VOLUME 21 ISSN 2456-9704

DATA PROTECTION REGIME: A COMPARATIVE ANALYSIS

By Chetan Sikarwar, Vagish Pandey and Gowri Krishna
From Rajiv Gandhi School of Intellectual Property Law (IIT-KGP)

1. Introduction

We are living in the age of technology, where there are so many ways to share information swiftly. According to a study conducted globally, the expected volume of data we will generate by 2020 will be 44 zettabytes.[1] With such extensive data and such fast-growing technology, data protection poses a challenge to lawmakers. It is now imminent that the Government of India develop a robust data protection regime to prevents theft of individual's data and protects it from the State and corporates. This need has been reinforced by *Justice Puttaswamy's judgment,*[2] where the honorable Supreme Court of India has declared Privacy as a fundamental right. As the data protection law is yet to be developed in India, the research aims to study and analyze the existing legal regimes of different jurisdictions to establish a robust data protection law in India.

2. Privacy and Data Protection:

In *Justice K.S.Puttaswamy(Retd) case,* Justice D Y Chandrachud said: *"privacy ensures the fulfillment of dignity and was a core value which is the protection of life and liberty was intended to achieve."*[3] It highlights the importance of Privacy, but the irony is we do not understand what it means?

According to IAPP, the world's largest global information privacy community, Privacy is the right to be left alone or the freedom from intrusion or interference.[4] It establishes the boundaries around an individual and provides the individual a say in matters having a direct bearing on him. The concept of Privacy is more extensive than our comprehension in the legal sense, which is seclusion and secrecy. It encompasses much more than that; it is about one's control over all matters restated to one's personal information.

Privacy has three different facets; Firstly, one's physical space, body, and things known as spatial Privacy. Secondly, the choice of an individual is known as decisional Privacy, and lastly, the informational aspect of Privacy that is information related to the individual himself.[5]

Data protection is typically related to informational Privacy, but the intrusive nature of technology and its pervasive presence has impacted spatial as well as the decisional aspect of Privacy. Protecting the privacy of an individual is critical, as its impact is significant and intangible. We have seen that the disclosure of certain sensitive and inflammatory information, no matter

[1] 'The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things', EMC Digital Universe with Research and Analysis by IDC (April 2014), available at:https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm, (visited on 18 April 2020).

[2] *Justice K S Puttaswamy(Retd)* v *Union of India & Ors.* 2017 (10) SCALE 1

[3] *Ibid*

[4] About the IAPP, https://iapp.org/about/what-is-privacy/ (visted on 18 April 2020)

[5] Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review 1193, 1202-03 (April 1998).

how true it is, has resulted in stereotyping and pre-judging of person[6].

In modern times data fuels world economies. This development has posed a new challenge for the lawmaker to develop a cohesive and robust system that not only acts as a floodgate to protect the overflow of user information but also ensure the sufficient flow to maintain the engine running. So, any competent data protection legislature must have

a. Identification of critical information
b. Ensure the freedom of an individuals' choice of disclosing their information.

3. Evolution of Data Protection regime

Evolution in data protection rules and policy started in the 1970s data of individuals were computerized.[7] This matter was addressed by the United States government by appointing an Advisory Committee in the Department of Health, Education, and Welfare (HEW Committee). The committee has examined various legal and technological issues related to data processing. The committee published a report titled '*Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems.*' The committee's recommendation paved the way for a code of Fair Information Practices based on Fair Information Practice Principles (FIPPS), and now FIPPS acts as the foundation for modern data protection laws.

The key recommendation of FIPPS are as follows:

a. There must be no personal data record-keeping systems whose very existence is kept secret.
b. There must be a way for an individual to find out what information about him is in a record and how it is used.
c. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
d. There must be a way for an individual to correct or amend a record of identifiable information about him.
e. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the Data

The other significant development in the field of evolution of data protection law came in the 1980s when OECD published its privacy guidelines (which were updated in 2013)[8]. OECD guidelines were highly influenced by FIPPS.

OECD privacy guidelines provided a framework for member countries to harmonize their national data protection law accordingly while ensuring the human rights of users and providing the free international flow of data across borders[9].

[6]Jeffrey Rosen, 'The Unwanted Gaze: The Destruction of Privacy in America' (Random House, 2000).
[7]Robert Gellman, 'Fair Information Practices: A Brief History' (April 10, 2017), available at: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (visited on 18 April 2020).

[8] OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.ht m (visted on 18 April 2020).
[9]*Ibid*

Based on OECD guidelines, various member nation has streamlined their national legislations and so have the regional grouping like EU[10], Asia-Pacific Economic Cooperation framework (APEC framework)[11], Australia[12], New Zealand[13], Japan[14], etc.

4. Issues with Data Protection Principles

The continually increasing volume of personal data, advanced computing, and global nature information are some challenges where traditional privacy data protection principles failed to leave any impact. OECD amended its guidelines in 2013 to tackle the obstacles posed by new technology. These updated guidelines were the perfect blend of core privacy principles like collection limitation, data quality, and product specification, etc. and some more unique ideas like enhanced accountability of data controller through privacy management programs,[15] notification on data breach (mandates data controller to inform the individual on breach),[16] creation of privacy management authority,[17] cross border data flow,[18] the global corporation on interoperability of privacy frameworks.[19]

Many critics have believed that these updated guidelines are still not sufficient to deal with modern technology like big data analytics, which has revolutionized the manner of data collection and processing.[20] They have argued that the current guidelines only target the linear data collection like employee details, customer details, etc. but now the mode of data collection has evolved. The big Corporates are now collecting data in a manner that no one had ever foreseen. The modern-day data collection can be characterized in 3Vs, 'volume' (massive data set), 'velocity' (quick and real-time movement of data), 'variety' (related to different sources).[21] Another issue which traditional privacy principles are unable to

[10]European Directive 95/46/EC Data Protection Directive, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 (visited on 18 April 2020)

[11]APEC Framework in 2004, https://iapp.org/media/pdf/resource_center/APEC_Privacy_Framework.pdf (visited on 18 April 2020)

[12]Australia's Privacy Act, 1988 (Privacy Act), https://www.legislation.gov.au/Series/C2004A03712 (visited on 18 April 2020)

[13] New Zealand's Privacy Act, 1993, http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html (visted on 18 April 2020)

[14]Japan's Protection of Personal Information Act, 2003, https://www.jetro.go.jp/ext_images/usa/APPI.pdf (visted on 18 April 2020)

[15]Privacy management programmes are intended be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms to ensure data is safeguarded (Organisation for Economic Co-operation and Development, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (visited on 18 April 2020).

[16]OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (visited on 18 April 2020)

[17]*Ibid*

[18] *Ibid*

[19] *Ibid*

[20] Jordi Soria-Comas and Josep Domingo-Ferrer, 'Big Data Privacy: Challenges to Privacy Principles and Models', 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x (visted on 18 April 2020).

[21] Information Commissioner's Office (UK), 'Big Data, Artificial Intelligence, Machine Learning and Data Protection', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (visited on 18 April 2020)

cater to is free and informed consent that conforms to the basic tenets of contract law while availing free services that allow third parties to access/use such data without the free consent of the user,

5. Approaches to Data Protection in various jurisdictions:

On a broader analysis of foreign data protection regime, two general principles emerge, one is right based approach followed by EU, the second one is the market-based framework where sector-specific regulations are made, followed by the United States of America.

a. European Union

European charter on fundamental rights acknowledges the Right to Privacy as a fundamental right of its citizen; Article 7 ensures the right of Privacy[22], whereas Article 8 provides the right to protection of personal data[23]. To uphold, both the right EU came up with European Union General Data Protection Regulation 2016 (EU GDPR). OECD guidelines profoundly influence EU GDPR.

EU GDPR provides comprehensive protection against the processing of personal data, collection of personal data both by privates and the Government. But these protections are not absolute and make way for exceptions in cases of national security, defense, public safety. Due to the right based approach of EU GDPR, it possesses excellent emphasis on the processing of personal data during collection as well as post collection[24]. The GDPR describes certain information as sensitive information like ethnicity, religious faith, race, political opinion, philosophical beliefs, etc. and collection of such information is prohibited (subject to specific exception[25]

Article 5[26] of EU GDPR describes specific guidelines for the collection and processing of personal data these principles are: -

a) The processing of data should be lawful, fair, and transparent.[27]
b) The collection should be for specific, explicit, and legitimate purposes.[28]
c) The collection should be limited, adequate, and relevant.[29]
d) It should be accurate and up to date.[30]

[22] Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications

[23] Protection of personal data -
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[24] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

[25] Article 9, https://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm (visited on 18 April 2020)

[26] https://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm (Visited on 18 April 2020)

[27] Article 5(1)(a) of EU GDPR

[28] Article 5(1)(b) of EU GDPR

[29] Article 5(1)(c) of EU GDPR

[30] Article 5(1)(d) of EU GDPR

e) It must be anonymized, minimized, and only used for exempt purposes.[31]
f) Its appropriate security should be maintained.[32]

GDPR provides an exceptional level of control of users over their data. There are various rights enshrined in the document, which provides extensive control of users over the data pre and post collection. Some such rights are:-

a) Right to receive acknowledgment about data processing[33]
b) Right to access by the data subject[34]
c) Right to ratify data[35]
d) Right to portability of data[36]
e) Right of rectification or erasure of personal data or restriction of processing[37]
f) Right to erasure[38]
g) Right to object to processing[39]
h) Right to object to processing for direct marketing[40]
i) Right to object to automated decisions[41]

The EU GDPR also talks about a specific regulating authority that has various powers and functions.[42] Article 4(21) defines a 'supervisory authority,' which is an independent public body. Chapter VI of GDPR is dedicated to this authority and to ensure its independence[43]

Many countries have followed the EU model with specific changes. Two prominent nations that followed on the same line are Australia and Canada. The privacy Act of Australia and Personal Information Protection and Electronic Documents Act, 2000 have made specific changes to their regulatory model and opted for a hybrid model, where both industry and Government cooperate to regulate the activities concerned with data protection.

b. United States of America

In the USA the data protection is more or less protection of liberty, which means protection of personal space form government.[44] The American understanding of Privacy is a minimal intrusion from the State[45]. In contrast, the Supreme Court of the USA has recognized the Right to Privacy as a constitutional right as guaranteed by the First, Fourth, and Fifth amendments to its constitution[46].

In the United States of America, there is no comprehensive data protection regime; instead, there are some sector-specific

[31] Article 5(1)(e) of EU GDPR
[32] Article 5(1)(f) of EU GDPR
[33] Article 15(1), EU GDPR.
[34] Article 15, EU GDPR
[35] Article 16, EU GDPR
[36] Article 20, EU GDPR
[37] Article 19, EU GDPR
[38] Article 18, EU GDPR
[39] Article 21, EU GDPR
[40] Article 21 (2), EU GDPR
[41] Article 22, EU GDPR
[42] Article 4(21) and 51, EU GDPR

[43] Chapter VI contains two sections, Section 1: Independent Status (contains 4 Articles) and Section 2: Competence, task and power (contains 5 Articles)
[44] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005).
[45] *Ibid*
[46] Roe v. Wade 410 U.S. 113 (1973) and Griswold v. Connecticut 381 U.S. 479 (1965). See Ryan Moshell, 'And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework', 37 Texas Tech Law Review (2005)

regulations. Another variation form the EU approach is different guidelines for the public and private sectors.

5(b)(i) The Public sector

Certain legislations like The Privacy Act, 1974, The Electronic Communications Privacy Act, 1986, The Right to Financial Privacy Act, 1978 regulates the collection of data by the Government and its agencies.

5(b)(ii) The Private Sector

The Private Sector is entirely regulated by various sector-specific regulation, and above legislations (the public sector legislations) have no role to play in regulating the process in these areas. Some prominent regulations in private sectors are the Federal Trade Commission (FTC) Act, the Financial Services Modernization Act (Gramm-Leach-Bliley Act or GLB Act), the Health Insurance Portability and Accountability Act (HIPAA), and Children's Online Privacy Protection Act (COPPA), etc. Along with these specific regulations, States have their own rules and legislations.

These regulations are generally based on Notice and Consent practice. The FTC has two broad functions one is to ensure consumer data protection, and second is to ensure proper competition in the market. FTC provides data protection by bringing an action against companies that violate the 'most fundamental principles like the failure of companies to post their privacy policies and unauthorized disclosure of user information.'[47]

The GLB Act, as well as the HIPAA Act, are more focused on notice and consent. For instance, title V of the GLB Act emphasizes explicit consent and providing clear disclosure to consumers regarding such collection[48]. The HIPPA focused on types of consent and notice.[49]

c. The Indian Approach

India has witnessed various judicial pronouncements and legislations, which makeup the jurisprudence in this area.

5(c)(i) Judicial Developments Right to Privacy

The discussion on the right of Privacy was first brought in *M P Sharma,*[50] where the court held that the Right to Privacy is not a fundamental right. Later in *Kharak Singh,*[51] the Supreme Court of India stated that "Article 21 is a repository of residuary personal rights and it recognized the common law right to privacy.

The apex court of India, finally in *Puttaswamy,*[52] recognized the Right to Privacy as one of the fundamental rights. Justice D Y Chandrachud, in para 169 of the judgment, has argued that *"privacy facilitates freedom and is intrinsic to the exercise of liberty."* Court has drawn inferences from

[47] Martha K. Landesberg et al., 'Privacy Online: A Report to Congress', FTC (June, 1998) available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (Visited on 18 April 2020)

[48] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn ed., Routledge, 2006)

[49] *Ibid*

[50] *M P Sharma* v *Satish Chandra* (1954) SCR 1077

[51] *Kharak Singh* v *State of UP* 91964) 1 SCR 332

[52] *Supra.*

Article 25, Article 26, and Article 28(3) of the constitution and stated that the Right to Privacy was necessary to exercise these rights. The court focused on the overlapping nature of fundamental rights and highlighted that Privacy, not being a fundamental right, crippled the full enjoyment of these other rights. In this judgment, the court recognized the importance of "informational privacy" and categorized it as an important aspect of the Right to Privacy, which can be claimed against State as well as Non-State actors.

5(c)(ii) Legislative Development

The first attempt to institutionalized the protection of informational Privacy was seen in the Information Technology Act, 2000 (IT Act).[53] Section 43A of IT Acts empowers the ministry to issue rules, and the Ministry of Information and technology has issued SPDI rules[54]. It provides certain rights to an individual. For instance,

1. Rule 5(1), which mandate the requirement of consent for data collection,
2. Rule 5(2) emphasizes the collection of information for lawful purposes.
3. Rule 5(4) specifies the time limit for which the data can be retained.
4. Rule 5(6) provides the right to an individual to correct his or her information.
5. Rule 6 ensures no publication of information without consent unless disclosure is allowed by contract or necessary for legal compliance[55].

The SPDI Rules and IT Act are the combinations of the models followed in the EU and the US. On the one hand, it provides various rights to information holders, which makes these rules as citizen-centric and, on the other hand, adopts the consent and notice principle, which makes them more market-friendly. Another resemblance to the US model is its application, as these rules are only applicable to corporates and non-state actors. Another striking similarity of the IT Act with the EU model is the creation of a dedicated and separate regulating authority. Chapter VI deals with the creation of such authority in India.

The next relevant legislation, which is related to data collection and processing, is the Aadhaar Act.[56] The Act has more inclination toward the EU model, where one independent and centralized authority, (Unique Identification Authority of India or UIDAI),[57] is entrusted with the functions of data collection (including Biometric data)[58], Authentication of data,[59] etc. UIDAI can also allow other parties, both corporate and Government agencies, to use its authentication services, provided they take the consent of the user.[60] Aadhaar (Data Security) Regulation, 2016, imposes the regulations on UIDAI to protect the users' data. The Aadhaar Act has dedicated an entire Chapter to ensure the protection of the

[53] Act no 21 of 2000

[54] The Information Technology (Reasonable Security Practices and Sensitive Personal Data of Information) Rules, 2011 (SPDI Rules)

[55] Exception to this rule is provide in sub-rule1 which allows the disclosure of information without consent if government agencies require information.

[56] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 Act no 18 of 206.

[57] Section 11

[58] Section 3

[59] Section 8

[60] Ibid

information.[61] Section 28 of the Aadhar Act makes it mandatory for the authority to take all possible measures to ensure the safety of information against unauthorized access, unlawful disclosure, loss, destruction, or damage.[62] Section 29 places an absolute bar on sharing of biometrics information of an individual (sensitive information) with anyone, while the Act lays down specific exceptions as to when sharing of such information is allowed and lists down conditions in order to do so.[63]

Apart from centralized laws that regulate data collection and data processing, certain sector-specific laws also govern data privacy. For instance: in the financial sector, there are Credit Information Companies (Regulation) Act, 2005 (CIC Act)[64] , and RBI circulars. Apart from that, financial information like cards (credit, debit) and other payment instrument details are categorized as sensitive information, and hence provisions related to SPDI regulations are also applicable.

CIC Act primarily deals with credit card information and allows companies to collect such information.[65] Section 29 imposes certain Privacy principles on the companies in connection to collection, processing, collecting, recording, preservation, secrecy, and usage of credit information. Section 3 of the Act places an absolute bar on any business related to credit information without certification from RBI.

RBI circular on eKYC limits the information that banks or financial institutions can collect form their customers. Simultaneously imposes a duty on banks to keep such collected information safe.[66] Other circulars of RBI issued from time to time regulate the collection of such information.[67]

Telecom Sector is another critical sector that imposes stricter norms on companies when it comes to the collection of data and it's processing and protection. Indian Telegraph Act, 1885[68], the Indian Wireless Telegraphy Act, 1993[69], the Telecom Regulatory Authority of India Act, 1997[70], are some legislations that contains several provisions to regulate data and related activities.

Despite the Right of Privacy being a fundamental right in India, we were missing a centralized authority that could regulate the transfer and usage of personal data, create a relationship of trust between a person and data collection entities, make such entities accountable, lay down standard norms for all sectors to regulate the cross-border transfer of data, and prevent unauthorized collection and processing of data. To tackle these issues,

[61] Chapter VI: Protection of Information contains 6 sections like security and confidentiality of information, restriction on sharing information, biometric information deemed to be sensitive information etc.
[62] Section 28(3)
[63] Section 29(3)
[64] Act No 30 of 2005
[65] Regulation 2(b), CIC Regulations
[66] Master Direction – Know Your Customer (KYC) Direction, 2016 (Updated on April 20,2020), available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566 (visited on 10 May 2020)
[67] Master Circular on Credit Card, Debit Card and Rupee Dominated Cobranded Prepaid Card operations of Banks, 2014, available at https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=8998#6 (visted on 10 May 2020). Paragraph 6 of the Master Cerciular talks about protection of Customer's Rights, which includes Right to Privacy, Customer Confidentiality, etc.
[68] Act no 35 of 1885
[69] Act no 17 of 1993
[70] Act 24 of 1997

the Ministry of law and Justice introduced the Data Protection Bill 2019 in the Lok sabha.

Salient feature of the Data Protection Bill 2019

The statement of the object of the bill defines salient features of the bill

1. Promote the concept of consent framework, purpose limitation, and limitation of data minimization
2. Place certain obligation on data collecting and processing entities
3. Confers Rights on the citizens
4. Establishment of an Authority
5. Provide power to authority to protect data protection principles and prevent misuse of personal data.
6. Specify the provision related to social media intermediaries
7. Confer right of grievance
8. Empower the Central Government to exempt any governmental agencies form application of this law
9. Specify the code of practice to promote good practice of data protection
10. Appointment of adjudicating officer
11. Establishment of an appellate tribunal
12. Impose fine and penalties

Comparison

Item	The USA	The EU	Indian Bill
Applicability	The USA has separate sets of laws that apply to Government or on Corporates. In the USA, the laws (both federal as well as state) apply to companies which are dealing with the personal data of US citizens.	GDPR applies to both the Government as well as corporate. It is applicable on all who are processing the data of citizen of the Union	In the Indian bill, the Government has proposed one umbrella law that will apply to all state and non-state entities. Its applicability extends to foreign countries that deal with the personal data of Indian.
Rights of Individuals	Key Rights[71] includes 1. Right to Access to data/ copies of data.	The Key Rights[72] include 1. Right to receive acknowledgment about data	The Key Rights[73] include 1. Right to receive information about

[71] USA: Data Protection 2019 available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (visited on 10 may 2020)

[72] Chapter 3 of GDPR

[73] Chapter V of Data Protection Bill 2019

	2. Right to rectification of error. 3. Right to deletion 4. Right to object to processing 5. Right to restrict processing 6. Right to data portability 7. Right to withdraw consent 8. Right to	processing 2. Right to access by the data subject 3. Right to ratify data 4. Right to portability of data 5. Right of rectification or erasure of personal data or restriction of processing 6. Right to erasure	data processing 2. Right to correction of information 3. Right to data portability 4. Right to be forgotten 5. The right to transfer data in certain circumstances. The right to restrict continuing		object to marketing Right to complain to authorities	7. Right to object to processing 8. Right to object to processing for direct marketing Right to object to automated decisions	disclosure of data.
				Exception to Rights	Due to the absence to any centralized law, the exceptions are very specific, but general exceptions to Rights of the individual are:	Article 23[74] of GDPR defines exceptions like 1. National Security 2. Defense 3. Public Security 4. Prevention, Detection,	General Exceptions[75] are 1. The interest of Security of State 2. Public order 3. Sovereignty and integrity 4. Friendly relation with

[74] Article 23 of GDPR, available at https://gdpr-info.eu/art-23-gdpr/ (Visited on 10 May 2020)

[75] Secion 35 of Data Protection Bill, 2019

	1. Data Processing by Public authority Sharing of information for national security, Public Safety	investigation, or prosecution of a criminal offense, breaches of ethics for a regulated profession 5. Any objective related to the public interest 6. Protection of judicial independence 7. Protection of freedoms of other	foreign State 5. Preventing incitement to the commission of any cognizable offense 6. Prevention, prosecution, and investigation of any offense

		Enforcement of civil law claims	
Authority	The FTC has jurisdiction over the majority of commercial entities. It has the authority to issue and enforce privacy regulations in a specific area.[76]	Article 51 of GDPR mandates the creation of the independent supervisory authority. Independence of such authority is ensured by Article 52	Section 41 of the Bill suggest the creation of a separate authority called Data Protection Authority of India
Sensitive Data	It varies considerably based on sector and statutes. But generally, health data, financial data,	Recital 51 defines racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and	Section 2(36) categorized certain types of data as sensitive data like financial data, health data, sex life, sexual orientatio

[76] *Supra no 72*

	creditworthiness data, student data, biometric data, personal information collected from children under 13, information which could be used to carry out identity theft or fraud.[77]	information related to health and sex life as sensitive data. Article 9 places restrictions on the collection of such information.	n, etc. Section 15 allows the authority to laid down norms to restrict or to place additional safeguards while collecting or processing such information

safety and security of data collected form Indian citizens.

*****

Conclusion

In India, we see the best of both worlds; on the one hand, we have the fundamental right approach toward the Right to Privacy. On the other hand, we also have sector-specific regulations focusing on specific kinds of information and its protection. The present bill tries to streamline the various data protection system that exists in a specific sector with the present bill. One centralized authority will be responsible for ensuring the

[77] https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US (visitd on May 23, 2020)