LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 2

2023

A COMPARATIVE ANALYSIS OF THE DPDP BILL AND OTHER PRIVACY LAWS

Sneha Agarwal[1] & Ayush Pandey[2]

I. ABSTRACT

The Data Protection and Digital Privacy (DPDP) Bill, a fictitious privacy legislation, is compared in this research to actual privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). To further appreciate how the DPDP Bill could affect privacy protection, it is important to look at its commonalities, differences, strengths, and special characteristics.

The examination starts off by looking at the basic ideas behind the DPDP Bill and other privacy regulations. Data subject rights, permission requirements, data breach notifications, enforcement procedures, and extraterritorial application are important areas of concern. The research intends to find similarities and differences between the DPDP Bill and current legislation by comparing these elements.

The study underlines how the DPDP Bill and other privacy laws are comparable in terms of the creation of data protection bodies, the importance of informed consent, and the ability to access and correct personal data. These common goals and guidelines show a coordinated effort to solve privacy issues and guarantee data security.

On the basis of the implementation and enforcement of current privacy regulations, various obstacles and objections related to the DPDP Bill are also considered. Costs associated with compliance, regulatory complexity, and finding the ideal balance between privacy protection and data-driven innovation may all be part of these difficulties.

Policymakers, legal professionals, and stakeholders may benefit greatly from the conclusions of this comparative research by using them to better understand the implications of the DPDP Bill and its potential efficacy in protecting digital privacy. The research aids in the creation of

[1] student at National Law Institute University, Bhopal.
[2] student at National Law Institute University, Bhopal.

strong privacy frameworks and the continuing discussion of privacy laws by enabling informed decision-making.

II. KEY WORDS

California Consumer Privacy Act, General Data Protection Regulation, Personal Information Protection and Electronic Documents Act, Personal Information Protection Law, Digital Personal Data Protection.

III. INTRODUCTION

In today's world where the flow of information has become routine, data security and privacy are a vital concern. The development of technology has made personal data increasingly prone to theft, abuse, and manipulation. Numerous data protection and privacy laws have been introduced as a result of the need to safeguard personal data and control how businesses acquire, handle, and utilise it. The PIPEDA of Canada, the GDPR of the European Union, the PIPA of Hong Kong, and the CPRA of California are the four nations whose data protection and privacy laws will be covered in this essay. An overview of each rule, its major clauses, and comparisons and contrasts between them will be covered in the debate.

Overview of Data Protection and Privacy Regulations. First, we cover the General Data Protection Regulation 2016 (GDPR), which is the world's most comprehensive data protection and privacy regulation that took effect in the European Union (EU) in May 2018. The 1995 Data Protection Directive is replaced by the GDPR, which is applicable to all EU member states. Regardless of whether they are situated in the EU or not, all organisations that handle the personal data of EU individuals must comply with the GDPR. "Any information which are related to an identified or identifiable natural person" is the definition of personal data in Article 4(1) of the GDPR. The European Union's GDPR provides a framework for how various jurisdictions should structure their data protection legislation.

The next federal legislation that controls the gathering, use, and disclosure of personal information by organisations in Canada is the Personal Information Protection and Electronic Documents Act (PIPEDA). Except for those that are subject to provincial

regulation, the legislation is applicable to all private sector organisations. The goal of PIPEDA is to strike a balance between an individual's right to privacy and an organization's need to acquire, utilise, and disclose personal information for lawful business reasons.

Similar to other countries, China has enacted a data protection and privacy legislation known as the Personal Information Protection legislation, which went into effect on November 1, 2021. It serves as the foundation for China's data protection system. It is crucial for China's national security and the general interest that the legislation apply to both domestic and international data processing operations.

The California Consumer Privacy Act (CCPA), a data protection and privacy legislation, became operative in California, USA, in January 2020. It is the main statute in force in the US. Regardless of where they are located, all businesses that gather and use personal data on California residents are subject to the law. The CPRA offers Californians more control over their personal information and the right to know what information businesses have about them, what they are doing with it, and why.

The Digital Personal Data Protection (DPDP) bill is a suggested piece of legislation with the goal of defending peoples' rights to their personal data privacy. Other privacy laws that address the protection of personal data in their respective capacities include the California Privacy Rights Act (CPRA), the General Data Protection Regulation (GDPR), the Personal Information Protection Law (PIPL) of China, the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, and the General Data Protection Regulation (GDPR) of the European Union.

In order to pursue this study, we will talk about the numerous laws and regulations that the aforementioned nations impose and how we may incorporate them in our own nation in order to remove any possible drawbacks to our DPDP Bill.

IV. TRANSFER OF PERSONAL DATA

Transfer of personal data outside of India is one of the main problems with the DPDP law. The bill didn't specify the terms and conditions, and what countries will be

approved and based on what factor is still unclear. Section 17[3] of the bill states that "The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified."

Now, we will see how other countries has dealt with this issue.

A. GDPR (General Data Protection Regulation, 2016)

Article 44[4], which discusses the general principle of transfers, states that any transfer of personal data that is being processed or that is intended to be processed after transfer to a third country or to an international organisation shall only take place if the controller and processor, subject to the other provisions of this Regulation, comply with the conditions set forth in this Chapter, including for onward transfers of personal data from the third country.

Personal data cannot be transferred outside of the EEA (European Economic Area), which consists of all EU member states as well as Iceland, Liechtenstein, and Norway.[5]

There is certain condition where you can transfer the personal data outside EEA which are:

1. **Transfer on the basis of an adequacy decision –** The Commission may authorise the transfer of personal data to a third country, a territory, or one or more specific sectors within a third country, or to an international organisation, if it has determined that the third country, territory, or international organisation in question ensures an adequate level of protection. This transfer won't need any special authorization.

[3] Digital Privacy and Data Protection Bill 2022, s 17.
[4] General Data Protection Regulation (EU) 2016/679, art 44.
[5] European Commission, 'Data Protection' <https://ec.europa.eu/info/law/law-topic/data-protection_en> accessed 11 March 2023.

2. **Transfer subject to appropriate -** In the absence of a decision made in accordance with Article 45(3), a controller or processor may only transfer personal data to a third country or an international organisation if they have put in place the necessary safeguards and are confident that the data subjects will have access to enforceable legal rights and remedies.[6]

3. **Derogation for specific situation -** In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

    a) The data subject has explicitly consented to the proposed transfer

    b) The performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

    c) The important reasons of public interest.[7]

B. PIPL (Personal Information Protection Law, 2021)

The PIPL specifies a number of conditions for the cross-border transfer of personal data.

First, cross-border transfer of personal information should be sufficient to meet the need for the personal information processor to provide personal information beyond the People's Republic of China due to commercial or other obligations. Personal data won't be allowed to be sent outside in any other case.[8]

[6] International Association of Privacy Professionals, 'GDPR Compliance Checklist' (IAPP, n.d.) <https://iapp.org/resources/article/gdpr-compliance-checklist/> accessed 11 March 2023.
[7] Information Commissioner's Office, 'International transfers' (ICO)< https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ >accessed 11 March 2023.
[8] National People's Congress of China, 'Personal Information Protection Law' (19 August 2021) https://www.npc.gov.cn/npc/c30834/202108/df4d4c3db3e247f0841adfc2fa4b8f1b.shtml accessed 11 March 2023.

If the personal information processor really needs to provide the personal information abroad, it must meet any of the following conditions:

1. Pass the security assessment organized by the Cyberspace Administration of China ("CAC");
2. Certified by a specialized agency for protection of personal information in accordance with the provisions of CAC; and
3. Adopt CAC's standard contract into its contract with the overseas recipient, specifying the rights and obligations of both parties.[9]

Before transmitting personal information abroad, the data processor must get the subject's separate permission and tell the subject of the recipient's information (such as the recipient's name, contact information, the purpose of the processing, etc.).[10]

Critical Information Infrastructure Operators ("CIIO") and processors who handle personal information up to a particular threshold are subject to the PIPL's data localization mandate. In general, the personal data gathered must be maintained in China; if it has to be transmitted outside of China, a security assessment conducted by CAC must be passed.[11]

C. CPRA (California Privacy Rights Act, 2022) as an extension of CCPA (California Consumer Privacy Act, 2020)

Localization and cross-border data transfers are not specifically addressed under the CCPA's standards. However, the idea of selling encompasses giving away data to other parties.

[9] International Association of Privacy Professionals, 'China Releases New Personal Information Protection Law' (IAPP, 20 August 2021) < https://iapp.org/resources/article/china-releases-new-personal-information-protection-law/ >accessed 11 March 2023.
[10] Asia-Pacific Economic Cooperation, 'Cross-Border Data Transfers in the Asia-Pacific: A Guide for Businesses' (APEC, May 2021) < https://www.apec.org/Publications/2021/05/Cross-Border-Data-Transfers-in-the-Asia-Pacific-A-Guide-for-Businesses >accessed 11 March 2023.
[11] David Cheng and Qiao Liu, 'Data Localization Requirements under China's New Personal Information Protection Law' (2021) DLA Piper Data Protection Laws <https://www.dlapiperdataprotection.com/index.html?t=law&c=CN&kw=data-localization-requirements-under-chinas-new-personal-information-protection-law&p= >accessed 11 March 2023.

Additionally, in line with their rights to information, access, and objection, consumers have the choice not to have their data shared with other parties. Businesses are permitted to pay consumers in return for their personal information, but they are required to disclose these payments and be transparent about this practise in accordance with section 1798.140(t)(1) of the CCPA.[12]

A company is not permitted to sell customer information under the CCPA (1798.140(t)(2))[13] if:

1. The client uses or gives the business instructions to knowingly disclose personal information or interact with a third party, provided that the third party does not sell the personal information themselves or that the disclosure does not go against the terms of the CCPA.
2. The business uses or discloses an identifier for a client who has elected not to have their personal information sold with the intention of informing third parties.
3. The business transfers the consumer's personal information to the third party as an asset in the event of a merger, acquisition, bankruptcy, or other transaction in which a third-party gains control of all or a portion of the business, provided that the data is used or disclosed in accordance with the CCPA. In the event that a third party substantially departs from the commitments made at the time of collection and changes how it uses or discloses a customer's personal information, it is expected to provide the customer early notice of the new or changed conduct.

D. PIPEDA (Personal Information Protection and Electronic Documents Act, 2000)

[12] Michaela Ross, "How Businesses Can Comply with the California Privacy Rights Act,"(Bloomberg Law, January 13, 2021) <https://news.bloomberglaw.com/us-law-week/how-businesses-can-comply-with-the-california-privacy-rights-act.> accessed March 10, 2023.
[13] California Privacy Rights Act, 2022, s 1798.140(t)(2).

It is expressly acknowledged in paragraph 3 of Schedule 1[14] of the PIPEDA that personal data may be sent to third parties for processing.

The PIPEDA does not prohibit organisations based in Canada from transmitting personal data to a processor in another nation. In contrast, corporations are in charge of ensuring the security of any personal information provided as part of a particular outsourcing contract under the PIPEDA. The PIPEDA does set out criteria for processing transfers, but the OPC may investigate complaints and review how corporations handle personal information.

Organisations are expected to protect the personal data stored by processors and the transferring organisation is accountable for the data that has been provided to the receiving organisation. The primary instrument for doing this is a contract.

Organisations must also be transparent and truthful about how they manage personal data. Customers must be made aware that their personal data could be processed in another nation or area and might there be accessible by judicial, law enforcement, and national security organisations.[15]

V. SPECIAL CATEGORY IN PERSONAL DATA

Sensitive personal data, confidential data, commercial data, and many other sorts of special categories of personal data are not discussed in the DPDP law. However, in this study, we are focused on sensitive personal data since it is a category of data that requires more security than the others.[16]

Sensitive personal information is protected by law and includes biometrics, financial information, information on a person's sexual orientation and political affiliations, among other categories of personal information.

[14] Personal Information Protection and Electronic Documents Act, 2000 (Canada), Sch 1, Principle 4.1.3.
[15] Justice Laws Website, 'Personal Information Protection and Electronic Documents Act, 2000 (Canada),'< https://laws-lois.justice.gc.ca/eng/acts/P-8.6/> accessed March 10, 2023.
[16] Rosemary Jay, Data Protection Law and Practice (Bloomsbury Professional, 2021).

Data that may be used to commit crimes like identity theft, such as government-issued IDs, may be sensitive. Other information is sensitive because there is a higher risk of damage from its acquisition and its abuse. Nazi Germany, for instance, exploited databases of religious, ethnic, and other information to carry out genocide and other war crimes during World War II. Individuals have also been discriminated against, denied benefits, and excluded from neighbourhoods and academic institutions based on their race, ethnicity, religion, and sexual orientation.[17]

A. GDPR (General Data Protection Regulation, 2016)

Sensitive personal data is included in the categories of personal data established by the GDPR.

According to Article 9[18] processing of special categories of personal data, "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation shall be prohibited."

There is exception where Article 9 will not be applicable which are:

1. data subject has given explicit consent.
2. the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
3. protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
4. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

[17] Stewart Dresner, Data Protection and Privacy: The International Framework (Bloomsbury Professional, 2020).
[18] General Data Protection Regulation, Regulation (EU) 2016/679, art 9.

5. processing relates to personal data which are manifestly made public by the data subject.
6. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.
7. There is other more exception to this but we are not including in this paper.[19]

B. PIPL (Personal Information Protection Law, 2021)

The PIPL imposes tougher rules on data processors in order to safeguard sensitive personal data.

Article 28[20] defines sensitive personal information as "personal information that, once leaked or used illegally, may easily cause grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors unrelated to the data subject."

Only when it is absolutely essential, with strict protections in place to prevent misuse or exploitation, may a personal information processor handle sensitive personal information.

Furthermore, each individual must separately agree to the processing of their sensitive personal information. Such criteria take priority when laws and administrative procedures need express authorisation for the processing of sensitive personal information. Before processing the personal information of a minor under the age of 14, the personal information processor must get the consent of the child's parents or other guardians.

[19] European Data Protection Board, 'Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679' (EDPB, 4 June 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2019_codesofconductmonitoringbodies_en.pdf > accessed 11 March 2023, [86]-[90].
[20] Personal Information Protection Law, 2021 article 28.

In addition, unless the PIPL exempts the personal information processor from doing so, the personal information processor must notify the individual of the necessity of processing sensitive personal information as well as the impact on their personal rights and interests, in addition to the usual notification requirements.[21]

C. CPRA (California Privacy Rights Act) as an extension of CCPA (California Consumer Privacy Act)

Section 1798.135 of the CPRA[22] provides a thorough description of the measures your business may take to limit the sale, transfer, and use of personal and sensitive personal information.

It establishes the new classification of sensitive personal information (SPI), which is subject to stricter regulation than personal information (PI). The CCPA established what constitutes personal information. The CPRA broadens the definition of that word with the inclusion of the subcategory of sensitive personal information, which includes government-issued identification, finances, race, religion, and union membership, as well as geolocation, communication, genetics, biometrics, health, and sexual orientation. Companies that collect, keep, process, disclose, and transfer personal data about their customers need to provide a higher level of security for all information in this category.[23]

Where there is right there is obligation so, here comes certain obligations that comes with it:

1. Disclosing to the consumer at or before the point of collection
2. Disclose to the consumer in its privacy notice.

[21] Bloomberg Law, 'China Personal Information Protection Law (PIPL) FAQs' (Bloomberg Law) <https://pro.bloomberglaw.com/brief/china-personal-information-protection-law-pipl-faqs/ > accessed march 10 2023.
[22] Official California Legislative Information (2018) Assembly Bill No. 375.
[23] What's the Difference Between CCPA & CPRA | Bloomberg Law. (n.d.). Bloomberg Law < https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/> accessed march 10 2023.

3. to safeguard sensitive personal information against unauthorised or unlawful access, destruction, use, modification, or disclosure under the CPRA, suitable security policies and practises must be implemented.
4. Make requests for access, erasure, or correction of sensitive personal information accessible to consumers via two or more designated channels and respond to such requests within 45 days.
5. obtaining the consumer's permission, the first time at least a year later before asking them again to approve the sale, sharing, or use of their sensitive personal information for new reasons.

D. PIPEDA (Personal Information Protection and Electronic Documents Act, 2000)

Sensitive personal data is described in Principle 4.7 of PIPEDA[24] as follows: Personal information should be secured by security protections proportionate to the information's sensitivity.

Any personal information under the PIPEDA may be deemed sensitive depending on the circumstances, however some categories of personal information are often regarded as sensitive owing to the particular risks they pose to the individuals involved in its collection, use, or disclosure.

Health and financial information, ethnic and racial origins, political beliefs, genetic and biometric information, and an individual's sexual orientation are the types of information that are often viewed as sensitive and need a higher degree of protection. Companies are required under PIPEDA to use security measures that are commensurate with the sensitivity of the data they are securing.[25]

The OPC creates interpretation bulletins in an attempt to summarise the broad concepts that have resulted from court decisions and the Commissioner's

[24] Personal Information Protection and Electronic Documents Act, 2000 (Can), Schedule 1, Principle 4.7.
[25] Office of the Privacy Commissioner of Canada, 'The Personal Information Protection and Electronic Documents Act (PIPEDA),'< https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ > accessed March 10, 2023.

judgements on particular instances. These interpretations are not binding legal interpretations; rather, they are intended to be used as a reference for PIPEDA compliance. As the Commissioner issues further findings and the courts issue additional judgements, these Interpretations may change and become more refined.[26]

VI. EXEMPTION

The DPDP bill's section 18(2), which states that The Central Government may, by notice, exclude the processing of personal data from the application of this Act's requirements, addresses this problem as well as other key ones.

1. the preservation of public order, the prevention of incitement to any cognizable crime related to any of these, the security of the State, the sovereignty and integrity of India, cordial relations with other States, and the maintenance of the State.
2. if the personal data is not to be used to make decisions that are specifically related to a Data Principal and the processing is done in compliance with the requirements outlined by the Board, then it is necessary for research, archiving, or statistical reasons.[27]

According to Section 2(18)(d)[28], if public order is maintained, the provisions of this Act will not apply. However, it is still unclear what constitutes maintaining public order. This gives the government authority to make decisions.

A. GDPR (General Data Protection Regulation, 2016)

There is an exemption for processing in the public interest, but again, what is covered will depend on the government. GDPR Article 89[29] states that "Processing for archiving in the public interest, scientific or historical research

[26] Canadian Bar Association, 'Privacy law and the Personal Information Protection and Electronic Documents Act (PIPEDA),'<https://www.cba.org/Publications-Resources/CBA-Practice-Link/Privacy-law-and-the-Personal-Information-Protection-and-Electronic-Documents-Act-(PIPEDA)> accessed March 10, 2023.
[27] Livemint, 'Data Protection Bill exempts processing of personal data for security of state'<https://www.livemint.com/industry/telecom/data-protection-bill-exempts-processing-of-personal-data-for-security-of-state-11640005727453.html >accessed March 11, 2023.
[28] The Digital Privacy and Data Protection Bill, 2022, s 2(18)(d).
[29] General Data Protection Regulation, art 89.

purposes, or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject."

B. PIPL (Personal Information Protection Law, 2021)

Article 34[30] of the Personal Information Protection and Electronic Documents Act (PIPL) states that state agencies handling personal data "shall conduct them in accordance with the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfil their statutory duties and responsibilities."

The article already makes clear that government entities may handle personal data in accordance with the authority granted to them by law or administrative rule, ensuring that the entity in question will not abuse the data.

C. CPRA (California Privacy Rights Act) as an extension of CCPA (California Consumer Privacy Act)

The exceptions to the legislation are specifically listed in Code Section 1798.145. The California Consumer Privacy Act's (CCPA's) exclusions are consistent with those of the CPRA. Both the laws' obligations and their exemptions work best together.[31]

The CPRA does not apply when observing its requirements interferes with conducting an investigation or upholding other federal, state, or local laws. Where the CPRA would impede legal proceedings, it does not apply.[32]

If a consumer's life or health is in danger, you must accede to a government agency's request for immediate access to their personal information, therefore the CPRA is not applicable. Any such request must fully adhere to the standards listed below:

[30] Personal Information Protection Law, art 34.
[31] International Association of Privacy Professionals, California Privacy Rights Act (CPRA), <https://iapp.org/resources/article/california-privacy-rights-act-cpra/> accessed march 11,2023.
[32] Official California Legislative Information, 'California Civil Code - Section 1798.100-1798.199.98: California Consumer Privacy Act of 2018', (2018).

1. Given the agency's good faith belief that it has a legal basis for accessing the information on a non-emergency basis.
2. Approved by a senior agency officer.
3. The agency consents to get an appropriate order from a court within three days and, in the event such request is denied, to delete the material[33].

D. PIPEDA (Personal Information Protection and Electronic Documents Act, 2000)

If the collection, use, or disclosure of personal information takes place within a province that has legislation that has been deemed substantially similar to the PIPEDA, the Governor in Council may, in accordance with paragraph 26(2)(b)[34], exempt an organisation or class of organisations, an activity or a class of activities from the PIPEDA.[35]

The Governor in Council may exempt an organisation or a class of organisations, an activity or a class of activities from the PIPEDA if the collection, use, or disclosure of personal information occurs in a province with legislation that has been determined to be substantially similar to the PIPEDA. Therefore, wherever it is relevant, the provincial law that is essentially equivalent to the federal law shall prevail.[36]

VII. DATA SUBJECT RIGHTS

The data subject rights that are given to people in India are one of the most significant features of the DPDP. These rights are intended to offer people greater control over their personal information and to guarantee that their privacy is respected. Because

[33] California Attorney General, 'CCPA/CPRA Fact Sheet', (2021).
[34] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, s. 26(2)(b).
[35] Office of the Privacy Commissioner of Canada, 'PIPEDA FAQs: Exemptions' (3 July 2019) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-frequently-asked-questions/pipeda_faqs_110703/ >accessed 10 March 2023.
[36] Lindsay Scott, 'Privacy Law: Exemptions to PIPEDA' (Canadian Bar Association, 6 July 2014) <https://www.cbapd.org/details_en.aspx?id=NA_ON_14PBC0706B >accessed 10 March 2023.

personal information is often gathered and used by businesses without the individual's knowledge or permission, this right is especially crucial.[37]

The DPDP provides several rights to data subjects, including:

1. **Right to information about personal data –** One of the essential rights granted to Data Principals under the DPDP is the right to knowledge about personal data. Data subjects have a right to know how their personal data is collected, used, and disclosed.

   It enables people to comprehend what information is being gathered, how it is being utilised, and with whom it is being shared. This knowledge is crucial because it enables people to decide if they are okay with their data being used in certain ways.[38]

2. **Right to correction and erasure of personal data –** Data principals have the right to rectification when data is inaccurate or to update the data. The section also discusses the right to erasure, which allows you to request the deletion of data when it is no longer required for the intended purpose. The data fiduciary is obligated to take prompt action to address rectification requests and make any necessary corrections to the data.[39]

3. **Right of grievance redressal –** The Data Principal have right to register a grievance with a data fiduciary and if data principal is not satisfied with response, they may register a complaint with Board.[40]

4. **Right to nominate –** In the case of the principal's death or incapacity, the data principal has the option to choose a replacement.[41]

A. GDPR (General Personal Data Protection, 2016)

We will now go into greater detail about the rights of data subjects under the GDPR, including the rights to information, access, rectification, erasure,

[37] Information Commissioner's Office (ICO) - Your Data Rights: Information Commissioner's Office, 'Your Data Rights' (last updated 19 January 2022) < https://ico.org.uk/your-data-matters/ >accessed 11 March 2023.
[38] Digital Privacy and Data Protection bill, s 12.
[39] Digital Privacy and Data Protection bill, s 13.
[40] Digital Privacy and Data Protection bill, s 14.
[41] Digital Privacy and Data Protection bill, s 15.

restriction of processing, data portability, objection, and not to be the subject of automated decision-making.[42]

1. **Right to Informed -** Under this right, data controllers must notify people in a clear and straightforward manner about the personal data that is being gathered, used, and stored. Data controllers must make it clear to persons what information is being collected and why it is being gathered, and they must do so in a transparent way. The data subject must be able to quickly access this information, which must be presented in a clear and straightforward way.[43]

2. **Right to Access -** People have the right to ask for and receive information about how data controllers are using their personal information. The data controller must demonstrate that the information being given is accurate and current, and it must be done so promptly.

   Data subjects have a right to information about the categories of personal data that are processed, the processing's goals, and the recipients of the data who may receive them. Additionally, people have the right to a free copy of their personal data in a format that is simple for them to comprehend.[44]

3. **Right to Rectification -**If a person's personal information is incomplete or erroneous, they have the right to request that it be rectified. This right is crucial because it enables people to confirm that their personal information is correct and up to date.

   Data controllers must respond to requests for rectification and make any required updates to the data without delay. If the data controller is unable to

[42] European Commission, 'Data protection - rights of data subjects' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_en>accessed 11 March 2023.
[43] UK Government, 'Guide to the General Data Protection Regulation (GDPR)' <https://www.gov.uk/guidance/general-data-protection-regulation-gdpr>accessed 11 March 2023.
[44] GDPR, art 15, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

rectify the data, the data subject has the right to request that the data be deleted or that its processing be restricted.[45]

4. **Right to Erasure -** Also referred to as the "right to be forgotten," this right allows anyone to ask that their personal data be removed. Because it gives people choice over how their personal data is used and preserved, this right is crucial.

   Whenever possible, data controllers shall take measures to delete personal information if it is no longer required for the purposes for which it was obtained or if the data subject withdraws consent.[46]

B. PIPL (Personal Information Protection Law, 2021)

The protection of data subjects' rights, which include the ability to access, rectify, and erase personal information, is one of the law's most important clauses.

1. **Right to Informed -** Data subjects have the right to access their personal information, including the right to know what information is being gathered and processed about them as well as how it will be used. Upon request, organisations must provide people a copy of their personal information together with an overview of the reason(s), type(s), and method(s) for processing their data.[47]

2. **Right to Privacy -** The right to privacy applies to data subjects. Organisations are thus required to protect people's privacy and refrain from gathering, storing, using, transferring, or disclosing personal information for reasons that are incompatible with the rights of the individual to privacy. Additionally, organisations are required to take reasonable measures to limit the acquisition,

[45] GDPR, art 16, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[46] GDPR, art 17, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[47] Personal Information Protection Law (PIPL), art 12 (promulgated by the Standing Committee of the National People's Congress on 20 August 2021, effective from 1 November 2021).

storage, and use of personal data that is not required for the initial purpose of collection.

3. **Right to objection to the collection -** In addition to these rights, data subjects also have the option to object to the gathering, storing, using, and transfer of their personal data. As a result, people have the choice whether or not their personal information is utilised for specific reasons, such direct marketing. Organisations are required to provide data subjects with information about their right to object and must respect their choice to do so.

C. CPRA (California Privacy Rights Act) as an extension of CCPA (California Consumer Privacy Act)

In accordance with CPRA, individuals have the right to access their personal information, including to request a copy and seek further information about how the data controller is managing it. rights of access and disclosure that are basically equivalent. The CCPA's right is only applicable to written disclosures of the information. The following rights set the CPRA apart from the DPDP:

1. **The Right to Correct and Delete Inaccurate Personal Information -** Under the CPRA, customers have the right to update and delete inaccurate personal information. Additionally, in response to verified consumer requests, covered organisations must notify customers of this right and take reasonable steps to fix or delete mistakes.[48]

2. **Storage Limitation and Data Minimization -** This law specifies data minimization and storage limitation. Similar to the General Data Protection Regulation (GDPR) of the European Union, the CPRA requires organisations to only collect personal information when it is "reasonably reasonable" for the purpose for which it is gathered or when it is "essential."[49]

[48] California Privacy Rights Act 2020, s 1798.105.
[49] California Privacy Rights Act 2020, s 1798.100.

Companies are also prohibited from keeping customer information for any longer than is necessary to fulfil the objectives for which it was collected.

3. **Consumers have a right to data portability -** Customers have the right to data portability, which allows them to ask for the transfer of part of the collected personal information to another company. According to CPRA, the data must be presented in a form that is both easy to understand and machine-readable.[50]

D. PIPEDA (Personal Information Protection and Electronic Documents Act, 2000)

Before collecting, using, or disclosing users' personal information, companies in Canada are required under the PIPEDA to get their permission. The goal of this legislation is to protect internet users' right to privacy. In addition, the 10 fair information principles provide a view of the data subject. Among them are:

1. **Penalties -** The DPDP fines are now infamous: businesses found to be breaking its core principles can be fined up to $2.5 Billion for failing to take adequate precautions against data breaches; $2 Billion for failing to report a breach or comply with provisions related to children; $0.1 Billion for breaking data localization norms; PIPEDA's fines are significantly less severe in comparison. They can only go up to $100,000 (roughly $76,000) in three specific situations: if businesses retaliate against employees who reported wrongdoing, if an organisation fails to keep personal data under request for as long as necessary to allow the subject to exhaust any available remedies, or if someone prevents the federal privacy commissioner from conducting an investigation into a complaint or an audit.[51]
2. **Accessibility-** PIPEDA, there are specific instances in which a company may not be able to provide access to all the personal data it has on hand

[50] California Privacy Rights Act 2020, s 1798.126.
[51] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 28.

about a person, such as when such data pertains to other persons or would, for instance, violate solicitor/client privilege.

An entity must respond to an individual's access request as soon as reasonably possible, but under no circumstances more than 30 days after receiving it, unless this limit is extended.[52]

3. **Additional Remedies-** In addition to any other remedies, the Federal Court may order a firm to alter its practises, publish a notice of any steps it has taken or intends to take to alter its practises, and award damages.[53]

VIII. CONCLUSION

By providing more comprehensive privacy safeguards, more effective enforcement tools, and enhanced openness and responsibility for organisations managing personal data, PIPEDA, GDPR, and PIPA all address some of the potential flaws in the DPDP bill. For instance, the GDPR gives people more control over their personal data by granting them the right to view, rectify, and transfer their data. PIPA gives people the power to sue companies that violate their privacy obligations by establishing clear privacy criteria for organisations, including data security and retention rules. The DPDP law, PIPEDA, GDPR, and PIPA all have various jurisdictional scopes and could not be relevant in all circumstances, it is crucial to keep in mind. When assessing their possible influence on privacy and data protection, it is vital to thoroughly evaluate each legislation since the exact terms and requirements of each one may differ.

The DPDP law, PIPEDA, GDPR, and PIPA together constitute a complete framework for defending people's privacy rights with regard to their personal data. While each legislation has its own criteria and safeguards, they all contribute significantly to protecting the security and privacy of personal information in the digital era.

IX. SUGGESTION

[52] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 7.
[53] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 14.

Following are some recommendations in a DPDP bill based on other jurisdictions' laws:

To strengthen the requirements for privacy-by-design and privacy-by-default, including mandatory privacy impact assessments so that one who is unaware of his or her right may also avail of this and the use of privacy-enhancing technologies to reduce the potential human error, the GDPR's data protection by design and default principle mandates that the data protection issues must be included into all aspects of controllers' and processors' processing operations.

Data protection authorities are "independent public authorities that monitor, through investigative and corrective powers, the application of the data protection law," according to the EU's GDPR. They address complaints about infringements of the General Data Protection Regulation and other national legislation and provide professional advice on data protection matters. It essentially increases the ability of data protection authorities to enforce the law and provide just punishments for non-compliance.

transmitting personal data over international borders, i.e., to a different country or jurisdiction. In order to secure personal data and guarantee that it is sent in compliance with international privacy rules, it incorporates procedures for cross-border data transfers. Strong legislation addressing this might significantly impact the localization of data. This provision benefits both established businesses and new startups whose private data is kept outside of India.

The next item on the list is transparency, which may be utilised to guarantee that no one's personal information is obtained or used without that person's agreement. Additionally, the legislation includes provisions requiring companies to use adequate security measures to prevent unauthorised access to or disclosure of personal data. The DPDP law should mandate that businesses disclose all of their data processing operations, including how they gather, utilise, and share individual customer data.

The DPDP bill should create an independent privacy regulator with the authority to enforce privacy laws, investigate complaints, and impose penalties on organisations

that violate privacy rights because the above-mentioned provision is useless if the end controller is either the government or private entities.

In addition to all of this, there should be severe sanctions to guarantee that businesses abide with the law's requirements.

We must create rules that are compatible with other international laws in order to maintain a fair playing field in the global economy, keeping in mind the idea that the world is a global village.