India's Evolving Cyberlaw Framework: A Comparative Analysis of India's DPDP Act, EU GDPR, UK Framework and Singapore's PDPA

Aditya Jitendra Choudhary[1], Dr. Swapnesh Taterh[2]
[1]*MIT Arts, Commerce and Science College, Pune, India*
[2]*Professor, MIT Arts, Commerce and Science College, Pune, India*
doi.org/10.64643/ijirt.208472-459

***Abstract*—India now runs a large part of its economic and social life through digital systems, and this has meant that huge amounts of personal data move between government bodies, businesses and online platforms every day.**

At the same time, technologies such as artificial intelligence, cloud computing, the Internet of Things, automated profiling and synthetic media are creating risks that older, narrower cyberlaw provisions were never designed to handle. India deals with these issues with the laws and rules like IT Act 2000, IT Rules 2021, DPDP Act 2023 and the DPDP Rules 2025. The main objective of my paper is to ask the question whether is this framework capable enough to keep up with the new technology or does it need new patches. The paper compares India's system with the EU GDPR, the UK and Singapore's PDPA in areas such as privacy rights, consent, data security, breach reporting, cross border data transfers, accountability and enforcement. It finds that India has created a strong legal base for the framework but its success will depend on proper implementation, capable regulators and clear guidance for new emerging technologies.

This paper will recommend a new approach to regulations one that is reviewed on regular periods and is backed up by proper implemented guidance. The research will use the results of the gap analysis between these frameworks allowing to identify strength, limitations, weakness to be identified.

A simple five-point comparative table is used to identify the differences between these frameworks. These steps can help India develop a stronger and more compatible framework which will support the growth of digital economy

***Index Terms*—India's Cyberlaw, Data Privacy, Data Protection, Cybersecurity, DPDP Act, Information Technology Act, GDPR, PDPA, Artificial Intelligence, Regulatory Gaps, Digital Governance.**

I. INTRODUCTION

Digital infrastructure is no longer a separate part of Indian life it is woven into banking, payments, e-commerce, healthcare, education, communication and public services. Even simple online transactions may involve several organisations including the service providers, payment gateway, cloud host and other third parties. As the same data that the user provides is accessible to many parties there are concerns relating to cybersecurity and data protection. India's cyberlaw framework has developed gradually over time. The starting point was the IT Act 2000, it gave legal recognition to electronic records and transactions and introduced rules for computer related offences and the liability of intermediaries [1]. The law was written for simpler internet in mind but as the new technologies keep emerging, we need to keep them updated so that they match the global standards.

As a result, the legal framework has had to expand. The Information Technology Rules 2021 added new compliance obligations for intermediaries and digital platforms [2].

Digital Personal Data Protection Act 2023

Digital Personal Data Protection Act 2023, which for the first time gave India a dedicated statute focused specifically on how digital personal data should be processed [3]. The Digital Personal Data Protection Rules 2025 followed, rolling out the Act's implementation in phases [4]. Just passing a new law every time does not solve the problems. Artificial intelligence can process data in ways that are too large-scale and too complex for traditional transparency requirements to really capture. Deepfakes can be used to impersonate real people for fraud or to damage

someone's reputation. Cloud platforms often process data across several countries at once, and IoT devices smart cameras, wearables, connected cars, home assistants can collect information continuously, often without the user being fully aware of it.

EU General Data Protection Regulation (GDPR)

The GDPR is one of the major data protection frameworks used in the European Union. This regulation applies to the organisations that deal with personal data of the people in the EU and in certain locations. The important principles that the GDPR is based on are lawfulness, transparency, purpose limitations, data security. It also gives individuals several rights over their personal data like right to access their data, correct the incorrect information, request deletion in certain cases and know how their personal data is being used [5]. An important part of GDPR is how it approaches towards cases like data breaches and international data transfers. It determines how organisations are required to take suitable security measures when a personal data breach occurs. GDPR also provides conditions on transferring data outside the EU [8]. These detailed requirements make the GDPR a useful framework for comparing the development of digital framework of India.

UK Framework

The United Kingdom has developed a framework for protecting personal data. The main laws for the framework include both EU GDPR and Data Protection Act 2018. Together these laws set how organisations should collect, use, store and share personal data. The UK Framework is based on the principles such as fairness, data transparency, data minimisation, purpose limitations, storage and security. It includes rights for individuals such as access the information, correct it and request deletion of data in certain situations. Another important part of the UK Framework is accountability. It states how organisations are expected to take responsibility for how they process personal data and put suitable security measures in it. For this study the UK Framework is useful for comparison with India's cyberlaws because it shows how detailed laws can be supported by specialised regulator and is especially useful when looking at areas like data security, breach management, accountability and international data transfers.

Singapore Personal Data Protection Act (PDPA)

Singapore's PDPA deals with the protection of personal data in Singapore. It provides rules for organisations are expected to take responsibility for how they process personal data and put suitable security measures in it. The law aims at protecting individuals and also allowing organisations to use data for legitimate business and operational purposes. One important feature of the PDPA is its focus on practical responsibilities for organisations instead of only providing general privacy principles it also states certain conditions that they need to follow while handling personal data [7]. In this study Singapore's PDPA is used as another comparison for India's data protection framework. It helps in comparing area like individual consent, data protection, breach notification, international data transfers and organisational accountability.

This paper looks at whether India's cyberlaw and data protection regime can stay adaptable as these technologies keep evolving. It does this by comparing specific elements of the Indian framework with the EU's GDPR, the UK's data protection regime, and Singapore's PDPA. The intention is not to start from the assumption that Indian law is behind the curve, but to pinpoint the particular areas where more clarity, more guidance, or stronger institutions would genuinely help.

II. LITERATURE REVIEW

Most of the India's digital law centres on the IT Act 2000 and the IT rules 2021, and this literature deals mainly with electronic transactions, computer related offences and how much responsibilities the intermediaries should carry for content on their platforms [1], [2]. This body of work is useful for understanding how India's cyberlaw began but it says very little about personal data protection as a subject in its own right, mainly because neither was written with that specific purpose in mind.

Once the DPDP Act 2023 was passed a set of Indian scholarship began examining what the Act means for individuals and organisations. C. Malhotra and U. Malhotra looked at the act from the standpoint of the ordinary user, and argue that it puts what they call the "digital citizen" at the centre of India's approach to data protection [9]. Bisht and Sreenivasulu take a narrower and more doctrinal view studying the DPDP

Act specifically as an information privacy condition and asking how far its provision actually go in protecting personal information of Indian citizens [10]. Both of these are useful contributions but each of them studies the DPDP Act largely on its own terms without placing it side by side with data protection laws from other frameworks.

On the international frameworks there is already a well-established literature around the GDPR, the UK's data protection framework and Singapore's PDPA which cover topics such as consent, breach notification duties and the conditions attached to the moving data across borders [5]-[8]. This literature is valuable as a benchmark for what a mature data protection framework can look like but its written mainly from a European, British or Singaporean perspective and does not directly ask how India's newer framework measures up against it.

What is missing from the existing literature is a direct side by side comparison that line India's DPDP against these established frameworks on same practical parameters such as individual rights, consent, data minimisation, breach management, cross border transfers, also asking whether the India's framework will go with newer technologies such as AI, deepfakes, cloud computing, IOT. This paper is an attempt to address that specific gap.

III. METHODOLOGY

This paper follows a doctrinal, comparative law approach rather than an empirical approach. In simple terms, this means the study is based on reading and comparing the actual laws, rules, and official guidance. It does not use surveys, interviews, or field data. The main aim is to understand what each legal framework says and then compare them to identify their differences.

Two types of sources were used. The primary sources include the laws, rules and regulations themselves. For India these include the IT Act 2000, IT Rules 2021, DPDP Act 2024 and DPDP Rules 2025 [1]-[4]. For the international comparison the sources include the EU GDPR along with the Data Protection Act 2018, and Singapore's PDPA [5]-[8]. Official guidance from the UK's Information Commissioner's Office and Singapore's Personal Data Protection Commission was also considered. Secondary sources include academic research and commentary on these laws, including Indian research on the DPDP Act to understand how other researchers have interpreted its provisions [9]-[10].

Eight area were selected for comparison: individual rights, consent, data minimisation, breach management, international data transfers, organisational accountability, security obligations and enforcement. These areas were selected because they are important parts of the GDPR, UK Framework and PDPA. India's data protection framework also covers these areas in different ways. Using the same eight areas for all four frameworks allows a fair comparison of the different laws. Each framework was given a score out of 5 for each area.

A higher score means the law provides wider coverage and clear guidance in that area, while a lower score means that the area is less developed or has less detailed guidance. The scores were based on the author's reading of the laws and publicly available official guidance.

There are some limitations to this approach as the study is doctrinal, it does not include case law, actual enforcement results, interviews with regulators, organisations or individuals. Therefore, it cannot fully explain how these laws work in real life situations. Therefore, the scores for India may need to reviewed again as the rules are fully implemented.

IV. INDIA'S EVOLVING CYBERLAW FRAMEWORK

Information Technology Act 2000

The IT Act, 2000 is still the base on which India's cyberlaw sits. It was drafted mainly to give legal recognition to electronic records and transactions, alongside provisions covering certain computer-related offences [1]. Since then, India's digital environment has grown far beyond the e-commerce-focused model that existed when the Act was written. As online platforms grew in size and influence, new questions arose about how much responsibility intermediaries should bear for the content flowing through their platforms.

The IT Rules 2021 responded to this by placing compliance obligations on intermediaries and digital media entities [2]. The rules matter as the platforms today do more than hosting content but they change the perspective of a person.

Information Technology Rules 2021

The IT Rules 2021 were introduced by the government of India to provide updated rules for digital platforms. The rules placed certain conditions on online platforms regarding the content and information handled through their services. The rules introduced requirements for intermediaries including social media platforms and other digital services [2]. These provisions are important because online platforms have become a major part of communication, information sharing and digital services. The rules also cover digital media and online news publishers through the Digital Media Ethics Code. They are an important part of India's cyberlaw framework along with IT Act 2000.

Digital Personal Data Protection Act 2023

The bigger shift, though, came with the DPDP Act 2023. This Act set up a structured system built around three roles' Data Principals, Data Fiduciaries, and Data Processors [3]. It covers consent, notice requirements, the duties of Data Fiduciaries, individual rights, protections for children's data, and rules for processing that happens outside India. What makes the DPDP Act significant is the shift in thinking behind it.

Earlier cyberlaw tended to treat data protection as something that mattered mainly when data was stolen or accessed without permission. The DPDP Act recognises that data collected perfectly legitimately can still create problems later for instance, if it is combined with other datasets, profiled, or reused in ways the individual never anticipated.

The DPDP Rules 2025 add the operational detail that the Act itself does not spell out, and they are being rolled out in phases rather than all at once [4]. Taken together, these four instruments show India moving away from a single, narrowly-focused statute and toward a broader system of digital governance. The main question is whether the Indian laws can keep up with the new digital risks.

Digital Personal Data Protection Rules 2025

The DPDP rules 2025 were introduced to provide more detailed requirements to implement the Digital Personal Data Protection Act. The rules are important part of India's cyberlaw framework as they explain how organisations should follow the requirements of the act in practical situations. The rules state organisations need clear procedures and technical safeguards to properly use, store, and protect personal data. The DPDP Rules 2025 add the operational detail that the Act itself does not spell out, and they are being rolled out in phases rather than all at once [4]. Taken together, these four instruments show India moving away from a single, narrowly-focused statute and toward a broader system of digital governance. The main question is whether the Indian laws can keep up with the new digital risks.

Emerging Technological Challenges

- Artificial intelligence is probably the hardest challenge for current data governance to handle. AI systems often process very large datasets to produce predictions, recommendations, or fully automated decisions. In a typical AI pipeline, several different parties may be involved the developer who built the model, the party who supplied the training data, and the organisation that deployed the final product. When something goes wrong, it becomes genuinely difficult to say which of these parties should be held responsible.
- Deepfakes and other synthetic media raise a different kind of problem. A convincingly faked image, audio clip or video can be used to impersonate a real person, and a single incident might combine fraud, privacy violation, identity misuse and misinformation all at once. It is hard to regulate new technology because the harm may be clear even when the law does not cover the new method.
- Cloud computing complicates things further because data is no longer tied to one physical location. An Indian company might run its systems on infrastructure spread across several countries, which means questions about who can access the data, where it is stored, and who is responsible for it become tangled up with the separate issue of international data transfers.
- IoT devices add another layer of difficulty because they tend to collect data continuously rather than at a single, identifiable moment. Smart cameras, wearables, connected vehicles and home devices generate ongoing streams of behavioural and usage data. Traditional notice-and-consent models where a user reads a policy once and agrees start to lose their meaning when the user cannot realistically track every point at which their data is being collected.

These examples show that laws should focus on basic principles like security, transparency, and accountability instead of regulating each technology separately.

V. COMPARATIVE ANALYSIS AND GAP ASSESSMENT

To get a clearer picture of where India stands, this paper compares four frameworks India, the EU GDPR, the UK, and Singapore's PDPA across eight parameters that are widely treated as core elements of modern data governance: individual rights, consent, data minimisation, breach management, international transfers, organisational accountability, security obligations, and enforcement.

The comparison uses a five-point scale, where a score of 5 reflects broader legal coverage and clearer operational mechanisms for that particular parameter. These scores are based on the author's own analysis and are not official government or regulatory ratings.

Table 1. Comparative Assessment of Selected Parameters

Parameter	India DPDP	EU GDPR	UK Framework	Singapore PDPA
Individual rights	3	5	5	4
Consent	4	5	5	4
Data minimisation	3	5	5	4
Breach management	3	5	4	5
International transfers	3	5	5	4
Organisational accountability	4	5	5	4
Security obligations	4	5	5	4
Enforcement	3	5	5	4
Average	3.4	5.0	4.9	4.1

Table 2. Qualitative Analysis

Area	India DPDP	EU GDPR	UK Framework	Singapore PDPA
Main Legal Framework	DPDP Act, 2023	GDPR	UK GDPR + DPA 2018	PDPA
Individual Rights	Moderate	Broad	Broad	Moderate
Consent	Required in many cases	Strong consent requirements	Strong consent requirements	Consent-based approach
Data Minimisation	Present	Strong principle	Strong principle	Present
Breach Management	Developing	Detailed requirements	Detailed requirements	Defined requirements
Cross-border Data	Developing	Detailed mechanisms	Detailed mechanisms	Defined mechanisms
Regulatory Guidance	Developing	Extensive	Extensive	Extensive
Enforcement	Developing	Established	Established	Established

The GDPR sets out a fairly comprehensive model built on principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability [5]. It also has well-developed mechanisms for breach notification and for governing international data transfers. Because of this level of detail, the GDPR works well as a benchmark for judging how broad legal principles can be translated into concrete, day-to-day obligations for organisations.

The UK's data protection regime follows a similar structure, built around established principles combined with detailed guidance from its regulator, the Information Commissioner's Office [6]. The UK example shows that clear guidance from a strong regulator can make laws easier to follow in practice.

Singapore's PDPA offers a useful non-Western comparison point. It sets out obligations covering consent, purpose limitation, protection of data, retention limits, data transfers and breach notification [7]. Singapore shows that laws can be based on broad principles while still giving organisations clear duties to follow.

India's lower score does not mean that its framework is ineffective. India's system, particularly on the personal-data side, is simply much newer than the other three. The lower scores mostly reflect the fact that implementation mechanisms, regulatory guidance, and enforcement structures are all still being built out, not that the underlying legal principles are missing.

The main gap is not in basic legal principles, because India already has rules for personal data and security. The real gap is in the level of operational detail available to organisations, and in how mature the implementation and enforcement mechanisms currently are.

Breach management illustrates this well. Having a legal duty to respond to a data breach is only the starting point an organisation still has to detect the breach, work out how serious it is, keep a proper record of what it did, and notify both the regulator and the affected individuals. The GDPR and Singapore's PDPA both provide relatively well-established processes for this [5], [7], and India stands to benefit from similar clarity as the DPDP framework becomes fully operational.

International data transfers are another area that needs continued attention. Because cloud computing and multinational digital services routinely move data across several jurisdictions at once, the GDPR, the UK framework and Singapore's PDPA all provide specific mechanisms to govern this [5]– [7]. As India's digital economy keeps expanding internationally, having clear rules on cross-border processing will only become more important.

VI. RESULTS

Three main findings come out of this comparison.

First, India has genuinely made progress in building a wider digital regulatory system. The IT Act, 2000 laid the groundwork for electronic transactions and technology-related offences, and the IT Rules, 2021 together with the DPDP framework have since extended this to cover intermediary responsibility and personal data protection.

Second the main issue is whether the law can adapt to new changes. Technologies such as AI, deepfakes and IoT devices keep producing harms that do not fit neatly into pre-existing legal categories. Trying to pass a new, separate law for every new technology risk creating a fragmented and inconsistent system. A more workable approach is to keep the underlying legal principles broad and stable, while letting regulators issue updated guidance as new technologies emerge.

Third strong institutions are just as important as good laws. A law on paper does not protect anyone by itself organisations need trained staff, working security controls and tested incident-response procedures, and regulators need enough technical and legal expertise to actually investigate complex digital systems when something goes wrong.

Based on these results, five recommendations follow:

1. Technology-neutral guidance: existing principles around privacy, security and accountability should be explained specifically in the context of technologies like AI and synthetic media, rather than left at a purely abstract level.
2. Clearer accountability in multi-party systems: where several organisations are involved in building, processing or deploying a digital system, their individual responsibilities should be spelled out rather than left ambiguous.
3. Stronger, more practical breach-response mechanisms: organisations should be expected to maintain documented procedures for identifying, assessing and responding to security incidents, not just a general legal obligation to "respond."
4. Better guidance on international data processing: organisations that rely on foreign cloud or technology providers need more clarity on exactly what their responsibilities are when personal data is transferred or processed outside India.
5. Regular, built-in review of the law: cyberlaw should be revisited on a regular schedule in light of new technology, major cybersecurity incidents, and how other countries' frameworks are evolving.

India will be better served by keeping basic principles stable and updating guidance as technology changes, instead of making a new law for every technology.

VII. CONCLUSION

India's cyberlaw has moved a long way from the IT Act 2000 toward a more complete system that now includes intermediary obligations and a dedicated data protection regime. The DPDP Act 2023 and the DPDP Rules, 2025 are the clearest markers of this shift.

The comparison carried out in this paper suggests that India has built a solid legal foundation, but is still at an earlier stage of implementation compared with the more established frameworks in the EU, UK and Singapore. The areas that most need continued attention are operational clarity, breach management, international data processing, institutional capacity, and accountability for newer technologies.

The comparative analysis shows that the EU, UK and Singapore frameworks currently provide more detailed guidance and established enforcement mechanisms than India. However, India has developed a strong foundation through the DPDP Act and Rules. The main difference is therefore not absence of legal provisions but the level of practical implementation, regulatory guidance and institutional capacity

This paper does not say that Indian cyberlaw is outdated. It asks whether the law can keep up with new technology without needing a new law every time.

Going forward, India can strengthen its digital governance through technology-neutral principles, more detailed regulatory guidance, stronger organisational accountability, and a habit of periodic review. Done well, this can protect individuals while still leaving room for innovation and continued growth in India's digital economy.

REFERENCES

[1] Government of India, The Information Technology Act 2000, Act No. 21 of 2000, New Delhi, India, 2000.

[2] Ministry of Electronics and Information Technology, Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, New Delhi, India, 2021.

[3] Government of India, The Digital Personal Data Protection Act 2023, Act No. 22 of 2023, New Delhi, India, 2023.

[4] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025, Gazette of India, G.S.R. 846(E), Nov. 13, 2025.

[5] European Parliament and Council of the European Union, “Regulation (EU) 2016/679 (General Data Protection Regulation),” Official Journal of the European Union, vol. L119, pp. 1–88, May 2016.

[6] Information Commissioner's Office, Guide to the UK General Data Protection Regulation, United Kingdom.

[7] Personal Data Protection Commission Singapore, Data Protection Obligations under the Personal Data Protection Act, Singapore.

[8] Information Commissioner's Office, International Transfers: A Guide to the UK GDPR, United Kingdom.

[9] C. Malhotra and U. Malhotra, “Putting interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India,” *Indian Journal of Public Administration*, vol. 70, no. 3, 2024.

[10] A. K. Bisht and N. S. Sreenivasulu, “Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023,” 2024.