RIGHT TO PRIVACY AND DATA PROTECTION AN ILLUSION IN THE ERA OF DIGITALISATION? A CRITICAL STUDY

Mr. Hanumanthappa GT, Research Scholar, P.G Department of Studies in Law, Karnatak University, Dharwad

ABSTRACT

The high pace of digitalisation of the state machinery and business processes made the issue of individual data security and the right to privacy even more acute. This paper is a critical analysis of how privacy as a constitutional right has evolved in India, especially in the light of its being considered one of the fundamental rights and the study of the emergent data protection regulatory framework in the wider context of global regulative trends. The study uses a comparative and doctrinal approach to assess the Indian legal regime and the other international systems, which are the rights-based approach used by the European Union and the sectoral approach which is used by the United States. The research outlines the major problems associated with the underdeveloped enforcement systems, the increasing penetration of the State surveillance, the complexity of the data transfers, and the increased commoditisation of personal data. It contends that despite the recent changes of laws, there is more to be desired as far as accountability and safeguarding individual autonomy are concerned. The paper has ended by reiterating how innovation requires a balanced and rights-based methodology that builds sound privacy controls in tandem with innovation that is backed by proper institutional frameworks and international alignment.

Keywords: Right to Privacy, data protection, digital governance, surveillance, GDPR

Introduction

The fast-growing digital technologies, such as artificial intelligence (AI), big data analytics, and biometric identification systems, have fundamentally altered the essence of governance and individual interaction in modern society. Such technologies have allowed the States and individual players to amass an unprecedented amount of personal information due to their integration into daily living.[1] This information-based ecosystem has enabled efficiency, innovation and economic development, yet it has also created some fears when it comes to individual privacy and autonomy.

Conventionally, the concept of privacy was a spatial or physical concept that ensured that individuals were not intruded upon against their will in their homes or personal space.[2] However, in the digitalised era, the concept of privacy has become more complicated, as a concept of informational privacy, which includes the control over personal information and online identity.[3] The decline of physical privacy in favor of informational privacy is an accurate depiction of the networked world in which personal information is constantly being created, disseminated, and studied on a cross-platform basis. As such, the constitutional forms of governance are now obligated to keep in touch with these technological changes in order to protect the basic rights.

Problem Statement

The growth of digital spy systems by the state, which is frequently based on the ideas of national security and citizens' order, has developed a fissure between the interests of the collective and the freedom of the individual.[4] Mass surveillance schemes, data retention laws, and biometric identification laws are raising crucial issues of proportionality and neediness on constitutional democracies.

Moreover, developing nations such as India are usually confronted with difficulties of broken or dynamic regulatory provisions, which find it difficult to cope with the changes in technology.[5] Such a regulatory gap increases the risks of the unauthorized data processing, data

[1] Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* 6–8 (2013).
[2] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890).
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶ 248 (India).
[4] David Lyon, *Surveillance Studies: An Overview* 3–5 (2007).
[5] Graham Greenleaf, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR

breaches, and algorithmic profiling that can result in the presence of discrimination and civil liberty loss.[6] The lack of effective implementation systems also exacerbates these problems as people are left defenseless against the state and corporate excess.

Research Objectives

The present study aims at examining the constitutional basis of the right to privacy, especially following its declaration as a fundamental right in India. It also seeks to analyze the available data protection regimes in India and contrast them with the international ones, such as the European Union and the United States. Moreover, the study assesses the problem of governance presented by digitalisation, such as surveillance and data commodification. Lastly, it suggests reforms to enhance privacy protection and accountability in the system of data governance.

Research Questions

The research questions that guide the study are the following ones:

- Whether the right to privacy retains its status as a fundamental right in the digital age;
- How effective current data protection laws are in safeguarding individual rights, and
- What lessons can India derive from established international data protection frameworks?

Scope & Methodology

The study employs a doctrinal approach to law, and the legal study is based on the interpretation of the constitutional provisions, judicial precedents, and statutory provisions. It also applies a comparative method and studies the legal evolution in India as compared to that of the European Union and the United States. The developing landscape in privacy and data protection is critically assessed by the use of authoritative sources such as case law, legislation, and institutional reports.

Dominance, 169 Privacy Laws & Bus. Int'l Rep. 10, 12 (2021).

[6] Shoshana Zuboff, *The Age of Surveillance Capitalism* 94–97 (2019).

Conceptual Framework: Right to Privacy and Data Protection

Meaning of Privacy

The concept of privacy has significantly changed in its classical form and is currently expressed in digital form. Privacy used to be viewed traditionally as a right to be left alone and the main focus of privacy is guarding individuals against physical encroachment in their personal sphere. This concept included bodily privacy, protection of bodily integrity and space control.[7] In the course of time, the concept was broadened by the courts and academics to include decisional privacy, which safeguards personal autonomy in intimate personal decisions concerning family, marriage and bodily integrity.[8]

However, in the digital age, the greatest change that has taken place is that there is the introduction of informational privacy, whereby there is the control of individual personal data and its distribution.[9] The spread of digital environments, surveillance policies and data analytics has not only moved the parameters of privacy to the virtual instead of the physical realm but also transformed it into data streams rather than spaces. This development can be seen in the fact that the concept of privacy has become recognized in constitutional jurisprudence as an essential right, and that informational self-determination is part of dignity and freedom.[10] One therefore assumes that privacy in a contemporary society is a multidimensional concept that can no longer be maintained within physical boundaries but rather through control over one's digital identity.

Data Protection

Data protection can be defined as the legal and regulatory framework that maintains the protection of personal information against misuse, unauthorized access, and usage. It includes regulations of information about gathering, processing, storage and transfer of personal information.[11] There is a significant difference between personal data and sensitive personal data; the latter is considered to contain health information, biometric data, and financial information, among others, which demand extra protection because they can and do identify or

[7] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890).
[8] *Roe v. Wade*, 410 U.S. 113, 152–53 (1973).
[9] Alan F. Westin, *Privacy and Freedom* 7 (1967).
[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 248, 297 (India).
[11] European Parliament & Council Regulation 2016/679, art. 4(1), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

have some connection to a person.[12]

The contemporary data protection regimes are set up on the basis of fundamental values. They are consent, whereby individuals willingly consent to the processing of their data; purpose limitation, where data can only be used in a finite number of legitimate objectives; and data minimisation, where it is necessary that only the essential data must be collected.[13] Other principles like transparency, accountability and limitation of storage also strengthen the regulatory structure. All these principles are intended to strike a balance between innovation and economic utility, and personal rights protection.

Relationship between Privacy & Data Protection

Data protection is commonly considered to be an extension and operationalisation of the overall right to privacy. Data protection is a procedural and institutional means by which privacy is instigated in a digital environment as a normative right (which is founded on dignity and autonomy).[14] In this regard, data protection regulations put into effect abstract constitutional guarantees by turning them into specific duties of the State as well as non-State actors.

Yet, the rising commercialization of individual information poses great problems to such relationships. The threat of data-driven business models has capitalised on individual information as an economic resource, traded and analysed in large volumes, with no significant control by the user.[15] This has been called the so-called surveillance capitalism and is dangerous in that it is likely to compromise the principle of autonomy and increase the imbalance of power between the data controllers and the data subjects. As a result, a sound conceptual framework should acknowledge that sound data protection is essential to the maintenance of privacy in the digital era, as it is the solution to commoditisation of data, which represents a systemic risk.

Constitutional Perspective on Privacy in India

Early Judicial Approach

The right to privacy is not clearly stated in the Constitution of India. The Supreme Court of the

[12] Id. art. 9.
[13] Id. art. 5.
[14] Orla Lynskey, *The Foundations of EU Data Protection Law* 5–7 (2015).
[15] Shoshana Zuboff, *The Age of Surveillance Capitalism* 94–97 (2019).

early constitutional jurisprudence followed a limited approach in interpreting the constitution that it refused to acknowledge privacy as a separate basic right. In *M.P. Sharma v. Satish Chandra*, the Court held that the Constitution did not guarantee a general right to privacy analogous to the Fourth Amendment of the United States Constitution.[16] Similarly, in *Kharak Singh v. State of Uttar Pradesh*, the majority rejected the existence of a constitutional right to privacy, although it struck down domiciliary visits on the ground of personal liberty under Article 21.[17]

Despite the hesitation of the first refusal, there was a gradual change in later decisions. In *Gobind v. State of Madhya Pradesh*, the Court indicated tentatively that the right to privacy might be implicit in the rights provided in Part III of the Constitution, especially Articles 19 and 21.[18] This trajectory continued in cases such as *R. Rajagopal v. State of Tamil Nadu and People's Union for Civil Liberties (PUCL) v. Union of India*, where the Court recognised facets of privacy in relation to reputation and telephone tapping, respectively.[19] So, although the establishment of privacy as a constitutional right was not explicitly known before, privacy had been gradually incorporated into the constitutional fabric by judicial interpretation.

Landmark Judgment

This was finally resolved in *Justice K.S. Puttaswamy (Retd.) v. Union of India,* where a bench of nine judges in the Supreme Court voted unanimously that the right to privacy was a basic right to part III of the Constitution.[20] The Court reasoned that privacy was inherent to the right of life and personal liberty in Article 21 and inseparable with the freedoms which were enshrined in Article19.[21]

Noticeably, the conceptualisation and idealisation of privacy considered privacy as including dignity, independence and self-determination of an individual. It has realised that in the digital era, informational privacy is an essential factor whereby individuals have to maintain power over their personal information.[22] The Court reversed previous decisions like M.P. Sharma and

[16] *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300, 306 (India).
[17] *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295, 1302 (India).
[18] *Gobind v. State of Madhya Pradesh*, (1975) 2 S.C.C. 148, 155 (India).
[19] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632 (India); *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 S.C.C. 301 (India).
[20] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[21] Id. ¶¶ 297, 325.
[22] Id. ¶ 248.

Kharak Singh to the degree that they failed to recognize that a basic right of privacy was a constitutional right and literary turned out to be a ground breaking development in the Indian constitutional statute.[23]

Key Principles Evolved

The structure of the function established in the Puttaswamy judgment was to determine the correctness of the State action that violated privacy. The first principle of this system is the principle of proportionality, which states that every limitation on privacy must be based on a proper purpose, be appropriate to fulfill that purpose, and be essential in the case of a lack of restrictions that would be equally effective.[24]

The Court also made the legality, necessity and procedural protections requirements articulate. The interception of privacy should be founded on some legal basis, have respect to some lawful purpose by the State, and they should have certain mandatory protection against unreasonable invasion.[25] These principles would provide that the power of the State is checked by constitutional boundaries and is courts, therefore, strengthening the rule of law.

Challenges in Constitutional Governance

Regardless of the clear doctrines presented by Puttaswamy, there are still major obstacles towards implementing privacy rights in the context of the Indian constitution. The executive has been allowed wide authority in interception by several statutes concerning surveillance, such as the Indian Telegraph Act, along with the Information Technology Act, but these provisions are often provided without much transparency or accountability.[26] This brings up the question of possible mass surveillance and misuse of power.

The Aadhaar project, which implies the gathering of biometric and demographic information, also illustrates the conflict between the welfare goals and the privacy rights. In K.S. Puttaswamy (Aadhaar), the Supreme Court authorized the scheme Aadhaar as constitutional but imposed a limit on its application, especially by non-government entities.[27] Still, data

[23] Id. ¶¶ 3, 119.
[24] Id. ¶ 325.
[25] Id. ¶¶ 180–182.
[26] Indian Telegraph Act, 1885, § 5(2); Information Technology Act, 2000, § 69.
[27] *K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 S.C.C. 1 (India).

security, exclusion, and function creep are the issues of concern.

In the end, the problem of reconciliation is the relationship between State interests in government, national security, and prosperity on the one hand and interests of individual autonomy and dignity on the other. This growth of digital governance requires strong institutional protections to avoid disproportional interferences with privacy, as well as constitutional responsibility.

Data Protection Framework in India

Existing Legal Framework

Over the years, India has been regulated by the Information Technology Act, 2000 (IT Act), supplemented by other related acts like the Information technology (Reasonable security practices and procedures and Sensitive Personal Data or Information) Rules, 2011.[28] These laws initiated the responsibilities that body corporates should have reasonable security practices and seek consent before using and collecting sensitive personal information.[29]

Nevertheless, the IT Act framework has continuously been criticised on the basis of its small coverage and dispersive nature. It is applicable mainly on the registration of the private ones and not exhaustive in terms of the surveillance by the State and data processing.[30] Besides, the scope of sensitive personal data is limited and means of enforcement are weak since there is no external regulating body.[31] With the growing digital ecosystems, these failures led to vulnerability, including data breaches, unauthorised sharing, and inefficacy of remedies, which resulted in the need to have a more robust and more comprehensive legal framework.

Recent Developments

To address these shortcomings, India has passed the Digital Personal Data Protection Act, 2023 (DPDP Act) which will be a major step in the transition to a formal regime of data protection.[32] The Act puts in place a rights framework of dealing with digital personal data, and addresses

[28] Information Technology Act, 2000, No. 21 of 2000, § 43A (India).
[29] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), § 3 (India).
[30] Justice B.N. Srikrishna (Chairman), *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 17–18 (2018).
[31] Id. at 45–47.
[32] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

all the aspects that involve the processing of such data, whether by a private or a government body.

One of the most prominent aspects of the DPDP Act is the priority to consent, which should correspond to free, informed, specific, and unambiguous.[33] The law brings in a new term of data fiduciaries, which are entities that establish the end use and the data course of action entailing accountability and liability.[34] Also, it acknowledges other rights of individuals (data principals) such as the right to access information, rectify errors and request redressal of grievance.[35]

The Act also offers the formation of a Data Protection Board of India to supervise the compliance, as well as resolve conflicts.[36] This institutional tool is supposed to increase the level of enforcement and increase compliance to statutory responsibilities in a fast changing digital world.

Critical Evaluation

The DPDP Act can be seen as an important reform in the Indian data protection framework due to the introduction of the more coherent and structured regulatory system. To the extent that it prioritizes consent and accountability and establishes specific roles, notably data fiduciaries, it fits into the global standards like the GDPR, to a certain degree.[37] The establishment of a specialized enforcement authority also enhances the structure by implementing a compliance and redress avenue.

However, flaws of the legislation exist. The wide exemptions accorded to the State are one of the issues of great concern, especially on the reasons like national security and maintaining the order which can further erode the very provisions of the protection as had been intended in the Act.[38] These exemptions lead to the concern of proportionality and the risks of unscrupulous surveillance. Also, institutional autonomy might be destabilized by the lack of a completely independent data protection authority and the use of executive-influenced mechanisms.[39]

[33] Id. § 6.
[34] Id. § 2(i).
[35] Id. §§ 11–14.
[36] Id. § 18.
[37] European Parliament & Council Regulation 2016/679, art. 5, 2016 O.J. (L 119) 1 (EU).
[38] Digital Personal Data Protection Act, 2023, § 17 (India).
[39] Apar Gupta & Udbhav Tiwari, The DPDP Act and the Question of Independence, 58 Econ. & Pol. Wkly. 12,

There are also still gaps in enforcement especially on the issue of data flows across borders, technological impossibilities, and low levels of public understanding. Therefore, the DPDP act is a progressive move but its operationalization, judicial interpretation and building of a secure institutional framework that ensures that governance needs are met and the rights of individuals to their privacy are addressed will determine its success.

International Scenario: Comparative Analysis

European Union

The most thorough and strict example of data protection in the world is the one of the European Union (EU), which is mostly the General Data Protection Regulation (GDPR).[40] The GDPR has created a common law foundation to the member states, which is based on basic rights and the security of personal data expansion of human dignity under Article 8 of the EU Charter of Fundamental Rights.[41]

Accountability, transparency, and strong user rights (right to access, rectification, erasure, or failure to forget), are the main values of the GDPR that need to be fulfilled by data controllers, who have to prove their compliance with the regulations like data protection, transparency, and the right to have all necessary information about data processing.[42] The regulation also ensures good terms of consent and high punishment against a non-compliant person and thus makes sure that it is well enforced.[43] The EU model is extensively considered to be a model because it is rights-focused and it is institutionally strong, considering all independent supervisory authorities across every member state.

United States

Conversely, the United States is more sectoral in regulating data protection, that is, regulation is broken down into particular industries, instead of England having a single federal system of regulation.[44] Some of the key laws are Health Insurance Portability and Accountability Act (HIPAA), health information laws, and the Gramm-Leach-Bliley Act (GLBA), information

14 (2023).
[40] European Parliament & Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[41] Charter of Fundamental Rights of the European Union art. 8, 2012 O.J. (C 326) 391.
[42] GDPR arts. 5, 12–22.
[43] Id. art. 83.
[44] Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* 881–83 (6th ed. 2018).

privacy laws regarding financial data.[45]

It is a market-driven paradigm that relates more to innovation and economic development, at times giving relatively low value to comprehensive privacy protection. Although some states, especially California, with the California Consumer Privacy Act (CCPA), proposed more extended protection, the lack of a comparable federal law leads to the inconsistency of regulations across jurisdictions and differences in the intensity of protection.[46] The regulation is usually done through industry-specific authorities or bodies like the Federal Trade Commission, which results in a reactive and not a proactive regulatory system.

Other Jurisdictions

Other governments, such as the United Kingdom and Australia, have come up with hybrid models that incorporate the things of the EU model but to suit the domestic laws. The Data Protection Act 2018 of the United Kingdom is in line with the UK GDPR and as a result, is in line with EU standards after Brexit.[47] Equally, the Privacy Act 1988 of Australia creates the Australian Privacy Principles, which govern the data handling practice with relatively less stringent enforcement measures.

It is now an international trend in harmonisation towards emerging economies adopting data protection laws based on the GDPR. The problem however, is the actual implementation because the challenges are often faced by enforcing certain laws, institutional capacity and the developmental priorities.[48]

Comparative Insights

When compared, it can be found that the model of the EU represents the global gold standard, due to its extensive coverage, rights orientation, and effective enforcement systems. Conversely, U.S. model is flexible and has lack of coherence and uniformity in protection. Other jurisdictions hold a middle ground whereby they have both regulations and a liberal

[45] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[46] Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. 902, 906–07 (2009).
[47] Data Protection Act 2018, c. 12 (UK).
[48] Graham Greenleaf, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, 169 Privacy Laws & Bus. Int'l Rep. 10, 12–13 (2021).

attitude on economic matters.

There are still notable disparities regarding enforcement, institutional autonomy and the level of protection of the citizens. The stress of the EU on independent supervisory bodies and harsh penalties seems to have the opposite of their relatively decentralised and industry-based enforcement in the United States.[49]

These comparative insights have specific implications in the case of India, which stipulates the necessity to follow a balanced approach in the combination of effective enforcement with substantial rights-based protections. Among the lessons learned are the necessity of an independent regulatory body, the uniqueness of the data processing principles and strong protections against overreaching by the State. Simultaneously, the Indian framework should be adjusted to the local socio-economic environment so that data protection fosters the rights of people and online innovations.

Challenges in Data Protection

The modern state of data protection is characterized by continuous structural and technological issues that do not support the successful implementation of privacy rights. One of the basic issues includes the ignorance of the citizens concerning the rights to data and computer risks that undermine the intellectual consent and reduces the possibility of pursuing legal justice.[50] This is further worsened by poor enforcement mechanisms, especially where the regulatory agencies have no independence, resources, and technical know-how to enforce compliance.

Cross-border data transfers make the governance even more baffling, considering that different legal systems come with conflict of jurisdiction and leak personal information to different protection. Meanwhile, the pace of rapid technological progress (artificial intelligence, big data analytics, etc.) remains faster than the legislative reaction, and current frameworks do not correspond to the current state.[51] Also, the growing number of cybersecurity risks, such as data leaks and ransomware, demonstrates system weaknesses in data processing systems. All these issues require adaptive, powerful, and globally aligned regulatory frameworks.

[49] Solove & Schwartz, supra note 5, at 889–90.
[50] Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 14–15 (2013).
[51] Shoshana Zuboff, *The Age of Surveillance Capitalism* 101–03 (2019).

Conclusion

Privacy is a principle that can be used as a guide of constitutional management in the digital world and strong data protection patterns are required. Although India has achieved a lot by getting Judicial recognition and legislative reform, enforcement, State surveillance, and technological evolution troubles are still in place. Comparative lessons suggest how significant a rights-based and accountable regulation model is. Going forward, a middle ground that protects the freedom of individuals and allows innovation is needed. Improving institutional controls, public awareness and global alignment will be very important in offering good and viable data protection in a society which is more digitalised.

Bibliography

Books

- Alan F. Westin, *Privacy and Freedom* (1967).
- Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* (6th ed. 2018).
- David Lyon, *Surveillance Studies: An Overview* (2007).
- Orla Lynskey, *The Foundations of EU Data Protection Law* (2015).
- Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).
- Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (2013).

Journal Articles

- Apar Gupta & Udbhav Tiwari, The DPDP Act and the Question of Independence, 58 Econ. & Pol. Wkly. 12 (2023).
- Graham Greenleaf, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, 169 Privacy Laws & Bus. Int'l Rep. 10 (2021).
- Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. 902 (2009).
- Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

Cases

- *Gobind v. State of Madhya Pradesh*, (1975) 2 S.C.C. 148 (India).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
- *K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 S.C.C. 1 (India).
- *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295 (India).
- *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India).
- *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 S.C.C. 301 (India).

- *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632 (India).
- *Roe v. Wade*, 410 U.S. 113 (1973).

Legislation & International Instruments

- California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2020).
- Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.
- Data Protection Act 2018, c. 12 (UK).
- Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
- European Parliament & Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation).
- Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
- Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.
- Indian Telegraph Act, 1885 (India).
- Information Technology Act, 2000, No. 21 of 2000 (India).
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
- Privacy Act 1988 (Cth) (Austl.).

Reports

- Justice B.N. Srikrishna (Chairman), *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).
- Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).