights Act (CPRA) [22], Virginia's Consumer Data Protection Act, Colorado Privacy Act (CPA), etc. In 1984, the United Kingdom (UK) proposed an act named the “Data Protection Act (DPA)” [19] to control the use of collected individual data and it’s processing. The primary role of the DPA was to establish a wide set of principles and practices to safeguard data across different sectors of the economy.

IV. WORLD’S MOST PREVALENT DATA PROTECTION ACTS (DPA)

Nowadays, every country of the world has a prime concern to protect and secure the data of its citizens, which organizations accumulate. For the same reason, most of governments have developed data protection codes of conduct, which they regularly review and improve. The present section deals with a broad discussion of the world’s most popular data/privacy protection acts. Each data protection act has some key elements/role players.

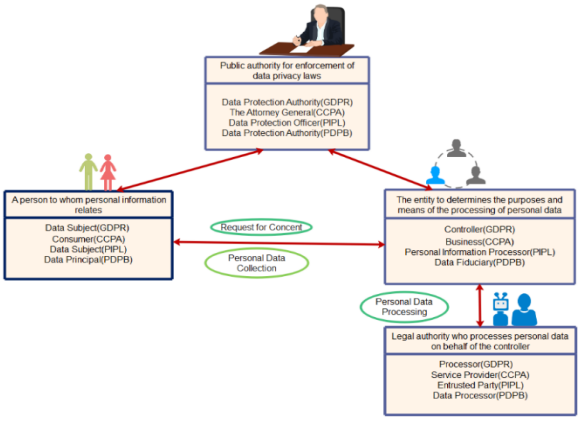

Fig. 2. Key Role Players of Renowned Data Protection Laws

Figure 2 provides an overview of the key elements and role players in relation to the General Data Protection Regulation (GDPR) [23-32], the California Consumer Privacy Act (CCPA) [22][33-34], the Personal Information Protection Law (PIPL) [35-46], and the Personal Data Protection Bill (PDPB) [47-49].

A. General Data Protection Regulation (GDPR)

It is a refined and extended form of the Data Protection Act (DPA) proposed in 1984 and the Data Protection Directive (DPD) proposed in 1995 for the European Union (EU). It has a bundle of 99 articles divided into 11 chapters. Each chapter deals with specific articles in a particular activity, such as general provisions, principles, rights, security, liabilities, penalties, etc. The GDPR aims to harmonize data protection laws across EU Member States by reducing complexity, legal fragmentation, and uncertainty. It applies to all Member States. However, Member States can implement their specific features under ‘derogations’ related to national security, judicial, financial, and public interest. According to GDPR, organizations should implement strict and efficient models for data protection. For this purpose, individual consent should be taken, and personal data handling policies must be shared with them. It shows the user-centric approach of GDPR. The GDPR also forces organisations to opt for a transparent data usage policy to make the data available for analysis. Transparency can be achieved through customized, reflective, and dynamic options instead of tick-box compliance. GDPR offers an information governance framework for Organizations and controls individuals' data. The present subsection briefly introduces the GDPR progression, entities, principles, and rights. Figure 3 shows the implementation process of GDPR on a timeline.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

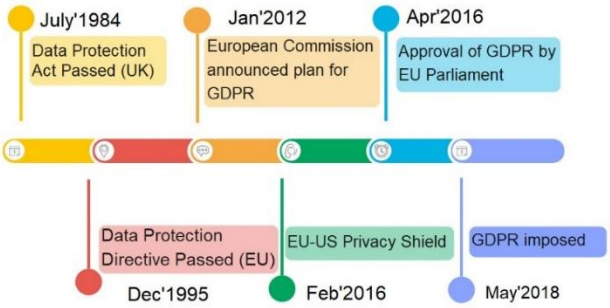

Fig 3. GDPR implementation process on the timeline

1) Key Role Player in GDPR
a) Data Subject: People whose personal data is collected by different organizations for processing.
b) Controller: A natural/authorised person, public authority, bureau/ individual organisation that governs the intent and reasons for processing personal data.
c) Processor: The processor is responsible for processing and handling personal data as per the instructions provided by the controller.
d) Data Protection Authority: The public authority is liable for enforcing the Data Protection Act.
2) Principles of GDPR
a) Lawfulness, fairness, and transparency: According to Article 5(1)(a) of the GDPR, lawfulness requires that the processing of personal data is carried out for legitimate and legal purposes. Fairness compels the collected data to be used for identified purposes. Transparency is being honest, open, and truthful with data subjects.
b) Purpose limitation: Under Article 5(1)(b) of the GDPR, the purpose for collecting personal data must be clearly defined, legitimate, and adhered to, without being changed after the data is gathered. In exceptional conditions, if an alteration in boundaries and purpose is required, then proper consent from the data subject should be taken with justification by describing an additional purpose.
c) Data Minimization: As per Article 5(1)(c) of the GDPR, it prohibits excessive data collection. The personal data collected for processing should be modest, adequate, and appropriate to fulfil the intention of data collection.
d) Accuracy: As per Article 5(1)(d) of the GDPR, the collected and stored data should be accurate; regular data accuracy checks should be done. However, the data subjects can also have the right to rectify, i.e., erase or update the inaccurate data collected by the controller.
e) Storage Limitation: Under Article 5(1)(e) of the GDPR, personal data must be retained only for a justified and predetermined period, after which the data controller must delete it.
f)Integrity and Confidentiality: According to Article 5(1)(f) of the GDPR, data controllers must implement clear policies and measures to ensure the integrity and confidentiality of personal data, protecting it against accidental loss, unauthorized access, as well as unlawful processing.
g) Accountability: Article 5(2) of the GDPR states that the Controller is responsible for data processing at each stage. They must opt for the best rank of accountability practice and document every step with justification.
3) Fundamental Rights in GDPR
a) Right to be Informed/Transparency: As per Articles 13 and 14 of the GDPR, the data subject has the right to know about what information is being collected, who is collecting it, the purpose of collecting the data, and how long the controller will retain the data.
b) Right to access: As per Article 15 of the GDPR, the data subjects can trace and get a reprint of their data and supplement information. However, it increases the cost to the controller in terms of human efforts and time.
c) Right for rectification: Under Article 16 of the GDPR, data subjects are entitled to request the correction or updating of their information whenever it is inaccurate or unclear at any point of time.
d) Right to forget: Article 17 of the GDPR states that the data subject can force the controller to erase their data.
e) Right to restrict: Under Article 18 of the GDPR, data subjects can exercise the right to limit how their information / personal data is processed.
f)Right to data portability: Under Article 20 of the GDPR, individuals can move their data between different data controllers.
g) Right to object: Under Article 21 of the GDPR, data subjects may oppose the processing of their personal data for any analytical purposes.
h) Right not to be part of automated decision-making: Article 22 of the GDPR restricts automated processing and decision making based that has legal impact on the data subject.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

B. California Consumer Privacy Act (CCPA)

The United States (US) is the fourth-largest geographical area globally and has no unique federal consumer data protection law. However, later on, various laws were introduced to deal with consumers' personal information. Some of the most popular laws are the "Health Insurance Portability and Accountability Act (HIPAA)", the "Children's Online Privacy Protection Act (COPPA)", etc. Still, these were not adequate to protect all consumers' personal information. In January 2018, to shield the privacy rights of its citizens, California introduced the CCPA as the personal data protection law and implemented it in January 2020. The Present subsection briefly introduces the CCPA progression, entities, principles, and rights. Figure 4 shows the implementation process of CCPA on a timeline.

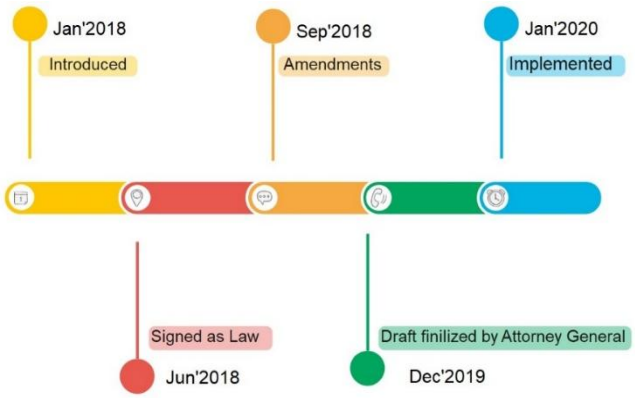

Fig. 4. CCPA implementation process on the timeline

1) Key Role Player in CCPA
a) Consumer: They are natural persons whose personal data is being collected by organisations for processing.
b) Business: A business is a profit-driven legal entity that sets the objectives and guidelines for handling personal data in California.
c) A legal entity operating in California to earn a profit. Business defines the motive and norms for processing personal data.
d) Service Provider: A service provider is an organization that processes information on behalf of a business. For this, a written contract must be required from the industry.
e) Third Party: An organization that collects consumer data from businesses and processes it for sale. It does not have a written contract with the company. In CCPA, consumers have the right to op" not of sharing their data with third parties.
f)Attorney General: In the CCPA, the Attorney General is responsible for enforcing data protection law and handling the related issues.
2) Principles of CCPA
a) Transparency: The basic aim is to build trust among consumers. The CCPA provides specific transparency obligations for collecting, processing, and selling personal data. A business must reveal consumers' privacy rights through privacy notices or on its website.
b) Control: CCPA provides high-order control over consumers' data through available consumer rights.
c) Accountability: In CCPA, businesses must be accountable for protecting consumers' data from any theft, accidental loss, or misuse.
3) Fundamental Rights of CCPA
a) Right to know: It allows consumers to learn about what businesses collect personal data, the purpose of collected data, its processing methods, and to whom it can be shared.
b) Right to delete: Consumers can request the deletion of personal data that a business collects.
c) Right to opt-out: This allows flexibility for consumers, whether they want to permit the selling of their data to a third party or not.
d) Right to non-discrimination: It allows all consumers equality of the rights of the CCPA without any discrimination.

C. Personal Information Protection Law (PIPL)

PIPL is a generic phrase used for regulation in China. It is defined as privacy protection along with other rights of individuals. In the early stages, sectoral laws were defined to deal with privacy issues, such as criminal law and civil law. Due to exponential growth in data breaches and trading compatibility issues with other countries' data regulation acts, China proposed a national data privacy framework. In the initial stage, the data protection

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

rules of China were influenced by US data protection regulations; later on, it diverged towards the comprehensive law framework of the EU.
In China, "The Ministry of Industry and Information Technology (MIIT)" approved the "Telecommunication and Internet Personal User Data Protection Regulation" in 2013; subsequently, the "Cybersecurity Law" was implemented in 2017. Later on, the Data Security Law was endorsed in June 2021. Building on this foundation, in August 2021, a comprehensive draft of the Personal Information Protection Law (PIPL) was introduced and officially enforced in November 2021 to address both domestic and international legislative concerns in China. Figure 5 shows the implementation process of PIPL on a timeline.
PIPL is a bundle of 74 articles and is divided into 08 chapters. PIPL applies to all personal information processing in China, regardless of the data subject's location. The Present subsection briefly introduces PIPL progression, entities, principles, and rights.

1) Key Role Player in PIPL
a) Data Subject: A Data Subject under PIPL is any natural person whose personal information is handled by organisations or businesses.

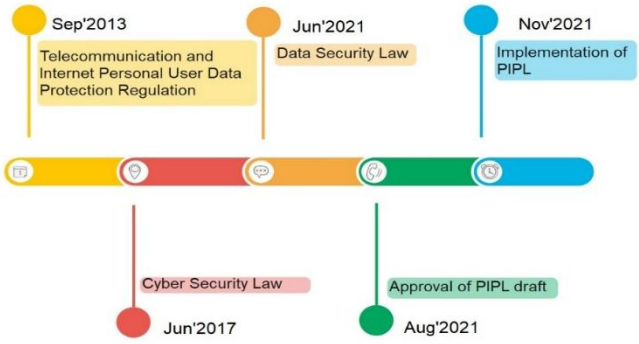

Fig.5. PIPL Implementation process on the timeline

b) Personal Information Processor (PIP) / Personal Information Handler (PIH): An individual or organization independently determines the purpose and methods for processing personal data. Under PIPL, the "Joint Information Processor" is accountable for addressing issues related to violating an individual's personal information rights.
c) Entrusted Party: A PIP-trusted party processes personal information analytically per PIPS guidelines. It is also responsible for taking necessary actions to secure the data subject's personal information.
d) Data Protection Officer: It is accountable for overseeing and managing the processing of data subjects' personal data and ensuring that the protection measures are in place.
2) Principles of PIPL
a) Lawfulness, Necessity: As per Article 5 of the PIPL, the processing of personal data should be legitimate and limited to the necessity of that particular purpose for which it is collected. The organization must maintain good faith in the data subject while drafting, analyzing, and fulfilling the obligations of privacy policies and official binding documents.
b) Purpose Limitation: As per Article 6 of the PIPL, there should be a specified and reasonable purpose for processing personal information, and it should not adversely impact data subjects' rights.
c) Collection limitation: The collection of personal data should be minimal, which could accomplish the purpose of the collection.
d) Openness and transparency: As per article 7 of the PIPL, Organizations processing personal data should clarify the purposes, ways, and scale of processing data subject to maintain openness.
e) Accuracy: As per Article 8 of PIPL, the collected or stored personal information should be accurate, complete, and reviewed promptly for any updates if required.
f)Accountability and Security: As per Article 9 of PIPL, the security of collected or stored personal information is the responsibility of personal information handlers. He must ensure the use of protection measures to secure the data from theft or accidental loss.
3) Fundamental Rights of PIPL
a) Right to know: According to Articles 17, 18, and 48 of the PIPL, a Personal Information Handler (PIH) must notify the data subject about the purpose, processing methods, and retention period of their data before any processing taking place.
b) Right to object: As per Article 44 of PIPL, Data subjects have the right to refuse data processing.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

c) Right to access: Article 45 of the PIPL stipulates that data subjects have the right to demand a copy of their personal data collected by a personal information handler.
d) Right to data portability: Under Article 15 of PIPL, the data subject has the right to data portability if the information stored by the information processor meets specific conditions of the Cyberspace Administration of China (CAC).
e) Right for correction: Data subjects can call to correct their data if found inappropriate.
f)Right to deletion: As per article 47 of PIPL, the data subject's personal information must be deleted when its purpose is completed or the retention period is over; the data subject has withdrawn the consent, which is a legal violation by the personal information handler.
g) Automated Decision-Making: Article 24 of PIPL states that the data subject can superimpose their requests over automated decision-making. Consent of the data subject plays the most crucial role in PIPL for processing personal data during data collection and at various steps, like sharing, disclosure, or transfer to other parties.

D. Personal Data Protection Bill (PDPB)

India has the longest written constitution, with 395 articles divided into 22 parts. The right to privacy is defined in Article 21. In 2000, the Information Technology Act (IT ACT 2000) was enforced to recognise Electronic Commerce legally. The act defines “data” and specifies the hacking and data breach penalties. It was further amended to the IT Act 2008 by incorporating electronic signatures, an enhanced cyber law framework, and additional data protection and privacy provisions. Subsequently, the “Information Technology Act 2011” was established. In 2017, an official committee was formed to draft the Personal Data Protection Bill (PDPB) based on the GDPR. By 2018, the committee presented a draft comprising 15 chapters and subsections, classifying data into three categories: personal, sensitive, and critical personal data. This subsection provides a brief overview of the progression of the PDPB, its entities, principles, and rights. Figure 6 shows the implementation process of PDPB on a timeline.

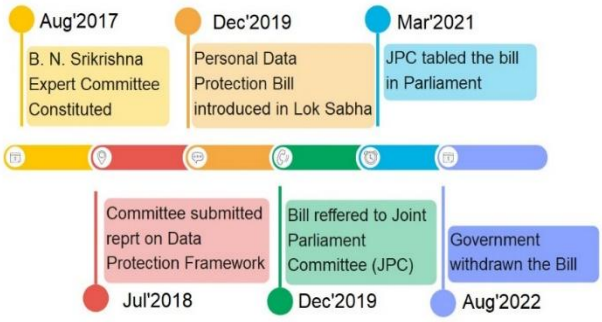

Figure 6: PDPB implementation process on the timeline

1) Key Role Player in PDPB
a) Data Principal: A data principal is a person whose data is being collected or processed.
b) Data Fiduciary: A data fiduciary is an individual, government body, organization, or legal entity that determines, alone or in collaboration with others, the purposes and methods of processing personal data.
c) Data Processor: A data processor is an individual, entity, organization, or legal body that processes personal data on behalf of a Data Fiduciary.
d) Data Protection Authority: The data fiduciary should designate a Data Protection Officer to oversee personal data processing activities and serve as the principal point of contact between the data principal and the data fiduciary in the event of grievances.
2) Principles of PDPB
a) Purpose Limitation: According to Chapter 2, Section 5 of the PDPB, the purpose of processing personal data must be fair and reasonable, ensuring that it does not infringe upon the privacy of data principals
b) Collection limitation: As per Chapter 2, section 6 of PDPB, the amount of collected personal data should be minimal, which is required for fulfilling the purpose of processing.
c) Specific, clear, and lawful: As per Chapter 2, section 7 of PDPB, it is mandatory for data fiduciaries to deliver precise details of collected specific information and the approach used for processing. This processing of personal data should be done legitimately.
d) Accuracy: As per Chapter 2, section 9 of PDPB, the data fiduciary should ensure that the collected personal data is complete, precise, and up to date.
e) Transparency and Accountability: As per Chapter 2, section 11 and Chapter 7, section 30 of PDPB, privacy policies of data fiduciaries should be transparent and accountable. Data fiduciaries should protect collected or stored data by using various security measures.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

f)Consent of data principals: As per Chapter 3, section 12 of PDPB, consent of data principals is compulsory in PDPB before processing the personal data.
3) Fundamental Rights of PDPB
a) Right of Confirmation: Chapter 6, section 24 of PDPB acknowledges the data principle about the processing of personal information.
b) Right to Correction: As per Chapter 6, section 25 of PDPB, the data principal can ask to correct personal information if it is inappropriate.
c) Data Portability: As per Chapter 6, section 26 of PDPB, the data principal can demand personal data transfer from one data fiduciary to another under specific circumstances.
d) To be Forgotten: As per Chapter 6, section 27 of PDPB, data principals can restrict the discloser of their personal information if they find the reason for which the collection is accomplished; in such cases, they can withdraw their consent or if the data principal finds its data is indulged in some prohibited activities.

The previous Data Protection Bill was scrapped, and in 2022, the Ministry of Electronics and Information Technology (MeitY) introduced a revised version called the "Digital Personal Data Protection Bill (DPDP)." The DPDP Bill was presented on August 3, 2023, and passed by the Lok Sabha (Lower House) on August 7, 2023, followed by the Rajya Sabha (Upper House) on August 9, 2023. After receiving the President's assent, it was officially gazetted and became law on August 11, 2023. Following amendments to the DPDP Act (2023), MeitY released a draft of the new Digital Personal Data Protection Rules on January 3, 2025. These rules provide a framework for enforcing the DPDP Act, including details on the responsibilities of data fiduciaries, data subject rights, and security measures. The draft is being circulated for public review, and a committee has been set up to gather suggestions from both individuals and organizations. The final version of the Data Protection Act is expected to be published soon..

V. Comparative Analysis of Data Protection Acts

The United Nations (UN) declared privacy a fundamental human right. Privacy advocates individual control over the data collection and processing with confidentiality. Every country is drafting or has already proposed a Data Protection Law to protect consumer's data. Table 1 shows the comparative analysis of the world's most popular data protection acts, i.e., CCPA, GDPR, PIPL, and PDPB, based on specific features.

Table 1. Qualitative Analysis of Data Protection Laws

S. No.	Attributes	CCPA	GDPR	PIPL	PDPB
1	Proposed On	Jan-2018	Apr-2016	Aug-2021	Jul-2018
2	Implemented On	Jan-2020	May-2018	Nov-2021	Not Implemented
3	No. of Articles	NA	99	74	NA
4	No. of Sections / Chapters	NA	11	8	15
5	A person to whom personal information is related	Consumer	Data Subject	Data Subject	Data Principal
6	The entity that defines objectives and procedures for personal data processing	Business	Controller	Personal Information Processor	Data Fiduciary
7	Legal authorities who are responsible for the personal information processing on behalf of the data collector	Service Provider	Processor	Entrusted Party	Data Processor

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

8	No. Of. Principles / Obligations	3	7	6	6
9	No. of Rights	4	8	7	4
10	Sensitive information	Name, address, Social Security Number (SSN), religious beliefs, political beliefs, Fingerprints, Genetic Data, Email Address, Products purchased, Internet Browsing History, IP address, Unique cookie ID, and Geolocation data.	Racial data, political preference, religious information, genetic information, biometrics, sexual preference, and health records of EU citizens	Biometrics information, religious orientation, identification details, health records, financial data and location stalking and data of minors	Passwords, financial information, Health records, sexual preference, biometric details, genomic data, transgender status, caste or tribe, religious belief
11	Rules for Implementation / Applied on	For-profit business entities operational in California that satisfy any of the following criteria: ➢ Gross revenue ≥ $25 million. ➢ Buying, processing, or selling personal data of ≥50000 consumers ➢ Derives more than half of its annual revenue by selling/sharing consumers' personal information.	Data Controllers and Data Processors: ➢ Founded in the EU and involved in processing data subject information to establish the EU irrespective of location. ➢ Who is outside the EU and processing the personal information of EU's data subjects for offering them benefits/services?	Individuals/ Organizations: ➢ These are processing personal information of data subjects in China, apart from their nationality and location. ➢ These are located outside China and process the personal data of data subjects to provide better goods/services, along with their behavior analysis, under Chinese law and regulation.	Organizations /Individuals: ➢ Which are responsible for processing personal data of data principal accumulated, shared, and revealed within the Indian Territory. ➢ These are involved in processing and profiling activities on personal data of data principals within the Indian Territory for business purposes. ➢ Which processes personal data collected by Indian states, companies, citizens, and individuals under Indian laws.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

12	Intended to	Enhancement of consumer rights and privacy protection for residents of California	Enhancement of individuals' rights and controlling power of data subjects within the European Economic Area (EEA).	Enhancement of personal information rights of data subject and elucidate laws for data handling and processing.	Enhancement of data subject's controlling power over processing of their data.
13	Protection for	Consumers residing in California for temporary purposes or have domicile in California.	Data Subject	Data Subject	Data Principal
14	Penalty	The penalty varies with the type of violation and could be up to: ➢ $2,500 for every violation ➢ $7,500 for every intentional violation	Penalty varies with the type of violation and could be up to either: ➢ 2% of global annual turnover or €10million, whichever is higher; or ➢ 4% of global annual turnover or €20million, whichever is higher.	Risk of losing business licenses and monetary penalties of up to $ 7.8 million or 5% of the previous year's turnover.	The extreme penalty stipulated may be increased up to ➢ Rs. 15,00,00,000 or ➢ 4% of the penalized total worldwide turnover in the previous financial year, whichever is higher.
15	Automated decision-making and Profiling	In the CCPA, automated decision-making or data profiling is under the opt-out right.	Data subjects' personal information should not be part of automated decisions such as profiling unless the data subject has permitted it.	In PIPL, the consumer can refuse automated decision-making on their data by using the opt-out option.	There is no such provision.
16	Breach Notification	A business must notify a consumer whose personal information is acquired by an unauthorized person.	Controllers must notify DPA of the breach within 72 hours. The controller will inform individuals about violations when they cause 'high risk'.	Information must be given to the data protection department about the breach. However, individuals are informed only when it is causing or may cause harm to them.	Data fiduciaries must notify the DPA as soon as possible about a data breach when it may harm the data principal. DPA may post about the data breach on the website or ask the data fiduciary to do so.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

17	Protection of children's data	In the CCPA, opt-in consent for minors and parental consent for children is mandatory before selling their data under the CCPA. Persons under 16 years are referred to as minors and those under 13 years are children.	In GDPR, children are considered 'vulnerable natural persons'. Parental consent is necessary to provide information society services to children under 16. EU member states can decide on a lower age, which should not be under 13 years.	In PIPL, it is necessary to ask for the consent of a guardian before processing the personal information of minors under the age of 14 years. Data related to minors is considered sensitive personal information here.	In PDPB, children under 18 years old are considered children. Data fiduciaries must verify the child's age and obtain appropriate consent from the guardian before processing the child's data.
18	Data Audits	To prove your business compliance, data auditing is necessary. A third-party auditor will be appointed to conduct this. The audit checklist includes: ➢ Responding to Consumer Rights ➢ Required Disclosures ➢ Constraint on Selling Personal Information ➢ Information Retention ➢ Personal data re-identification ➢ Permissible financial incentives for collecting, selling, and erasing personal Information ➢ Employee training associated with consumer rights ➢ Third-party supervision ➢ Duty to implement and	No specified article in the GDPR advocates data auditing. Still, during the auditing, the data processor is responsible for: ➢ Handling of personal data ➢ Scope of application ➢ Lawful grounds for processing ➢ Transparency requirements ➢ Other data protection principles and accountability ➢ Data subject rights ➢ Data security ➢ Data breaches	An organization must audit its compliance with Chinese personal information protection laws and regulations. .	Independent auditors must accomplish the auditing process. Data auditors evaluate the compliance of the data fiduciary and submit data trust scores regarding the effectiveness of measures, security safeguards, transparency, and timely implementation of processes, etc.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

		maintain security measures ➢ Breach response			
19	Cross-border transfer of data	The CCPA, as a state law, does not explicitly regulate the transfer of personal information across international borders.	It may be transferred without restriction if EU authorities ensure adequate safeguards for data protection by third parties or countries. Furthermore, data protection certification mechanisms may allow cross-border transfer of data, which is approved by a competent supervisory authority and issued for a maximum period of 03 years. After the specified period, the certificate may be renewed.	Need consent from the relevant individual, and at least one of the following conditions must be satisfied: ➢ Must pass security evaluation performed by the Cyberspace Administration of China (CAC). ➢ Must have a "Personal information protection certificate" issued by a CAC-accredited authority or institution. ➢ Must follow the standard contracts published by the CAC.	It may be transferred to organizations nationwide if the data fiduciary ensures that the authority issues the data protection safeguards.
20	Rectification of Data	Not Allowed	Allowed	Allowed	Allowed
21	Response Time of Consumer Complaint	30 Days	40 Days	45 days	30 Days
22	The authority responsible for Data Security	A business must notify a consumer whose personal information is acquired by an unauthorized person.	Data controllers and Processors are responsible for setting up security levels to deal with the risk.	The personal information processor is responsible for technical security measures.	Data fiduciaries and data processors are responsible for implementing essential security precautions.
23	Legal Base for processing	CCPA does not have any legal framework for the processing of personal data. According to the CCPA, consumer consent is required when a business is entering any	GDPR has 06 lawful bases for the processing of personal data. ➢ Individual permission ➢ Execution of a contract ➢ Legal obligation ➢ Legal interests	PIPL has 07 lawful bases for processing personal data: Individual consent. ➢ Conclude or accomplish on contract. ➢ Necessary for legally approved contractual	PDPB has 07 legal bases for the processing of personal data: ➢ Consent ➢ Employment ➢ Obligation / Legitimate ➢ A health emergency or situation may cause a threat to life. Providing

		program that provides financial incentives for the use of personal data	➢ Life protection and essential welfare ➢ Public interests	obligations or commitments. ➢ Required for public health confrontations. ➢ For news reporting. ➢ Information disclosed by individuals themselves. ➢ Situation bylaws or governmental regulations.	medical health services ➢ Providing individual safety during a calamity. ➢ Any reasonable purpose defined in law for inhibiting or detecting unlawful actions. ➢ Special Purpose Data Processing (e.g., Research, Public Interest, etc.)

VI. CONCLUSION

In the present digital era, privacy is one of the supreme concerns for an individual. Organizations are processing their stakeholders' collected personal data without their consent and revealing it to third parties. To deal with such issues, most countries have proposed data protection acts. The most popular data protection acts implemented/proposed by California, the EU, China, and India are CCPA, GDPR, PIPL, and PDPB. These data protection acts are compared based on significant parameters such as principles, rights, key entities involved in processing sensitive information, cross-boundary rules, auditing, age, the legal basis for processing, penalties, etc. The comparative analysis observed that most data protection acts have the same characteristics, with a moderate difference. The definition of personal data is much broader in CCPA and PDPB than in GDPR and PIPL. There is a substantial overlap between how sensitive data is defined in all frameworks. The territorial reach of GDPR and PIPL is broader than that of CCPA, while PDPB covers potentially more significant space than these. Furthermore, PIPL and PDPB both include financial data in the category of sensitive personal information, while the rest do not consider it the same. There is a significant variation in principles for processing personal data; the CCPA has three principles, PIPL and PDPB have six principles, and GDPR has seven. Likewise, CCPA and PDPB have four consumer rights, while PIPL and GDPR have seven and eight consumer rights, respectively. CCPA has no legal base for processing personal data, and the other three have a similar legal base. The threshold values for children are 18, 16, and 14 in PDPB, CCPA, and PIPL, respectively, while in GDPR, it is 16, but EU member states can opt between 13 and 16. In GDPR, consumers have rights related to profiling, while in PIPL and CCPA, it is a part of the opt-out right, and in PDPB, there is no such provision. In GDPR and PDPB, it is compulsory to notify the data processing authority about the data breach, and the data processing authority may take necessary actions, while in PIPL, information is to be given to the department handling data protection. At the same time, there are no predefined rules for CCPA. The article provides a preliminary state-of-the-art review of the world's most popular data protection laws.

REFERENCES

[1] Pelteret, M.; Ophoff, J. A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science: The International Journal of an Emerging Transdiscipline. 2016, 19(1), 277–301.
[2] What Is Data Privacy? Available online: https://www.snia.org/education/what-is-data-privacy (accessed on 04 May 2022).
[3] Pötzsch, S. Privacy awareness: A means to solve the privacy paradox? The Future of Identity in the Information Society. 2009, 298, 226–236.
[4] Yao-Huai, L. Privacy and data privacy issues in contemporary China. Ethics Inf. Technol. 2005, 7, 7–15.
[5] Michael, J.; Kuhn, R.; Voas, J. Security or Privacy: Can You Have Both? Computer 2020, 53, 20–30.
[6] Olukoya, O. Assessing frameworks for eliciting privacy & security requirements from laws and regulations. Computers & Security, 117, June 2022, 102697.

[7] Boardman, R.; Munoz Rodriguez, J. The EU Data Governance Act: What Privacy Professionals Need to Know. Available online: https://www.twobirds.com/en/insights/2022/global/the-eu-data-governance-act-what-privacy-professionals-needto-know (accessed on 30 April 2022).
[8] Veliz, C. Privacy is Power: Why and How You Should Take Back Control of Your Data. Bantam Press, UK, September 2020.
[9] Data Privacy Guide: Definitions, Explanations and Legislation. Available online: https://www.varonis.com/blog/data-privacy/ (accessed on 02 September 2022).
[10] Pötzsch, S. Privacy awareness: A means to solve the privacy paradox? Future Identity Inf. Soc. 2009, 298, 226–236.
[11] Privacy, reputation, and control: public figure privacy law in contemporary China, Peking University Law Journal, 9 (2), 2022, 143-146.
[12] ISO/IEC 27001:2013; Information Security, Cybersecurity and Privacy Protection. International Organization for Standardi-zation: London, UK, 2013.
[13] Sadowski, J.; Viljoen, S.; Whittaker, M. Everyone should decide how their digital data are used, not just tech compa-nies. Nature 2021, 595, 169–171.
[14] Richards, Neil M. The Dangers of Surveillance. Harvard Law Review, 2013, Available online: https://ssrn.com/abstract=2239412.
[15] Goswami, V. What does big tech do with your data? Forbes Technology Council, Available online: https://www.forbes.com/sites/forbestechcouncil/2022/02/16/what-does-big-tech-actually-do-with-your-data/?sh=56bdf4d6515f (accessed on 16 July 2022).
[16] Seubert, S.; Becker, C. The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection. Ger. Law J. 2021, 22, 31–44.
[17] Blume, P. Data protection and privacy- Basic concepts in a changing world. Scandinavian Studies in Law. 2010, 56, 151–164.
[18] Cobb, S. Data Privacy and Data Protection: US Law and Legislation. ESET White Paper. 2016, 1–15. Available online: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjn3vC63IP6AhUzmYQIHRFuDT4QFnoECBkQAQ&url=https%3A%2F%2Fwww.welivesecurity.com%2Fwp-content%2Fuploads%2F2018%2F01%2FUS-data-privacy-legislation-white-paper.pdf&usg=AOvVaw1lYtt_VABfuVYTTWIuQpXy (accessed on 12 October 2021).
[19] Seubert, S.; Becker, C. The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection. German Law Journal. January 2021, 22 (1), 31–44.
[20] Universal Declaration of Human Rights. 1948. adopted by the UN General Assembly on 10 December 1948.
[21] Federal Data Protection Act (Bundesdatenschutzgesetz—BDSG); BDSG: Germany, 2019.
[22] State of California Department of Justice. California Consumer Privacy Act (CCPA). 2020. Available online: https://oag.ca.gov/privacy/ccpa (accessed on 13 June 2023).
[23] A Tovino, S. The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons. Seton Hall Law Rev. 2017, 47, 973–993.
[24] Voss, W.G. Cross-Border Data Flows, the GDPR, and Data Governance. Wash. Int. Law J. 2020, 29, 485–532.
[25] GDPR. Data Protection Impact Assessments, Article 35 of GDPR. Available online: https://gdpr-info.eu/art-35-gdpr/ (accessed on 5 May 2022).
[26] Voss, W.G. Cross-Border Data Flows, the GDPR, and Data Governance. Washington International Law Journal. 2020, 29(3), 485–532.
[27] Robol, M.; Salnitri, M.; Giorgini, P. Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework. Lecture Notein Business Information Processing book series, 305, 2017; 236–250.
[28] Chhetri T. R.; Kurteva A.; DeLong R. J.; Hilscher R.; Korte K; Fensel A. Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. Sensors, April 2022, 22(7), 2763.
[29] Voss, W. G. Cross-Border Data Flows, the GDPR, and Data Governance. Washington International Law Journal, 2020, 29 (3), 485–532.
[30] Brodin, M. A framework for GDPR compliance for small and medium-sized enterprises. European Journal for Security Research. 2019, 4, 243–264.
[31] GDPR (General Data Protection Regulation). Available online: www.gdpr-info.eu (accessed on 18 August 2022).
[32] Ernst & Young. The California Consumer Privacy Act: Overview and Comparison to the EU GDPR. Available online: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-the-california-consumer-privacy-act.pdf (accessed on 7 October 2021).

[33] CCPA (California Consumer Privacy Act). CCPA and GDPR Comparison Chart. Available online: https://iapp.org/resources/article/ccpa-and-gdpr-comparison-chart/ (accessed on 01 August 2022).
[34] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100. 2018. Available online: https://www.spirion.com/wp-content/uploads/2020/07/Spirion_CCPA_v3.pdf (accessed on 10 January 2022).
[35] Gamvros, A.; Wang, L. PIPL: A Game Changer for Companies in China. Available online: https://www.dataprotectionreport.com/2021/08/pipl-a-game-changer-for-companies-in-china/ (accessed on 22 June 2022).
[36] PIPL (Personal Information Protection Law). Available online: https://m.thepaper.cn/baijiahao_14154156 (accessed on 7 October 2021).
[37] The China Personal Information Protection Law (PIPL). Available online: https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html (accessed on 30 July 2022).
[38] The Personal Information Protection Law in China: A Legal Analysis. Available online: https://www.china-briefing.com/news/the-personal-information-protection-law-in-china-a-legal-analysis/ (accessed on 30 September 2021)
[39] The China Personal Information Protection Law (PIPL). Available online: https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html (accessed on 22 June 2022).
[40] Personal Information Protection Law (PIPL). Available online: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (accessed on 14 September 2022).
[41] Creemers R. China's emerging data protection framework. Journal of Cybersecurity, 2022, 1–12.
[42] Larry, Y. The emergence of social entrepreneurs in China. Journal of the International Council for Small Business. 2020, 1(1), 32–35.
[43] Yao-Huai, L. Privacy and data privacy issues in contemporary China. Ethics and Information Technology. 2005, 7(1), 7-15.
[44] Chen, J.; Sun, J. Understanding the Chinese Data Security Law. International Cybersecurity Law Review, 2021, 2, 209–221.
[45] Zheng, G. Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China: computer & Law Security Review, November 2021, 43, 105610.
[46] Calzada, I. Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities, 2022, 5(3), 1129-1150.
[47] Mathu, S. Indian PDPB 2019: Data trust score. Available online: https://www.dqindia.com/indian-pdpb-2019-data-trust-score/. (Accessed on 16 July 2022).
[48] Srinivas, N.; Biswas, A. Protecting Patient Information in India: Data Privacy Law and its Challenges. NUJS Law Review, 5, 2012, 1-14.
[49] Singh, R. G.; Ruj, S. A. Technical Look at The Indian Personal Data Protection Bill. Available online: https://arxiv.org/abs/2005.13812 (accessed on 13 July 2022).