PRIVACY BEHIND THE SCREENS: A COMPARATIVE ANALYSIS OF DATA PROTECTION FRAMEWORKS IN THE EU, CANADA, AND INDIA

Apoorv Dubey, B. Com LL.B. (Hons.), Institute of Law, Nirma University, Ahmedabad

Teja Mendikar, LL.B., Pendekanti Law College, Hyderabad

ABSTRACT

Ever since the onset of the 21st century, the Industrial Revolution has very quickly metamorphosed itself into what is now known as the "Digital Revolution" or the "Digital Age" where technology is constantly widening its abilities all while bringing the global population together, transcending the physical political boundaries. As modes of socialization and globalization become increasingly simpler, at the same time the intricacies of privacy and data protection keep getting more complex, especially in the absence of robust legislative frameworks that can keep up with the fast pace of this technological era. As the internet evolves into a form of cosmopolitan neo-society, there emerge many pressing issues like breach of privacy online, digital data theft, and many other forms of cybercrimes, therefore, this paper aims to address the same by evaluating the current legislation concerned with digital data protection in the European Union, Canada, and India respectively. This paper aims to shed light on the Rights available under the EU's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and India's recently enacted Digital Personal Data Protection Act (DPDPA), 2023 w.r.t the Draft Digital Personal Data Protection Rules, 2025.

Keywords: Privacy, Data Protection, Internet Laws, Globalization, Cybercrimes

INTRODUCTION

"Personal data is the new oil of the Internet and the new currency of the digital world."[1]

– Meglena Kuneva

As the number of internet users exceeds five billion globally[2] with over 900 million users in India[3] alone, it is clear from the statistics that the majority of the population both internationally and nationally are prone to be victims to a myriad of cybercrimes ranging from breach of privacy, leak of personal data, phishing attacks and to even theft of identity, 'netizens' or the citizens on the internet are often at a loss as to what to do because the perpetrators of these crimes are anonymous and the absence of robust mechanisms to report them make this all even more tedious than it needs to be. Even when there are remedies available under respective country's laws, they are yet to catch up to the pace of the criminals online who are always concocting newer methods each day to catch their preys without being visible.

With personal data being sold on the dark web[4], that too in mass amounts, potential attackers have wide range of resources to target from, transforming data leaks into a lucrative business with no strong legal frameworks to counter them. Ever since the Covid-19 Pandemic, a greater number of people have been joining the digital space, and it is imperative that we make online spaces safe where netizens don't have to worry about being 'digitally mugged' by adversaries whom they can't even see.

Having legal frameworks/legislations with easy to understand and simple mechanisms to seek recourses will save both people and the countries from heavy financial losses and it is also very important that such laws are embedded with big penalties that will serve as an impediment to cybercriminals, therefore preventing further losses.

---

[1] Kuneva, M. (2009) *Meglena Kuneva- European consumer commissioner - keynote speech - roundtable on online data collection, targeting and profiling*, *European Commission - European Commission*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (Accessed: 21 January 2025).
[2] Digital Around the World — DataReportal – Global Digital Insights, (July 7, 2022), https://datareportal.com/global-digital-overview.
[3] Times Of India, India now has 936.16 million internet subscribers: TRAI, - Times of India (Apr. 23, 2024), https://timesofindia.indiatimes.com/technology/tech-news/india-now-has-936-16-million-internet-subscribers trai/articleshow/109537789.cms.
[4] https://www.business-standard.com/companies/news/personal-information-of-750-mn-indians-up-for-sale-on-dark web-cloudsek-124012500973_1.html.

LEGISLATION IN THE EUROPEAN UNION

The European Union which comprises of 27 countries of Europe has one of the world's best legal framework concerned with privacy and data protection. Important judicial pronouncements from the European Court of Justice like *Google Spain v AEPD and Mario Costeja González*[5] (w.r.t Right to be Forgotten) continue to uphold the principles of reasonable expectation of privacy and data protection.

In the EU, privacy and data protection comes under the purview of the General Data Protection Regulation (GDPR) which was adopted by the EU Parliament and Council in 2016 and implemented from May 25, 2018.

Data Controller: bears the legal responsibility of compliance, makes decisions on data collection methods, objectives and sets purposes on how to use the collected data.

Data Processor: processes the personal data according to the instructions of the Data Controller.

Rights[6] mentioned under chapter 3 of the General Data Protection Regulation (GDPR), 2018:

1. **Right to be Informed:** the data subjects i.e., individuals whose data is being collected have the right to be informed about what and why their personal information is being collected, they also have the right to be informed about how and where their data will be processed or stored.

2. **Right to Access and Rectification**: the data subjects can request access to their personal data being stored by the data collecting agencies/organizations, they can further request their personal information to be corrected if any discrepancies are found.

3. **Right to Erasure**: popularly known as 'Right to be Forgotten', a data subject can request the organization to have their personal data permanently deleted, even from

[5] Google Spain v. AEPD and Mario Costeja González, (European Ct. Justice 2014).
[6] *Chapter 3 – Rights of the data subject*, General Data Protection Regulation (GDPR) https://gdpr-info.eu/chapter-3/

third parties to which the data may have been shared.

4. **Right to Restrict Processing**: if any individual feels like their data is inaccurate or for any other reason, they can ask the data controllers/organizations to stop processing their personal data.

5. **Data Portability**: a data subject can request an organization to directly transfer their personal data to a third party.

6. **Right to Object:** if the data subject believes that their data is being used for direct marketing, they can object to such use of their personal data.

7. **Automated Decision Making**: individuals have the right to opt out of such processes which involve automated decision making i.e., by machines etc.

Responsibilities[7] of Data Controllers:

- Must notify the data subject within 72 hours of any data breach.

- Must obtain valid express consent, and should use the collected data only for the purposes for which they collected it.

- Companies handling large volumes of data must appoint a Data Protection Officer (DPO) who oversees the governance of collected personal data.

Penalties[8]:

- Less severe violations: 10 million Euros, or up to 2% of the offending company's global turnover of the previous financial year.

- Severe violations: 20 million Euros, or up to 4% of the offending company's global turnover of the previous financial year.

[7] Rich Castagna, *General Data Protection Regulation (GDPR)*, Definition from TechTarget (Jan. 29, 2021), https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR.
[8] General Data Protection Regulation (GDPR) https://gdpr-info.eu/issues/fines-penalties/

Enforcement/Redressal:

Each country under the EU has its own Data Protection Authority (DPA) that enforce the GDPR[9]. Individuals whose rights have been infringed can lodge complaints with the respective Data Protection Agency of their country that can investigate, and enforce compliance/impose fines. In case of any cross-border issues, the European Data Protection Board resolves it.

LEGISLATION IN CANADA

Canada is the only country in North America to have specific legislation that addresses digital data protection, where various Judicial precedents have time and time upheld the principles of data protection and privacy in cases like *Jones v. Tsige*[10] and in the landmark case of *R v Spencer*[11] the Supreme Court of Canada held that people have a 'reasonable expectation of privacy' online.

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

- **Personal information**[12]: refers to any information that is identifiable whether it's through Govt issued IDs or Medical records.

Consumer Rights[13] **available under the PIPEDA, 2000:**

1. **Right to Access and Rectification:** users have the right to ask access to their personal information which is being held by the organization and whenever it is asked, the organization must provide access within a reasonable period of time. And, if users find any factual discrepancies of their personal information, then they have the right to have it corrected.

2. **Right to be informed:** the users have the right to know why, how, and what personal information is being collected by the organizations. The data collecting agencies must

[9] *Data Protection Authority & you*, European Data Protection Board https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en.
[10] Jones v. Tsige, 2012 ONCA 32 (CanLII)
[11] Matthew David Spencer v. Her Majesty The Queen, 2 SCR 212 (Supreme Ct. Canada 2014).
[12] Personal information protection and electronic documents act § 2(1) (2000).
[13] PIPEDA: Canada's Privacy And Data Protection Law, (May 26, 2024), https://usercentrics.com/knowledge hub/canada-personal-information-protection-and-electronic-documents-act-pipeda/

provide clear and specific information to the users as to their purposes of collecting personal data.

3. **Right to safeguards:** the individuals have the right to expect the data collecting agencies to have ample security measures to safeguard their personal data, they also have the right to be informed about what specific actions are being taken and by whom for the same.

4. **Right to Responsible Use:** whoever or whichever organization is collecting the personal data, are supposed to use it for the specific purposes for which they collected it, they aren't allowed to make use of such data for anything else.

5. **Right to complain:** *ubi jus ibi remedium* i.e., where there is a right there is a remedy and here too the individuals have the right to complain whenever their rights are infringed upon by any organization that collected their personal data.

Under the PIPEDA, 2000 the organizations which collect personal data are required to follow the below mentioned principles[14]:

- **Accountability**: the data collecting organizations are wholly responsible for the data they collect and they must appoint an officer that ensures their compliance with the regulations.

- **Purposes**: organizations are required to give complete information as to why they are collecting personal data, and they should do so before taking any information.

- **Consent**: after stating their purposes, the data collecting agencies must obtain informed consent from individuals to collect, use, and share their personal data.

- **Limitation**: all entities under the purview of PIPEDA, are expected to limit their collection of personal data to the extent they require. They are also required to dispose of any information after its collection purposes have been met.

[14] *PIPEDA fair information principles*, Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

- **Accuracy and safeguards**: whatever personal data is being collected, it should be factually correct and if any discrepancy has been brought to their notice, they are required to correct it. Organizations should also employ meaningful and sufficient security measures to safeguard the data.

Penalties and investigation: the Office of the Privacy Commissioner of Canada (OPC) has the power to investigate noncompliance and they can refer matters to the Federal Court which can then impose penalties upon the offending organizations. The data collecting agencies can be fined to the tune of $10,000 CAD for smaller violations and $100,000 CAD[15] for each severe violation of the PIPEDA, 2000.

Complaint/redressal mechanism: individuals can complain directly to the Office of the Privacy Commissioner (OPC) online and sometimes the OPC can initiate investigations on their own.

LEGISLATION IN INDIA

Data protection law in India was passed after a long series of verdicts and debates. The main precedent playing a pivotal role in laying foundation of legislation related to data protection in India is none other than *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)[16]. This case overruled all previous judgements which failed to consider the evolving societal and technological contexts that make privacy essential today.

This case revolved around the privacy concerns regarding the biometric and demographic data of crores of Indian citizens under the Aadhaar program. As the collection of this data was made mandatory by the government, it was argued that this violated individuals' right to privacy. The unanimous judgment was pronounced by a nine-judge bench, which introduced the tests of legitimacy, proportionality, and legality to evaluate any infringement of this right. The landmark judgment finally granted the long-awaited right to privacy to the citizens of India, recognizing it as a multifaceted fundamental right under the right to life enshrined in Article

[15] Osman Husain, *Penalties for Noncompliance With PIPEDA & How Its Enforced*, (Oct. 1, 2024), https://www.enzuzo.com/blog/pipeda-penalties-enforcement.
[16] Justice K.S. Puttaswamy (Retd) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

19[17] and Article 21[18] of the Indian Constitution.

Following this case, which established a constitutional basis for privacy, the government constituted the Justice B.N. Srikrishna Committee to draft a comprehensive data protection framework[19], which later evolved into the ***Digital Personal Data Protection Act, 2023.*** It is now India's legislation to tackle issues relating to privacy and safety of personal data.

Rights of Data Principals

1. **Right to Access**: DPDPA 2023 has granted Data Principals the right to access their personal data provided to the Data Fiduciaries.

2. **Right to Consent**: the consent obtained from Principals must be specific, free, and informed where consent taken with ambiguous conditions for data processing must be held invalid. The act has also granted Principals the freedom to withdraw consent at any time.

3. **Right to Correction**: along with access, Data Principals can request fiduciaries to correct their personal data which may be inaccurate or incomplete.

4. **Right to Erasure**: principals are granted the right to make fiduciaries clear or delete their personal data which is no longer necessary or is not needed for the purpose for which it was collected.

Responsibilities of Data Fiduciaries

- **Management of consent**: Data Fiduciaries are required to obtain clear consent from Data Principals before processing their personal data along with options to manage consent.

- **Data Protection Measures**: adequate measures of security are needed to be implemented to avoid any data breach or leak. Significant Data Fiduciaries (SDFs)

[17] INDIA CONST. art.19.
[18] INDIA CONST. art.21.
[19] Bluebook 21st ed. Anushka Rao, Pondering the Potency of Data Protection: A Comparative Review of Data Protection Framework in the European Union, the United States of America & India, 12 NIRMA U. L.J. 01 (December 2022).

must appoint a Data Protection Officer (DPO) who must serve as a contact for necessary grievance redressal process.[20]

- **Transparency**: Data Fiduciaries must disclose the purpose of data collection and practices used in processing data to the Data Principals.

- **Reporting Data Breaches**: in case of any data breach taking place, Data Fiduciaries are required to notify the principals and report the same to the Data Protection Board constituted under the act.

Redressal Mechanism

- **Filing Complaints**: Data Principals can file their complaints with the *Data Protection Board of India* in case of violation of their right by any Data Fiduciary.

- **Board Proceedings**: the Board constituted under the act will conduct proceedings on the complaint and impose penalties or order corrective actions if needed.

- **Appeal Process**: appeals against the decision of the board can be filed in the Appellate Tribunal constituted under the Telecom Regulatory Authority of India Act.

Penalties

If the board finds that a breach is significant based on the inquiry, it may impose penalty after giving an opportunity of being heard. The penalty is required to be monetary, and the amount must be decided based on nature, gravity and duration of the breach. The penalty may amount ten thousand rupees and may extend to two hundred and fifty crore rupees depending on factors of the breach. The sum realised from the imposed penalties is required to be credited to the Consolidated Fund of India.

This Data protection act, though a big step by the government, failed to describe specific operational and procedural details. In order to tackle this issue, government is planning to bring

[20] Bluebook 21st ed. Aniket Sharma, Transforming Data Privacy: An Analysis of India's Digital Personal Data Protection Act, 6 INT'l J.L. MGMT. & HUMAN. 1841 (2023).

a subordinate legislation called *Digital Personal Data Protection Rules, 2025*[21] to fill in the gaps of the parent act. A draft of these rules is put online to invite suggestions. As previously mentioned, the act mandates data fiduciaries to notify the data breach to the Data Protection Board. Subsequently, under the subordinate legislation, the conditions are specified under *rule 7*: the notification must include nature, timing, measures, extent, and potential impact of the breach and the same must be notified to the board within seventy-two hours of becoming aware of it. Likewise, *rule 8* also specifies a time limit of 48 hours for letting Data Principal to choose to retain data before erasure. Furthermore, *rule 6* specifies "reasonable security safeguards" which must be taken by the fiduciaries. The measures include encryption, access controls, and data backups to prevent breaches. *Rule 4* mandates consent managers to maintain an interoperable platform to manage consent and to retain records of consent for 7 years.

Additionally, *rule 10 & 11* mandates verifiable parental consent for children's data and provides exception to entities like educational institutions under specific conditions respectively. Notably, *rule 14* imposes restrictions and conditions on the cross-border transfer of personal data. Moreover, *rule 12, 13 & 15* specifies obligations of Significant Data Fiduciaries, rights of the Data Principals and provides exemptions for research, archiving and statistical purposes respectively.

This is how Draft Digital Personal Data Protection Rules, 2025 can effectively fill in the gaps and add up much needed procedural aspects in the Digital Personal Data Protection act 2023.

COMPARISON

India's dynamic framework, the EU's stringent regulations, and Canada's balanced approach create a diverse landscape of data protection. The table below contrasts these three regions' strategies for safeguarding personal information:

[21] *Draft Digital Personal Data Protection Rules, 2025 innovateindia.mygov.in*. Available at: https://innovateindia.mygov.in/ (Accessed: 21 January 2025).

Aspect	India(DPDPA)[22]	Europe(GDPR)[23]	Canada(PIPEDA)[24]
Relevant authorities	Data Protection Board of India (DPBI)	Data Protection Authority (DPA)	Office of the Privacy Commissioner (OPC)
Scope	Personal data processed digitally within or for India	Processing of data of EU residents, irrespective of location	Personal data collected during commercial activities
Consent	Specific, informed, unambiguous; withdrawal option	Freely given, specific, informed, explicit	Must be meaningful; includes implied consent
Data Breach Notification	Mandatory reporting to the Data Protection Board and affected individuals	Notify supervisory authority within 72 hours	Notify affected individuals if breach causes significant harm
Penalties	Fines up to ₹250 crore (approx. €30 million)	Fines up to €20 million or 4% of global turnover	Fines up to CAD 100,000 per violation
Cross Border Transfers	Restricted unless conditions are met for adequate safeguards	Allowed to countries with adequate protection levels	Requires adequate safeguards, consent, or legal necessity

CONCLUSION

Online Privacy and Digital Data Protection is not a privilege but a right that needs to be protected on par with other Fundamental Rights as cybercrimes too have real and serious

[22] Digital Personal Data Protection Act 2023
[23] European Union (2016) *Regulation (EU) 2016/679* Available at: https://eur-lex.europa.eu (Accessed: 21 January 2025).
[24] Canada (2000) *Personal Information Protection and Electronic Documents Act, SC 2000, c. 5.* Available at: https://laws-lois.justice.gc.ca (Accessed: 21 January 2025).

consequences. As much as it is appreciated, India's DPDPA, 2023 can also improve itself by: -

- Mandating States to establish their own Data Protection Boards with similar powers and responsibilities that of the National Board.

- Including right to data portability, right to compensation & right to be forgotten to effectively safeguard the privacy of Data Principals.

- Establishing a Separate Tribunal for Data Protection instead of relying on the TDSAT (Telecommunications Dispute Settlement and Appellate Tribunal) to adjudicate and to receive appeals from the Data Protection Board.

- Making Data Protection Board of India (DPBI) independent of government control and granting it suo-motu investigatory powers.

- Narrow down and clearly define exemptions for Government agencies to access citizens' personal data.

- Creating Privacy and Data Protection Awareness Cells in all Higher Education Institutes (HEI) to create and spread awareness with regard to Rights available under the DPDPA, 2023.